Vista Manager EX v3.10.x

User Guide

Introduction

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.

About this Guide

This Guide describes how to use Vista Manager EX running the base Vista Manager EX license. It is intended for computer system administrators and network engineers using Vista Manager EX.

You can obtain Vista Manager EX either on a hardware platform:

APL
- **VST-APL:** An application running on Vista Manager Network Appliance (VST-APL) hardware. This Guide also describes setting up Vista Manager on a VST-APL.

or as one of the following software deployments:

VRT
- **VST-VRT:** An application in Vista Manager Virtual (VST-VRT) deployed on VirtualBox 6.1. This Guide describes how to set up Vista Manager EX on VST-VRT. For information about using VST-VRT, including deploying it on VirtualBox, see the Vista Manager Virtual (VST-VRT User Guide).

WIN
- **Windows software:** Software installed directly on a device running Microsoft Windows OS. For installation, see the Vista Manager EX Windows-based Installation Guide.

VA

- **Virtual Appliance:** A stand-alone Vista Manager virtual appliance deployed on Windows Server 2012 R2 Hyper-V or VMware vSphere Hypervisor (ESXi) 6.0/6.5/6.7. For installation, see the Vista Manager EX Virtual Appliance Installation Guide. Note that this virtual appliance does not support Vista Manager plug-ins. If you need the plug-ins, use VST-VRT as the virtualized deployment of Vista Manager.

Where there are differences in this Guide, they are indicated by **APL**, **VRT**, **WIN** and **VA**.

Related documents

For more information, see:

- The Vista Manager web page
- APL The Vista Manager Network Appliance (VST-APL) Technical Documents—for information about how to install and use the VST-APL and the applications supported on it.
- VRT Vista Manager Virtual (VST-VRT) Technical Documents—for information about how to deploy and use the VST-APL and the applications supported on it.
- VA WIN The Vista Manager EX Technical Documents—for information about how to install Vista Manager EX as Windows software or as a virtual appliance on Windows Server 2012 R2 Hyper-V or VMware vSphere Hypervisor (ESXi) 6.0/6.5/6.7. This page also shows how to use Vista Manager EX and its optional features.plug-ins.

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

What Vista Manager EX does

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

- Dashboard
  Displays your network details and network map including all devices connected to each area. Also shows a 24-hour event history at a glance and a list of color-coded recent events.

- Asset Management
  Displays a complete list of all devices on the network and allows you to search for specific devices. This list can be filtered by categories or exported. To manage devices, you can create groups, assign icons or view licenses.

- 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 devices, guest devices, device name and IP address. Actions such as backup master, SSH to master, and backup device can be carried out directly from the network map.

- Events
  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.

- Network Services
  Allows an administrator to learn the status of services running on devices on the network. Configure a monitoring task to run periodically, or to monitor services on demand. You can also view the Access Control List Matrix and RADIUS information.

- Allied Intent-based Orchestrator / AMF Plus
  Provides network optimization, automation, management, and visualization. Also offers automation of branch security and WAN bandwidth management.

- SD-WAN
  Enables you to 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.

- 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.

Vista Manager plug-ins

Optional Vista Manager EX plug-ins are available on:

APL
- Vista Manager Network Appliance (VST-APL).

VRT
- Vista Manager Virtual (VST-VRT).

WIN
- Windows-based installations.

VA Plug-ins are not available on a standalone Vista Manager virtual appliance.

Vista Manager AWC (Wireless Controller) 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 Technical Documents.

Vista Manager 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 and Trap Receiver Technical Documents.

Vista Manager Trap Receiver plug-in

The Vista Manager Trap Receiver plug-in allows you to see a wide range of third-party devices and traps received for them. See the SNMP Plug-in and Trap Receiver Technical Documents.

Contents

Using the SD-WAN Feature

Preparing your AMF Network for Vista Manager EX

Vista Manager EX allows you to monitor and manage your AMF network. Before you can use Vista Manager EX, you need to configure your AMF network. This chapter does not describe how to set up an AMF network. For step-by step instructions, see the AMF Feature Overview and Configuration Guide. This section describes how to prepare your existing AMF network for use with Vista Manager EX.

VRT APL On VST-APL and VST-VRT, the AMF Master may be the AMF Cloud application on the same VST-APL that the Vista Manager EX application is running on, or it may be a remote device.

AMF software version compatibility with Vista Manager EX v3.10.x

- All AMF devices must run version 5.5.0-2.x or later.
- If any of your Controller or Master devices are running 5.5.0-2.x, then all other devices must run 5.5.0-1.1 or later.
- If your AMF Master device is running 5.5.0-0.x, then all other devices must also run 5.5.0-0.x (not 5.5.0-1.x or 5.5.0-2.x).
- If your AMF Master device is running 5.5.0-2.x, then member devices can run 5.5.0-0.x or 5.5.0-1.x.

Server requirement

Vista Manager EX needs to be installed on a server or appliance that has connectivity to your AMF master or controller.

Enable the HTTP service on your devices

To use Vista Manager EX, you must enable the HTTP service on all AMF devices, including all AMF masters and controllers. Some AlliedWare Plus devices are shipped with the HTTP service disabled by default. Ensure that it is enabled on all devices that you want to manage with Vista Manager EX.

To enable the HTTP service, use the commands:

```
awplus# configure terminal
awplus(config)# service http
```

You can use an AMF working set command to configure this option on all your devices:

```
awplus# atmf working-set group all
AMF[10]# configure terminal
AMF[10](config)# service http
```

Allow Vista Manager EX to discover the AMF network

Run the following commands on your AMF controller (if you have one in your network) and all AMF masters to allow Vista Manager EX to discovery your AMF network:

```
awplus# configure terminal
awplus(config)# atmf topology-gui enable
```

Configure the AMF log event host

If the AMF controller or AMF master you intend to register with Vista Manager EX is configured to send event notifications to Vista Manager EX, then Vista Manager EX will display them on its dashboard and event log page.

This command need only be run on the AMF controller/master registered with Vista Manager EX:

```
awplus# configure terminal
awplus(config)# log event-host <vista-manager-ip-addr> atmf-topology-event
```

Note: The IP address is the address of the server that Vista Manager EX is running on.

where `<vista-manager-ip-addr>` is the IP address of the Vista Manager EX instance.

Note: The AMF controller/master you intend to register with Vista Manager EX must have layer 3 connectivity to Vista Manager EX server.

Configure certificate for device authentication

Vista Manager EX is able to be configured to use a certificate to authenticate communication within your AMF network. Once the AMF controller/master has been configured, this process is automatic, and allows the controller/master to authenticate and connect to any device in the network without requiring a username and password.

Note: Using this feature is optional, but highly recommended. If you do not configure this option, you will need to ensure that all devices in the AMF network to be managed by Vista Manager EX have the same username and password as the AMF controller/master.

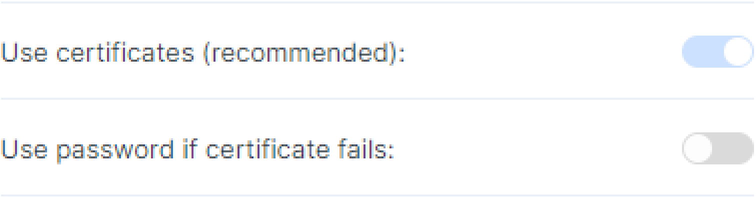
To configure your AMF network to use certificate authentication, enter the following commands on your AMF controller/master:

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint <trustpoint-name>
awplus(ca-trustpoint)# enrollment selfsigned
awplus(ca-trustpoint)# rsakeypair <key-name>
awplus(ca-trustpoint)# exit
awplus(config)# exit
awplus# crypto pki authenticate <trustpoint-name>
awplus# crypto pki enroll <trustpoint-name>
awplus# configure terminal
awplus(config)# atmf trustpoint <trustpoint-name>
```

Note: Save this configuration and reboot your AMF controller/master after running the **atmf trustpoint** command for this change to take affect.

Note: In an AMF network with multiple areas, this process only needs to be carried out on the controller/master. It does not need to be repeated on each individual area's master.

This functionality is disabled by default, but it is recommended that it is enabled. If you need to turn this feature on or off, this can be done from Vista Manager EX configuration settings:



Use certificates (recommended): ●

Use password if certificate fails: ○

The **Use password if certificate fails** option can also be enabled. When it is turned **On**, if the certificate authentication fails, it will revert to using the username and password to authenticate. This will only work if all devices have been configured with the same username and password as the controller/master, as mentioned above.

Connection timeout on masters and controllers

We recommend not changing the session timeout on your Vista Manager EX master or controller using the **line vty exec-timeout** command. If you do decide to change it, it should not be set to **0**, as this may result in sessions that can't be reached and never time out.

Initial Login to Vista Manager EX

This section describes logging in and initial setup for Vista Manager EX.

APL Before setting up Vista Manager EX on the VST-APL, you need to activate and start the Vista Manager application on the VST-APL. For information about using the VST-APL, including activating applications, see the Vista Manager Network Appliance (VST-APL) User Guide.

VRT Before setting up Vista Manager EX on VST-VRT, you need to deploy the VST-VRT. For deployment and configuration information for VST-VRT, see the Vista Manager Virtual (VST-VRT) User Guide.

VA WIN For installation instructions, see the Vista Manager EX™ Installation Guides.

This section describes:

- "Log in to Vista Manager EX" on page 12
- "Registering the plug-ins" on page 16

Note that dialog boxes in this section are from a VST-APL. In most cases, the dialog boxes are the same for all Vista Manager platforms.

Log in to Vista Manager EX

VRT APL To connect remotely, use your browser to go to the URL:

```
http://<ip-address>
```

where <ip-address> is the address of the Vista Manager application. This is the IP address you assigned statically to Vista Manager or that you set it to obtain by DHCP when configuring the application. You can find this IP address by hovering over the instance information icon for the Vista Manager application in the VST-APL or VST-VRT GUI.

WIN 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 assigned on the **Registration Server IP Address** dialog.

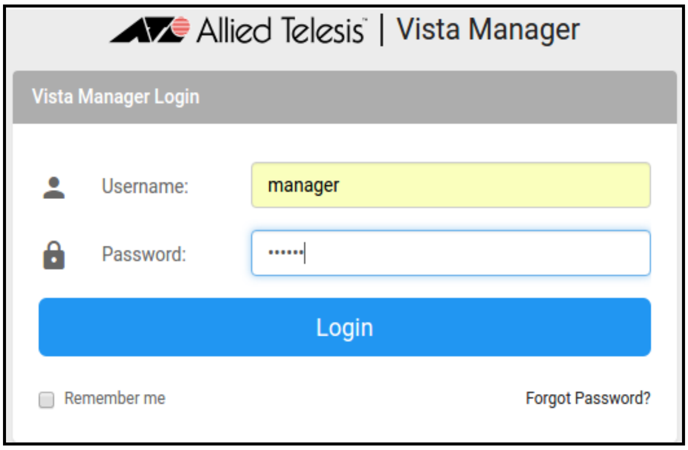
VA To connect remotely, use the URL:

```
http://<ip-address>
```

where <ip-address> is the address displayed on the Vista Manager EX appliance console screen after it boots.

Note: Vista Manager requires JavaScript to be enabled in your web browser.

From the **Vista Manager Login** dialog:

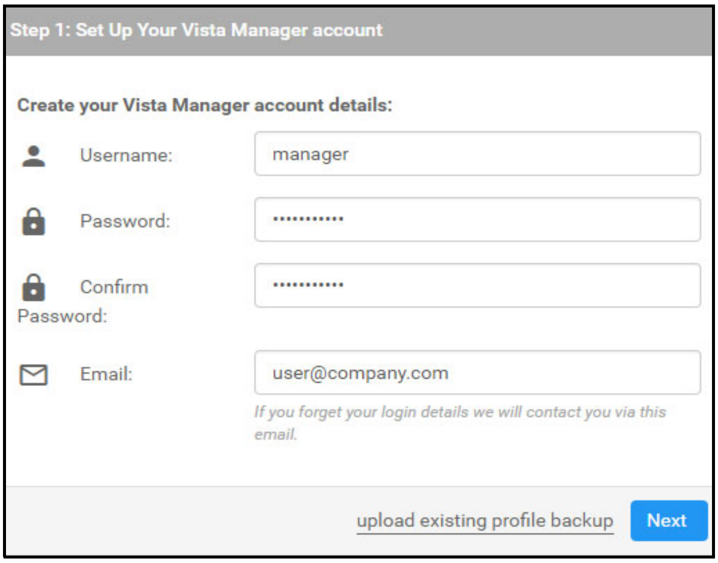


Username: manager

Password: ••••••

- Enter the **Username** manager
- Enter the **Password** friend
- Click **Login**

The **Set Up Your Vista Manager account** dialog displays:


Step 1: Set Up Your Vista Manager account
upload existing profile backup
Next

Create your Vista Manager account details:

Username: manager

Password: •••••••••••

Confirm Password: •••••••••••

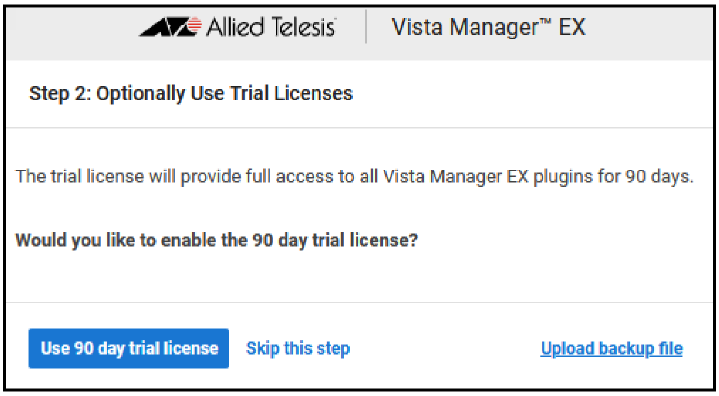
Email: user@company.com

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

- Enter your **Username**
- Enter your **Password**
- Re-enter your Password to **Confirm**
- Enter your **Email**
- Click **Next**.

If you want to use a backup to restore a previous database, click **upload existing profile backup**.

APL The **Optionally Use Trial Licenses** dialog displays:



Step 2: Optionally Use Trial Licenses

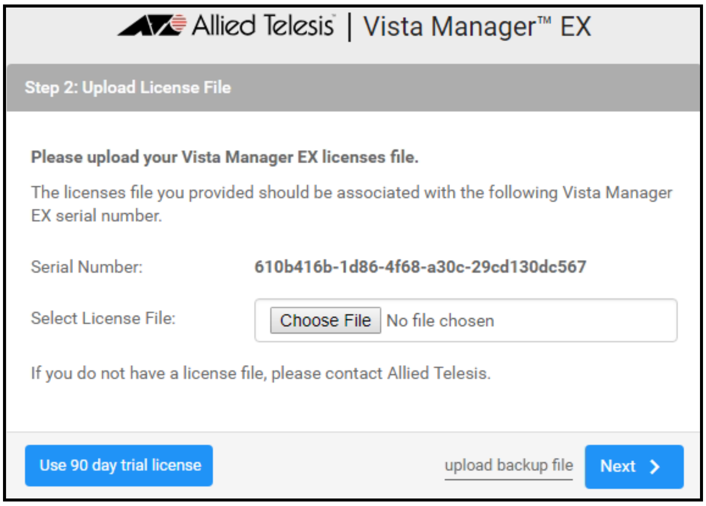
The trial license will provide full access to all Vista Manager EX plugins for 90 days.

Would you like to enable the 90 day trial license?

- On the VST-APL, you can click **Skip this step**.
  No license is required on the VST-APL for Vista Manager EX or the Trap Receiver plug-in.
- If you select the 90-day trial, you need to install your licenses before the end of that trial. See **"About Vista Manager EX Licenses" on page 19**.

VRT WIN VA

The **Upload License File** dialog displays:


Allied Telesis | Vista Manager™ EX

Step 2: Upload License File

Please upload your Vista Manager EX licenses file.

The licenses file you provided should be associated with the following Vista Manager EX serial number.

Serial Number: 610b416b-1d86-4f68-a30c-29cd130dc567

Select License File: Choose File No file chosen

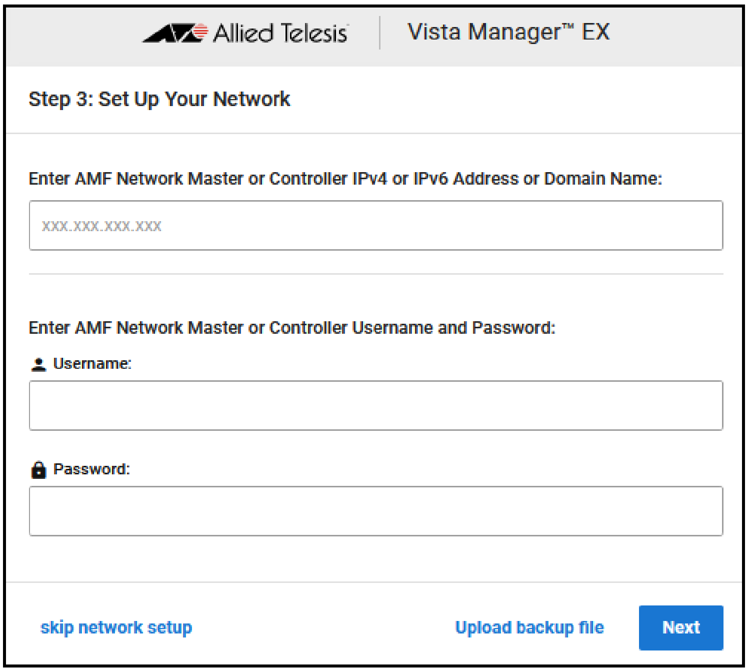
If you do not have a license file, please contact Allied Telesis.

- Otherwise, install your licenses now by selecting the license file, or select the 90-day trial.
- If you select the 90-day trial, you need to install your licenses before the end of that trial. See **"About Vista Manager EX Licenses" on page 19**.
- Click **Next**.

Note: If your licenses file is not associated with the Serial Number listed in your dialog or you do not have a license file, then contact your authorized Allied Telesis support center to obtain a license.

Note: If this is the first time you are using Vista Manager EX, you have the option to apply the 90 day trial license for other licensed features, such as the AWC plug-in and the AIO feature, by clicking **Use 90 day trial license**. On the VST-APL, the base Vista Manager EX license will continue to work after 90 days if you choose this option.

The **Set Up Your Network** dialog displays:


Allied Telesis | Vista Manager™ EX

Step 3: Set Up Your Network

Enter AMF Network Master or Controller IPv4 or IPv6 Address or Domain Name:

xxx.xxx.xxx.xxx

Enter AMF Network Master or Controller Username and Password:

Username:

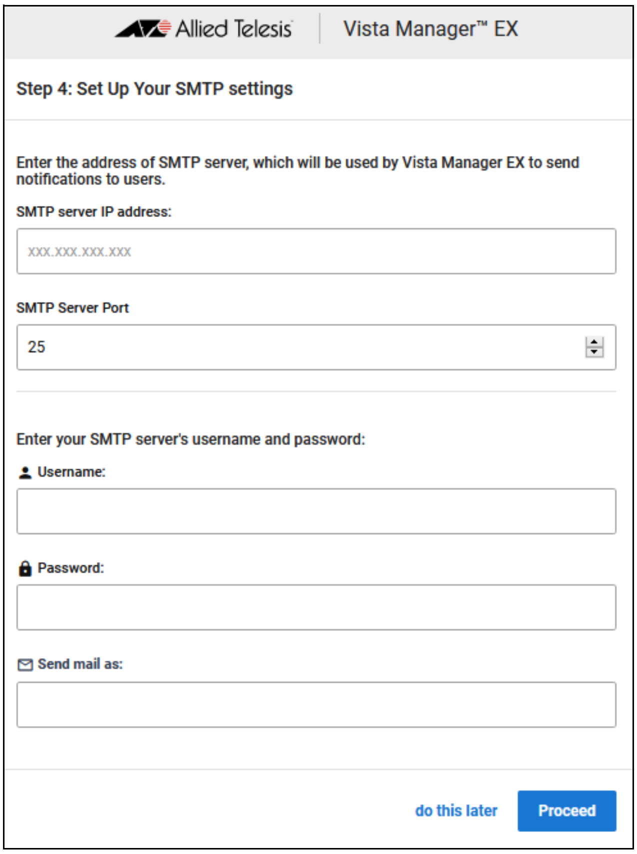
Password:

- Enter the **IP Address** for the AMF Master or Controller

VRT APL The AMF Master may be the AMF Cloud application on this VST-APL or VST-VRT deployment, or it may be any other AMF Master or Controller.

- Enter the AMF Controller or Master **Username**
- Enter the AMF Controller or Master **Password**

The **Set Up Your SMTP settings** dialog displays.



Allied Telesis | Vista Manager™ EX

Step 4: Set Up Your SMTP settings

Enter the address of SMTP server, which will be used by Vista Manager EX to send notifications to users.

SMTP server IP address: xxx.xxx.xxx.xxx

SMTP Server Port: 25

Enter your SMTP server's username and password:

Username:

Password:

Send mail as:

- Enter the **IP Address** of your SMTP server

You may also enter:

- the **SMTP Server Port**
- the SMTP Server **Username**
- the SMTP Server **Password**
- the **Send mail as** email address.

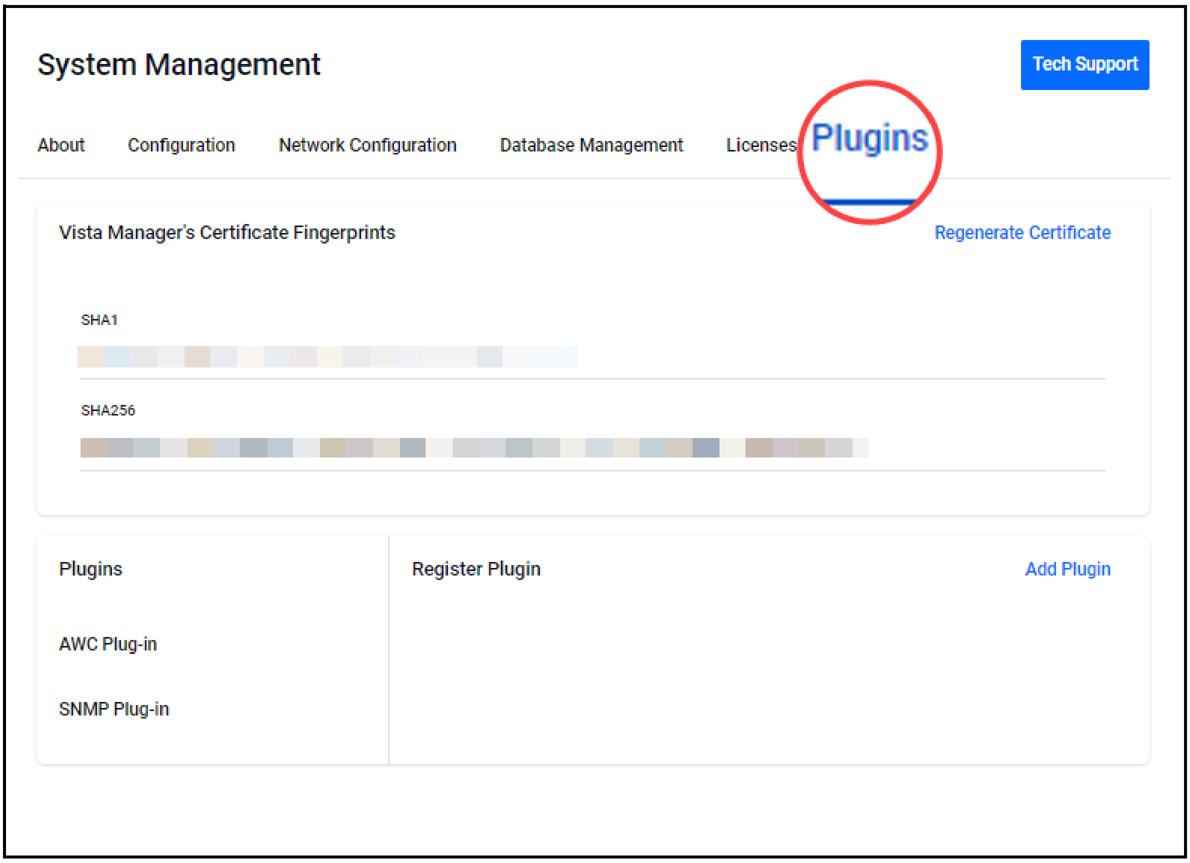
You will receive a message saying that the set up is successful.

Registering the plug-ins

VRT APL WIN

The AWC and SNMP (full) plug-ins require separate subscription licenses from Vista Manager. See **“Log in to Vista Manager EX” on page 12** and **“About Vista Manager EX Licenses” on page 19** for details.

After you have successfully logged in to Vista Manager EX, to set up the plug-ins, select **System Management** from the **Vista Manager EX** menu. Then go to the **Plugins** tab:



AWC plug-in

1. Click **Add Plug-in** and enter the following details for the AWC plug-in:

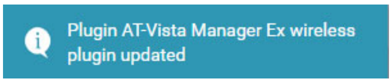
   Server URL: https://<ip-address>:5443/wireless_plugin

   where <ip-address> is the IP address of the Wireless Controller (AWC) plug-in application.

2. Click **Verify Connection**

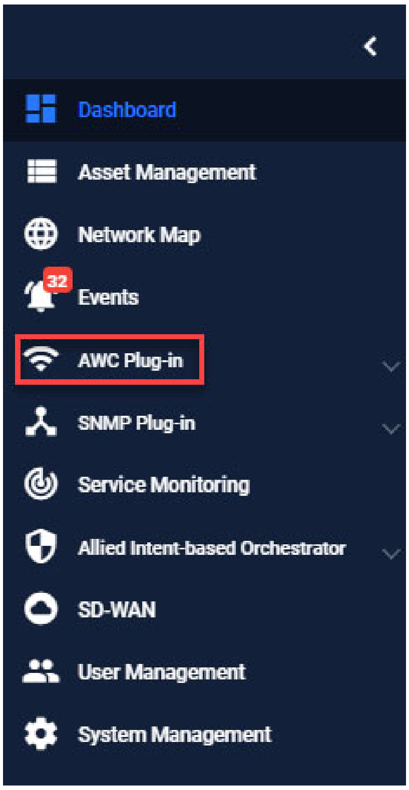
3. Click **Save**.

The following information message is displayed showing that the plug-in has been updated:

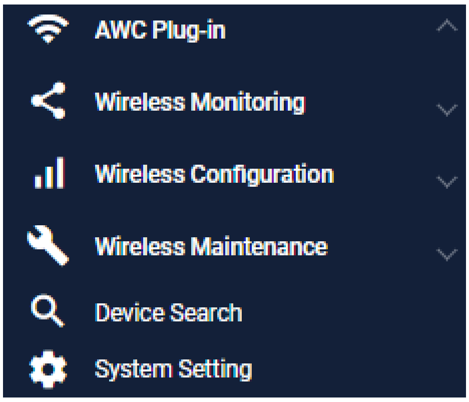


Plugin AT-Vista Manager Ex wireless plugin updated

You can now access the **AWC** plug-in from the **Vista Manager EX** menu as follows:



There is now a **Wireless** icon on the Vista Manager EX menu. When you click on this icon it will display the AWC menu items.



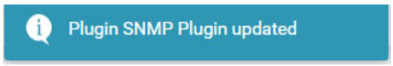
SNMP plug-in

1. Click **Add Plug-in** and enter the following details for the SNMP (full) or Trap Receiver plug-in:

   `Server URL: https://<ip-address>:6443/NetManager`

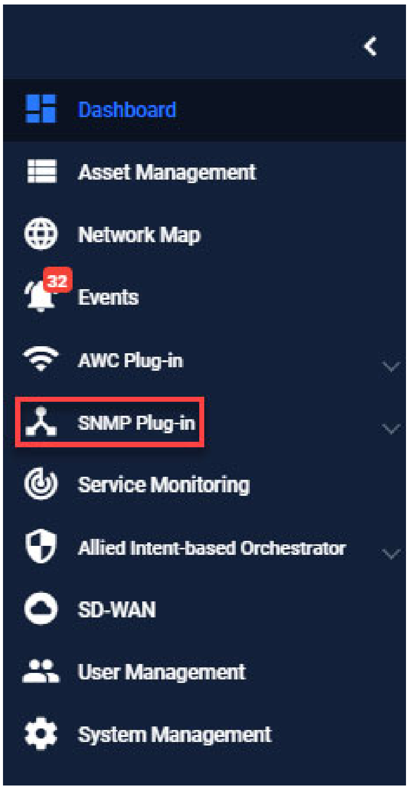
   where <ip-address> is the IP address of the SNMP or Trap Receiver plug-in application.
2. Click **Verify Connection**
3. Click **Save**.

The following information message is displayed showing that the plug-in has been updated:

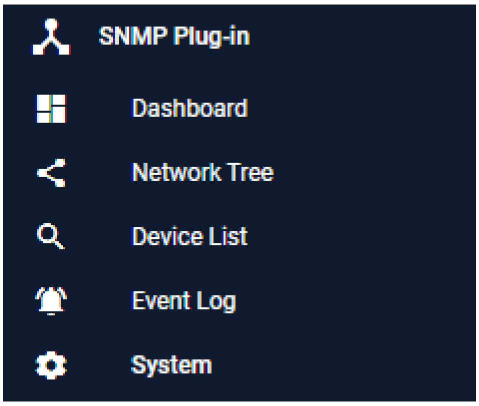


Plugin SNMP Plugin updated

You can now access the **SNMP** plug-in from the **Vista Manager EX** menu as follows:



There is now an **SNMP** icon on the Vista Manager EX menu. When you click on this icon it will display the SNMP menu items.



About Vista Manager EX Licenses

Licensed features

APL

Vista Manager EX base license is enabled by default on the VST-APL. Licenses for optional features and plug-ins are applied during the Vista Manager EX software installation procedure. Download the license file from the Allied Telesis download center. Subscription licenses are tied to the Vista Manager database and are maintained across backups and restores.

You can install multiple plug-in licenses (for the same feature) each with their own license period. This allows you to manage a total number of devices equal to the sum of the devices of the active licenses. For example, if you have two SNMP plug-in licenses installed, each for 10 devices, you will be able to manage a total of 20 devices through the SNMP plug-in.

After clearing the Vista Manager database:

- Trial licenses are retained.
- Non-trial licenses are lost. (Licenses are tied to a serial number; initialization loses the old serial number and generates a new one.)

If you import a backup, the serial number and any licenses are tied to the backup.

VRT WIN

Vista Manager EX licensing is subscription based. Download the license file from the Allied Telesis download center. The base license file is applied during the Vista Manager software installation procedure. Subscription licenses are tied to the Vista Manager database and are maintained across backups and restores. If, however, you reinitialize the database you will need to get a new license file.

The base license and optional plug-in licenses have separate license periods. If the base license expires, the optional features will not be available, even if they are still licensed.

You can install multiple plug-in licenses (for the same feature) each with their own license period. This allows you to manage a total number of devices equal to the sum of the devices of the active licenses. For example, if you have two SNMP plug-in licenses installed, each for 10 devices, you will be able to manage a total of 20 devices through the SNMP plug-in.

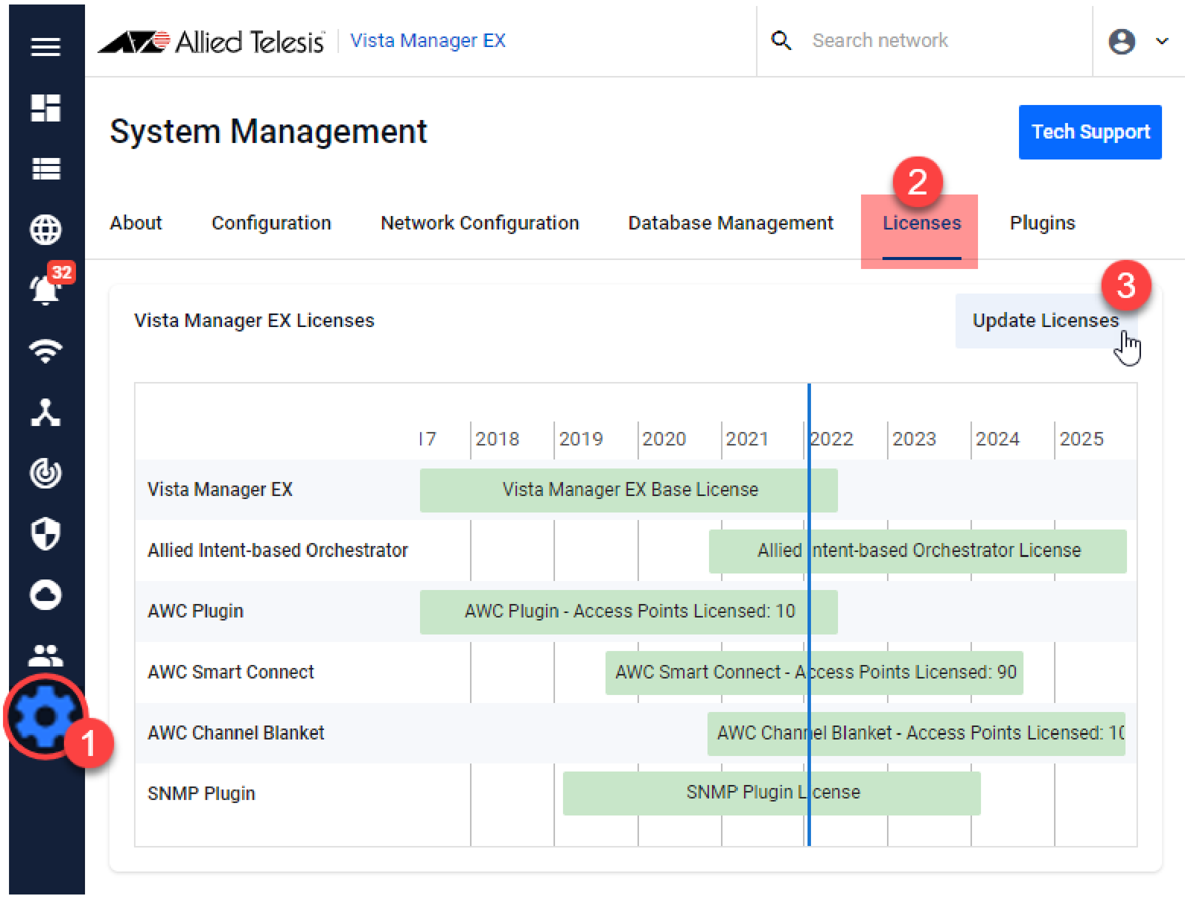
VA

Vista Manager EX licensing is subscription based. Download the license file from the Allied Telesis download center. The base license file is applied during the Vista Manager software installation procedure. Subscription licenses are tied to the Vista Manager database and are maintained across backups and restores. If, however, you reinitialize the database you will need to get a new license file.

Managing your licenses

The initial login procedure includes installation of licenses or the option to select the 90-day trial license. For instructions, see "Log in to Vista Manager EX" on page 12.

1. To add a new license to Vista Manager EX, or view existing licenses, navigate to **System Management**.
2. Then go to the **Licenses** tab.
3. To add a new license click the **Update Licenses** button and select the required license file to upload.



APL On the VST-APL, the Vista Manager EX base license is enabled by default. It is not shown in the graph. A note on the page indicates this.

For more information on licensing options and plug-ins see the Vista Manager EX Datasheet.

90-day trial license

As long as you are using Vista Manager EX for the first time, you can use a 90 day trial license. A trial license is only available on new installations. It is not available on systems that have been previously licensed, or systems restored from backups that have been previously licensed.

APL On the VST-APL, the base Vista Manager EX license is enabled by default, and does not give access to additional features including plug-ins. If you choose the 90-day trial license during login, this gives full access to additional features available for Vista Manager EX, including AMF Plus or the Allied Intent-based Orchestrator (AIO), and the plug-ins. There is no grace period after the license expires, but you will receive expiry notifications at 28, 21, 14, 7, and 1 day/s before expiry. You can add a purchased license on the license management page at any time before the trial has finished.

VRT WIN The 90-day trial license gives full access to Vista Manager EX, AMF Plus or the Allied Intent-based Orchestrator, and the plug-ins. There is no grace period after the license expires, but you will receive expiry notifications at 28, 21, 14, 7, and 1 day/s before expiry. You can add a purchased license on the license management page at any time before the trial has finished.

VA The 90-day trial license gives full access to Vista Manager EX and AMF Plus or the Allied Intent-based Orchestrator. There is no grace period after the license expires, but you will receive expiry notifications at 28, 21, 14, 7, and 1 day/s before expiry. You can add a purchased license on the license management page at any time before the trial has finished.

Using Vista Manager EX

Logging into Vista Manager EX

VRT APL

To connect remotely, use your browser to go to the URL:

```
http://<ip-address>
```

where <ip-address> is the address of the Vista Manager application. This is the IP address you assigned statically to the Vista Manager application or that you set it to obtain by DHCP when configuring the application. You can find this IP address by hovering over the instance information icon for the Vista Manager application in the VST-APL or VST-VRT GUI.

WIN

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.

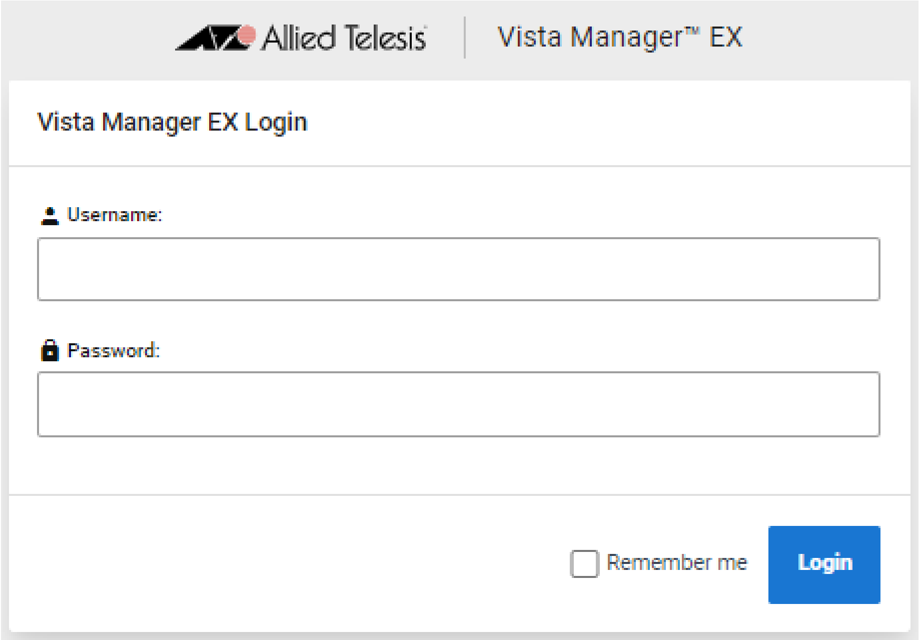
VA

To connect remotely, use the URL:

```
http://<ip-address>
```

where <ip-address> is the address displayed on the Vista Manager EX appliance console screen after it boots.

The **Vista Manager Login** dialog displays:



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

Change password

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

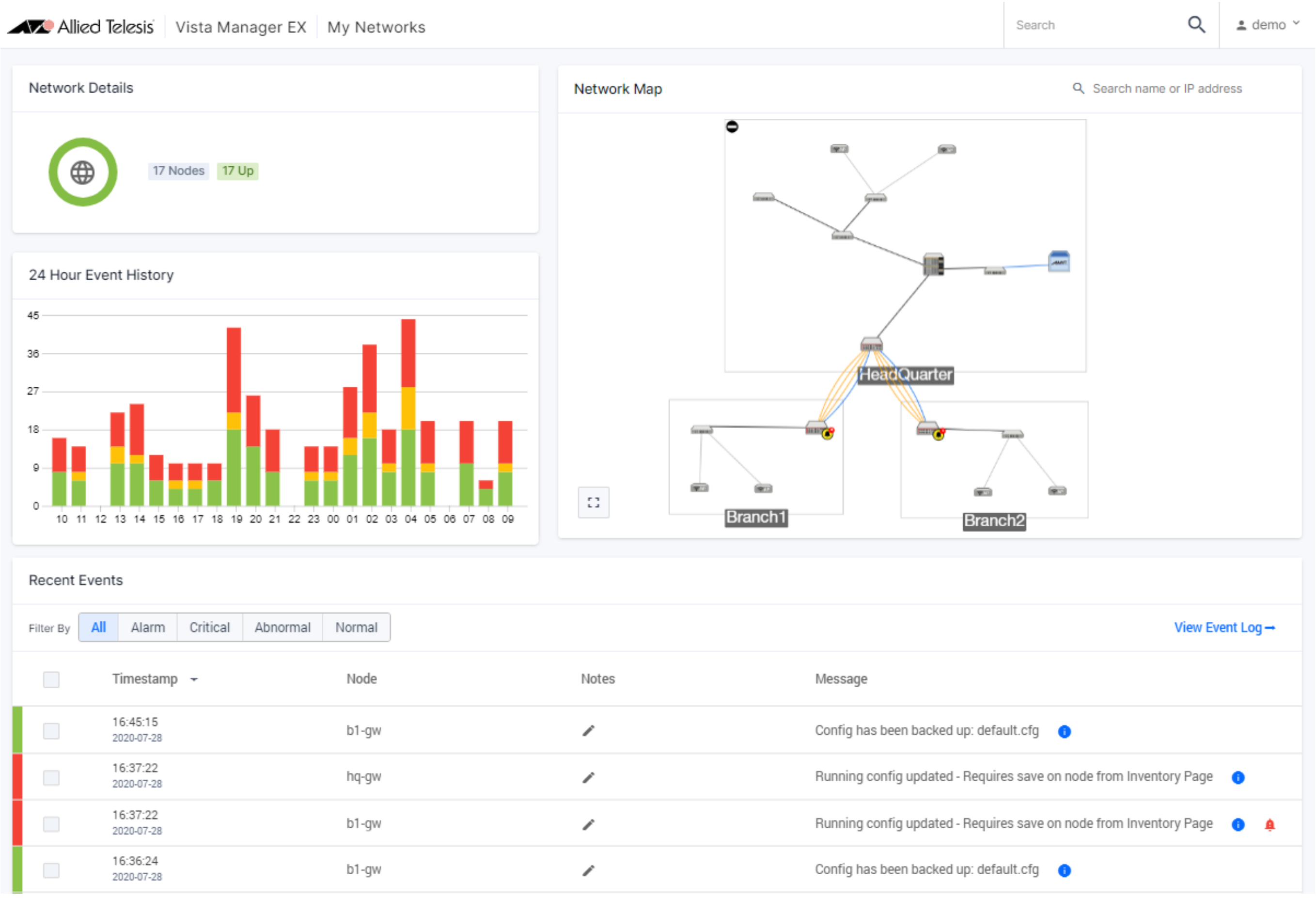
Logout

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:



□	Timestamp	Node	Notes	Message
□	16:45:15 2020-07-28	b1-gw	✎	Config has been backed up: default.cfg
□	16:37:22 2020-07-28	hq-gw	✎	Running config updated - Requires save on node from Inventory Page
□	16:37:22 2020-07-28	b1-gw	✎	Running config updated - Requires save on node from Inventory Page
□	16:36:24 2020-07-28	b1-gw	✎	Config has been backed up: default.cfg

The dashboard displays the following information about your network:

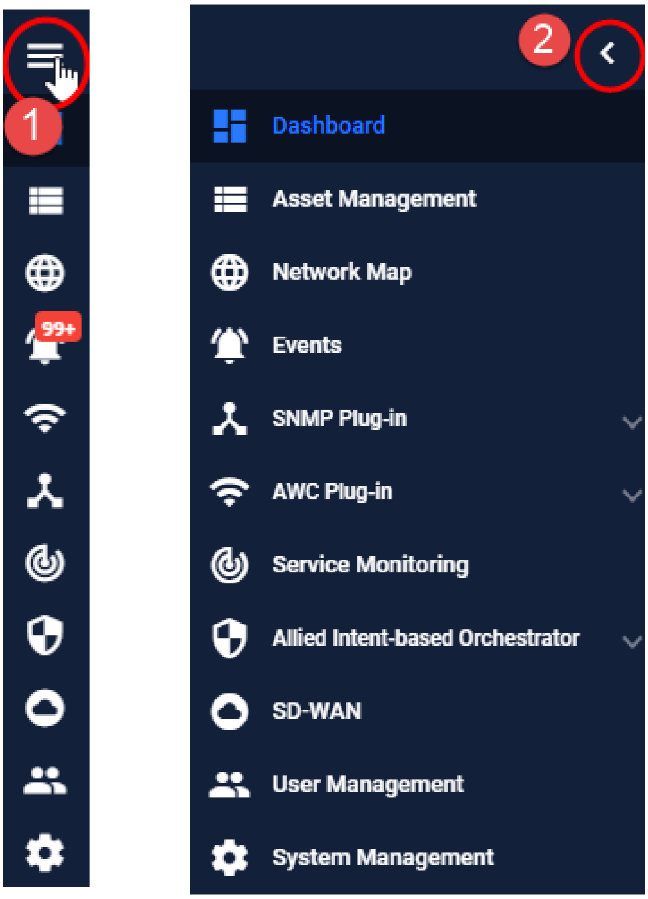
Field	Description
Network Details	Shows the number of devices and status (up, down, abnormal or unmanaged).
24 Hour Event History	Shows a graph of the last 24 hours of log events history.
Recent Events	Displays time, device and any notes or messages relating to each event.
Network Map	Displays the network 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, Allied Intent-based Orchestrator or AMF Plus, SD-WAN, User Management, and System Management. Any optional plug-ins will also appear in this menu.

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

1. Click the menu icon to expand the menu. The expanded menu displays the name of each menu option.
2. Click the small white arrow to collapse the menu.



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.

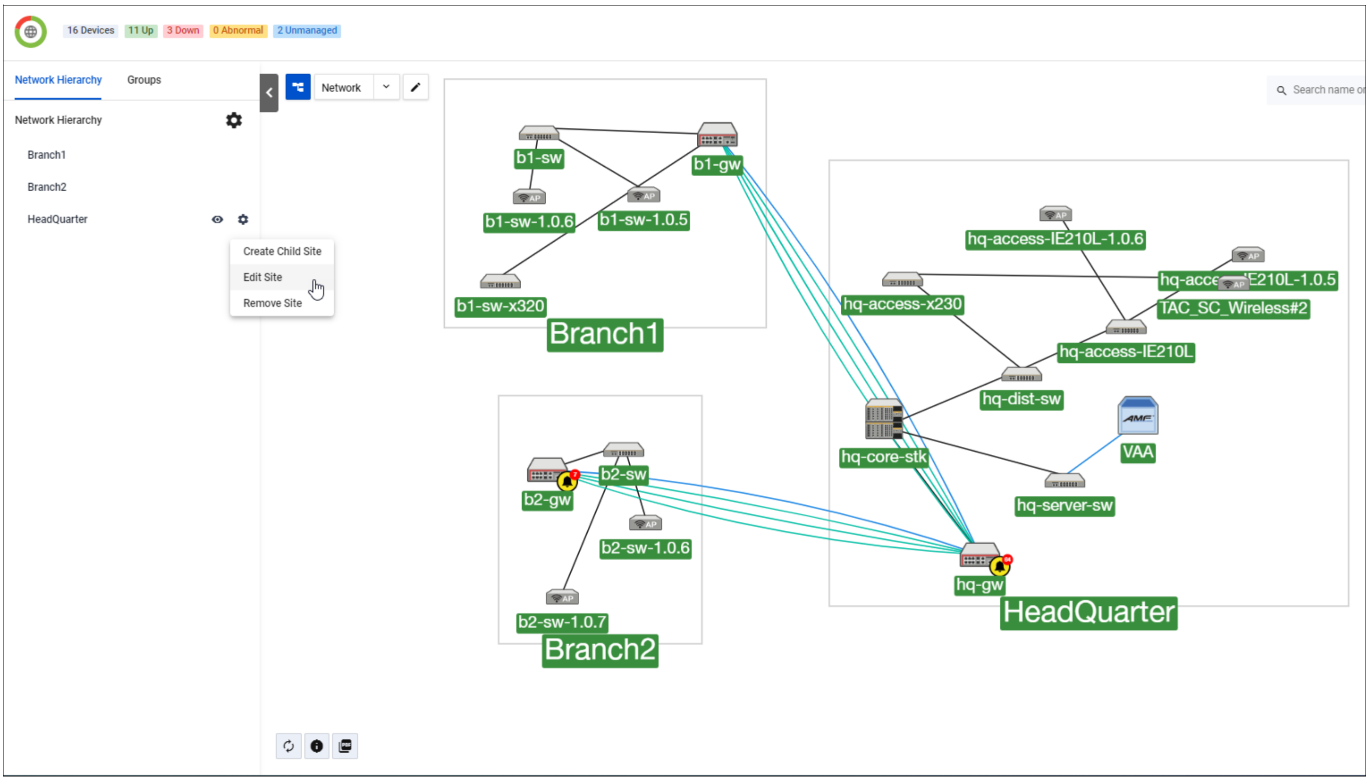
Access the integrated map in its own screen by using the Network Map option in the left-hand menu. From the Network Map you can display details about sites in the network hierarchy and identify the devices in each site.

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

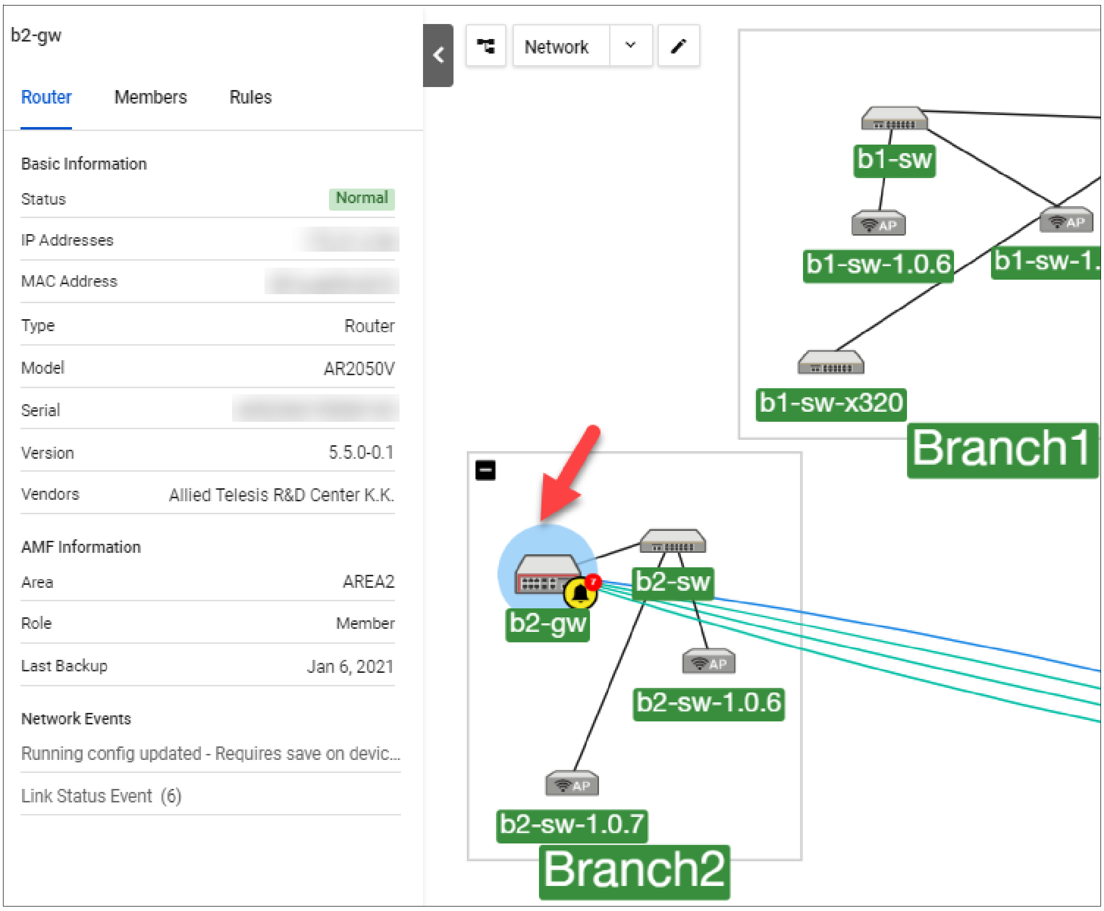
- Location - buildings and devices can be assigned to a location.
- Building - floors and devices can be assigned to a building.
- Floor - devices can be assigned to a floor.

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 device or double clicking on a device will show all the device information as follows:



b2-gw

Router | Members | Rules

Basic Information

Status	Normal
IP Addresses	[redacted]
MAC Address	[redacted]
Type	Router
Model	AR2050V
Serial	[redacted]
Version	5.5.0-0.1
Vendors	Allied Telesis R&D Center K.K.

AMF Information

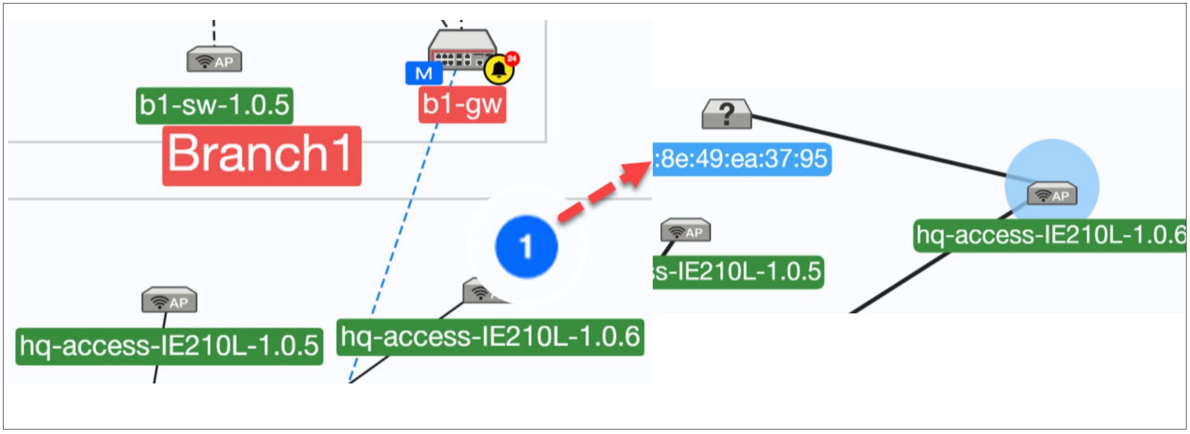
Area	AREA2
Role	Member
Last Backup	Jan 6, 2021

Network Events

Running config updated - Requires save on devic...

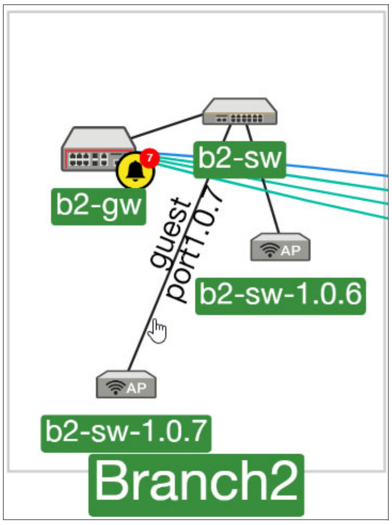
Link Status Event (6)

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



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

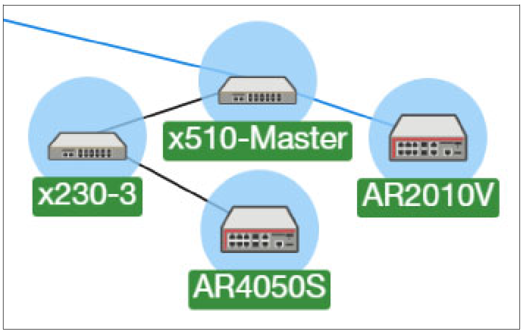
Managed guest devices attached to a device are indicated by grey links. Hovering over a grey link displays the port number.



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

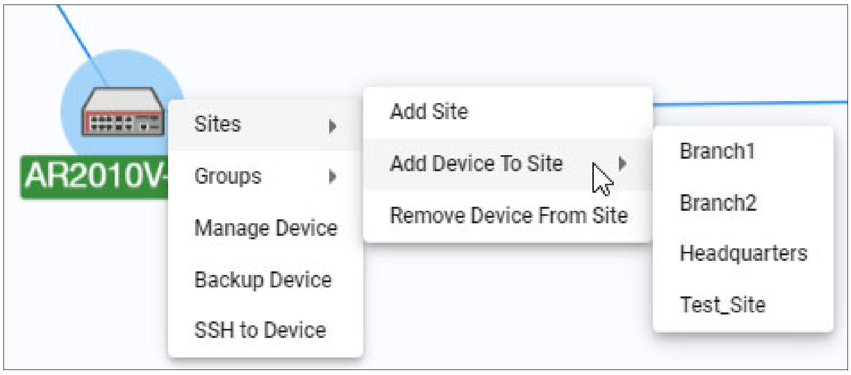
To select a device or devices, hold **Ctrl** and select each device you want selected. Alternatively, hold **Ctrl**, then click on the area and drag over the devices you want selected.

Selected devices are highlighted in blue as follows:



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

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

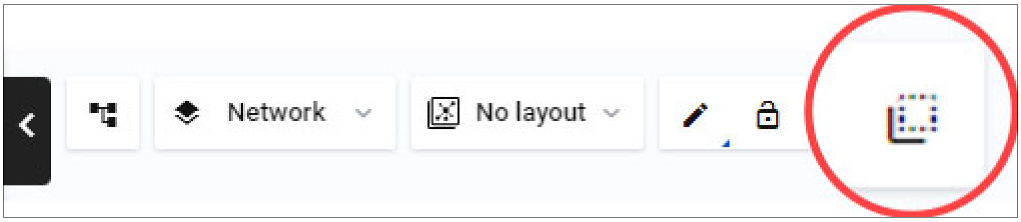


For more information on backing up a device, see **"Backup a device" on page 47**. For more information on SSH to Master, see **"SSH/Shell to a device" on page 48**.

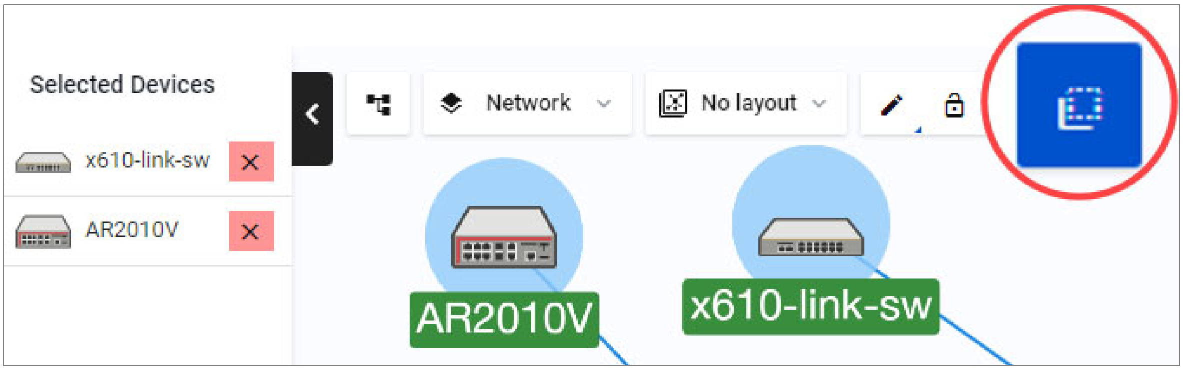
Multi-select mode

Enable this button to select multiple devices without holding the **control** or **shift** keys.

Note: The multi-select button will be available on all map modes, except **tracepath** and **tunnel creation**.



With the multi-select button enabled, the side panel appears showing a list of selected devices when more than one device is selected. Click on ‘x’ to remove a device from the list. Click a selected device on the map to deselect it. Click anywhere on the map to remove all selected devices from the list. When only one device is left selected, the side panel then shows details of that device.



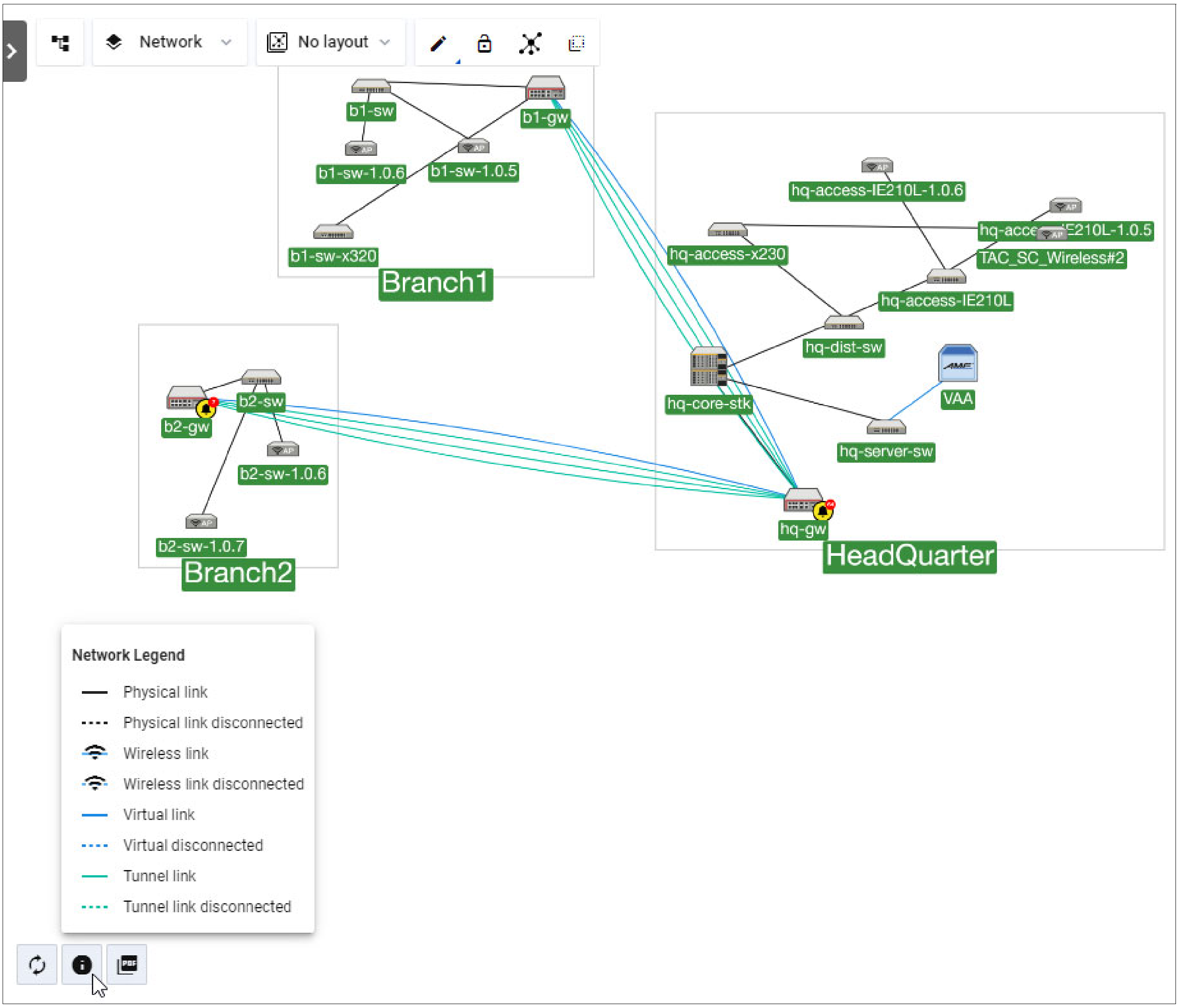
Backwards navigation

Backwards navigation is supported on specific pages. This button lets you move efficiently between pages during a single task flow on multiple devices, like updating release files or deploying policies.

For example, you navigate to the Device Info tab from Asset Management, and then browse through several different tabs from there. Clicking on the browser back button only returns you to the previous tab, but the backwards button takes you straight back to Asset Management.

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 a green 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

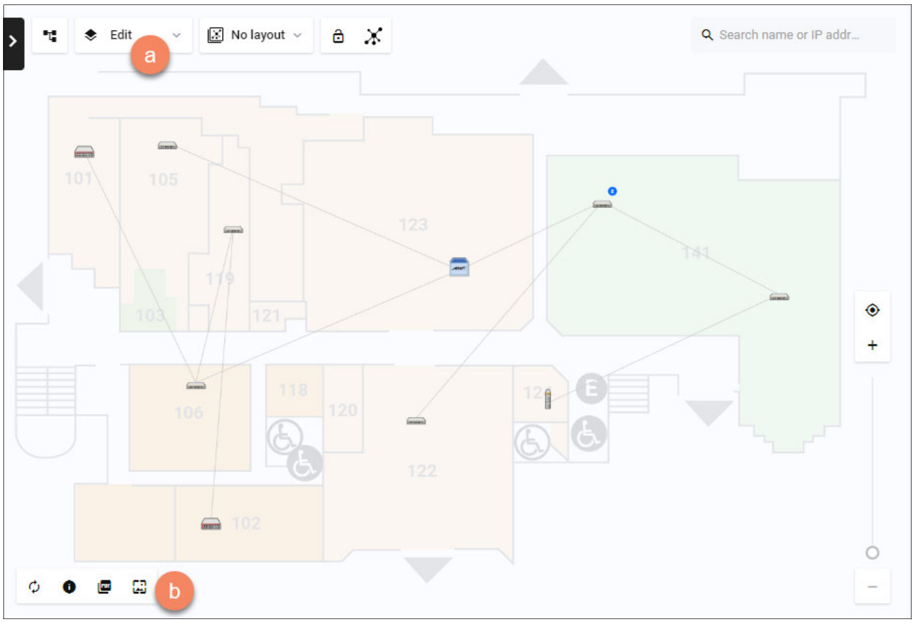
You can import a background image to a map screen. This is useful for using a building or floor map to show the physical location of devices.

a. From the **Network Map**, go to **Edit** mode.

b. Click on the image icon in the bottom left-hand corner.

Click **Select file** to browse for your floor plan and select the file. Then click **Open**. You can set 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 devices so they are located in the correct areas in the diagram as follows:



To delete an image, click on the image icon and click **Delete**. Confirm that you are sure you want to delete the image, and if you are sure, click the **Delete** button.

Refreshing the map when your AMF network changes

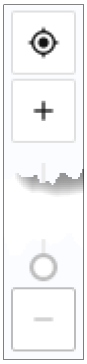
New devices appear automatically via polling, or you can click the Refresh icon on a map screen for an immediate result.

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.

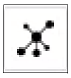


Zoom functionality on integrated maps

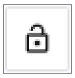
This functionality also supports touch input. You will be able to zoom in and out by clicking the (+/-) buttons or dragging the zoom slider. The reset zoom button lets you zoom out to fit the entire network within the map window.

Integrated map layouts

The integrated map supports two layout functionalities.



- **Auto generate layout** - This button lets you automatically generate a topology layout which creates a new layout for your map. Take note that this process cannot be reversed. It is disabled when locked layout is active.



- **Lock layout** - This button provides the lock/unlock ability to move devices around. The status will be saved even after you log out and back in again. You can use this layout to:
  - change the position of devices (when unlocked)
  - pan the map view around devices (not sites or groups)

Regardless of the lock status:

- zooming or looking around the map are not affected
- expanding or collapsing sites and stacks will function normally
- moving devices on the dashboard network map will now always be locked

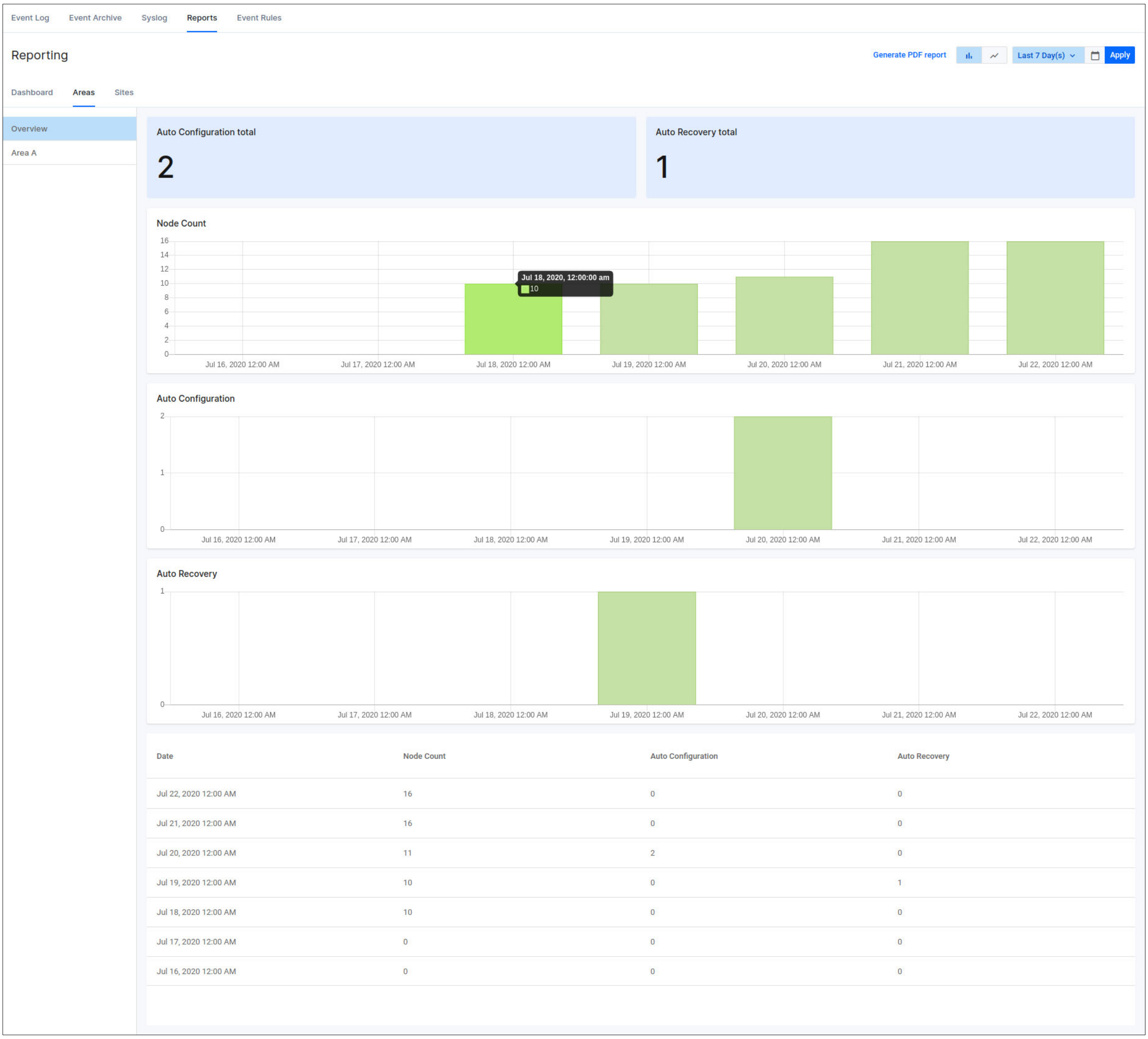
Note: As this is a per-user feature, in the event that an account is shared among multiple users, one user’s change will affect all users.

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.



Date	Node Count	Auto Configuration	Auto Recovery
Jul 22, 2020 12:00 AM	16	0	0
Jul 21, 2020 12:00 AM	16	0	0
Jul 20, 2020 12:00 AM	11	2	0
Jul 19, 2020 12:00 AM	10	0	1
Jul 18, 2020 12:00 AM	10	0	0
Jul 17, 2020 12:00 AM	0	0	0
Jul 16, 2020 12:00 AM	0	0	0

Topology map layout management

Topology map layout management gives you the ability to design map layouts so that you can predefine the default layouts for different users. You can design different network map layouts, and switch the network map layouts easily. You can also set a designed network map layout as the default map layout for everyone, or for a specific user. This means each user will see a well-organized network map when they log in for the first time.

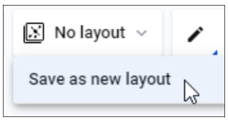
You can design integrated map layouts in all the map modes. The Topology Map layout contains the following:

- Node positions
- Background image
- Expand/collapse status of sites and stacking devices
- Zoom and panning position
- Manually added static/discovered devices

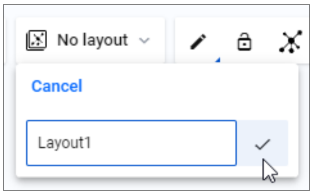
Creating a new layout

To create a new layout:

1. Click on the layout drop-down. If this is your first layout, the name will be **No layout**. Otherwise, it will be the name of the currently selected layout.

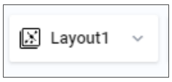


2. Enter a name for your new layout, and click on the check mark to save the layout.



Layout1

3. The new layout will become the selected layout.



You can create a new layout based on an existing layout by saving the current layout with a new name. Different users can have different map layouts with the same name.

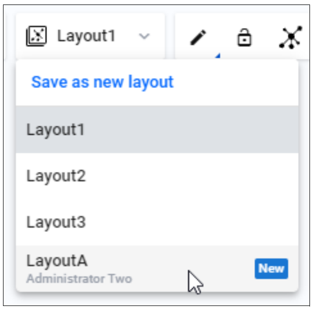
If you save your current layout with the name of an existing layout, it will overwrite it. You can only overwrite map layouts you create.

Selecting a layout

The integrated map has a drop-down list to show the current layout, and all available layouts. All the layouts created by the current user will be visible in the drop-down list. Additionally, if the current user is an administrator user, the layouts created by other administrators will also be visible in the drop-down list. If a network layout has been set as the default layout for this user or everyone, the default layout is also visible in the drop-down list. For map layouts created by other users, the author's name is displayed as part of the map name to help identify it.

To select a layout:

1. Click on the layout drop-down.
2. Select a layout from the displayed list.

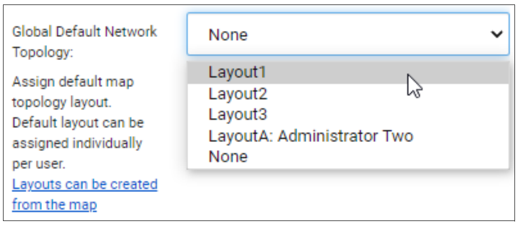


Setting the default layout

Administrators can select a map layout and set it as the global default map layout for all users.

To set the global default layout:

1. Select **User Management** from the menu.
2. Select your user, and click on the **Edit** button.
3. In the **Global Default Network Topology** section, click on the drop-down, and select the layout to be the default.



Global Default Network Topology:

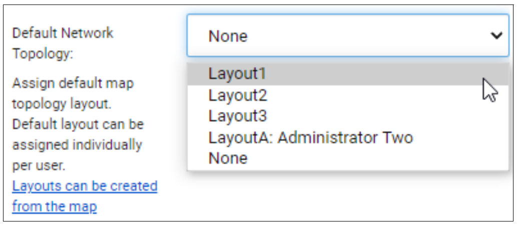
Assign default map topology layout. Default layout can be assigned individually per user. Layouts can be created from the map

4. Click on the **Save** button.

Administrators can also select a map layout and set it as the default map layout for a specific user.

To set the default layout for a specific user:

1. Select **User Management** from the menu.
2. Select the user whose default you want to set, and click on the **Edit** button.
3. In the **Global Default Network Topology** section, click on the drop-down, and select the layout to be the default.



Default Network Topology:

Assign default map topology layout. Default layout can be assigned individually per user. Layouts can be created from the map

4. Click on the **Save** button.

When a user logs in for the first time, the default map layout will be used. The default map layout will also be included in the map layout drop-down list.

Deleting a saved layout

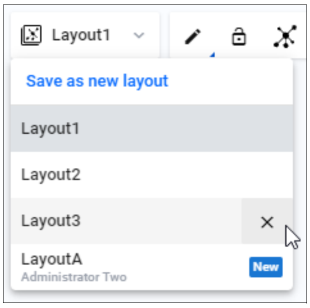
Administrators can delete any map layout. Users can only delete map layouts that they created.

If an administrator deletes a map layout that is being used as the default map layout by some Vista users, those users' default map layout will change to the global default map layout. If an administrator deletes the global default map layout, there will be no default map layout.

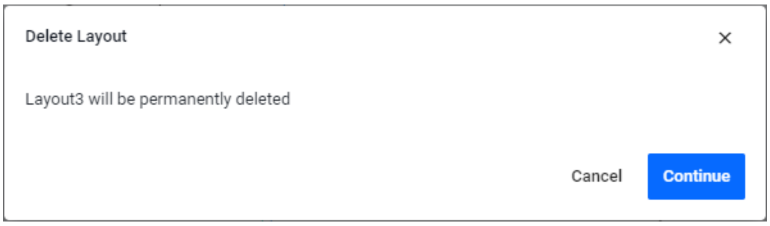
If the currently selected layout is deleted, including the default layout, the selected layout will be changed to be **No layout**, while the map will remain unchanged.

To delete a layout:

1. Click on the layout drop-down.
2. Select the layout you want to delete, and click on the X icon.



3. On the confirmation dialog, click **Continue** to delete the layout.


Delete Layout

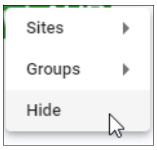
Layout3 will be permanently deleted

Hiding devices in the layout

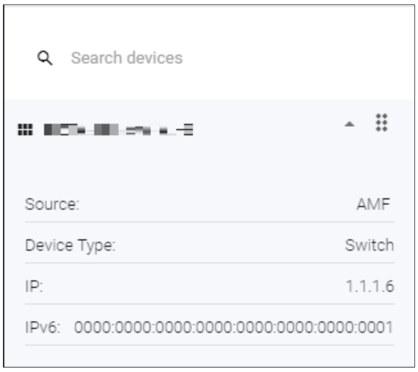
You can change which devices are visible on the network map. For example, you may only be interested in seeing servers on the network map, and can therefore hide the other devices.

To change the visibility of a device:

1. Click on **Edit** in the drop-down on the network map screen.
2. Right click on the device you want to hide.
3. Click on **Hide**.



The hidden device will be added to the **Devices** list. Click the down arrow to see the details of a device in the list.



[redacted]

Source: AMF

Device Type: Switch

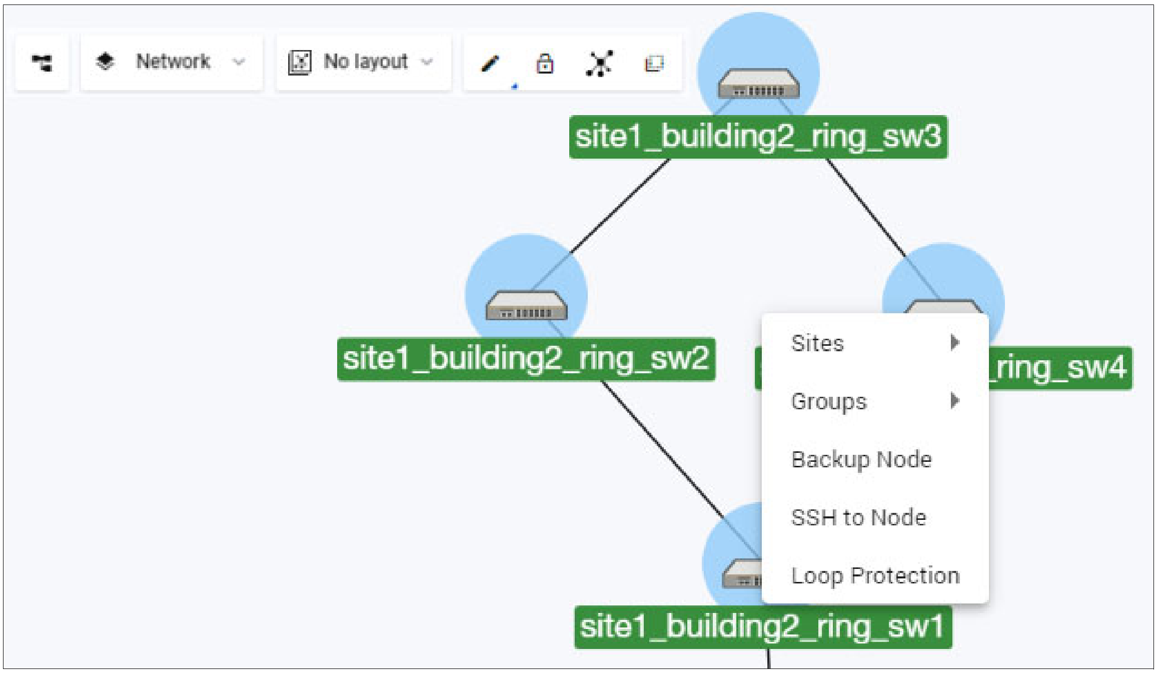
IP: 1.1.1.6

IPv6: 0000:0000:0000:0000:0000:0000:0000:0001

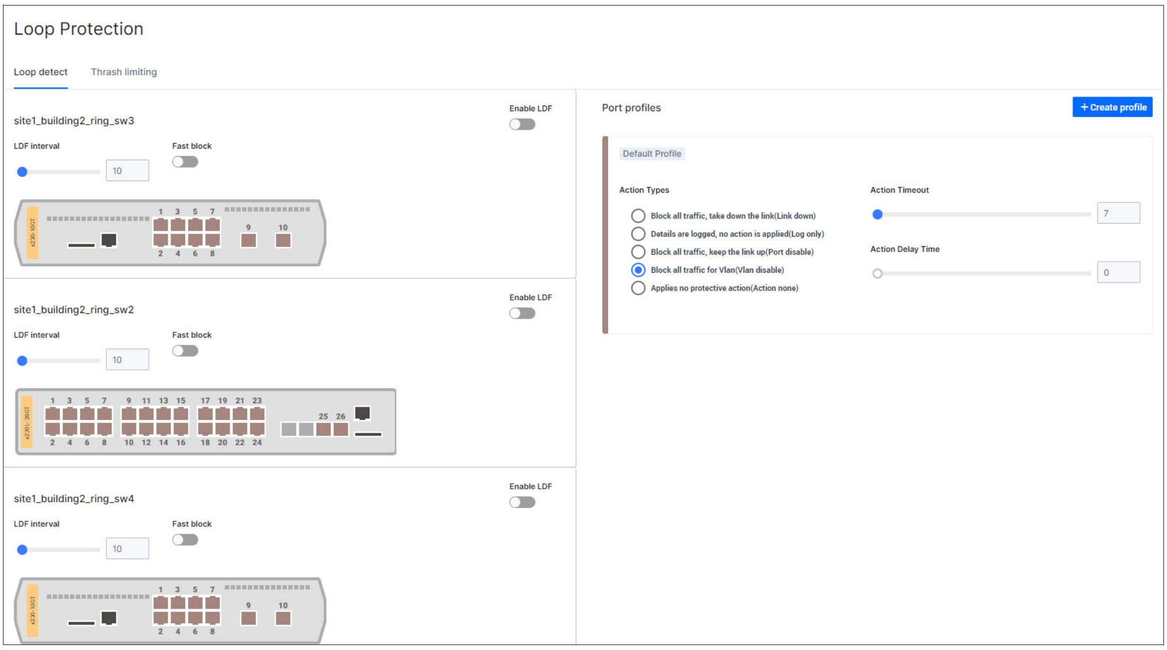
Hidden devices are specific to the layout. You can hide devices on a per-layout basis, and they will be hidden for any user using that layout.

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. This feature is supported when devices are running firmware version AlliedWare Plus v5.5.0-0.1 or later.



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.



Loop Protection

Loop detect | Thrash limiting

site1_building2_ring_sw3

Enable LDF ○

LDF interval 10

Fast block ○

site1_building2_ring_sw2

Enable LDF ○

LDF interval 10

Fast block ○

site1_building2_ring_sw4

Enable LDF ○

LDF interval 10

Fast block ○

Port profiles

+ Create profile

Default Profile

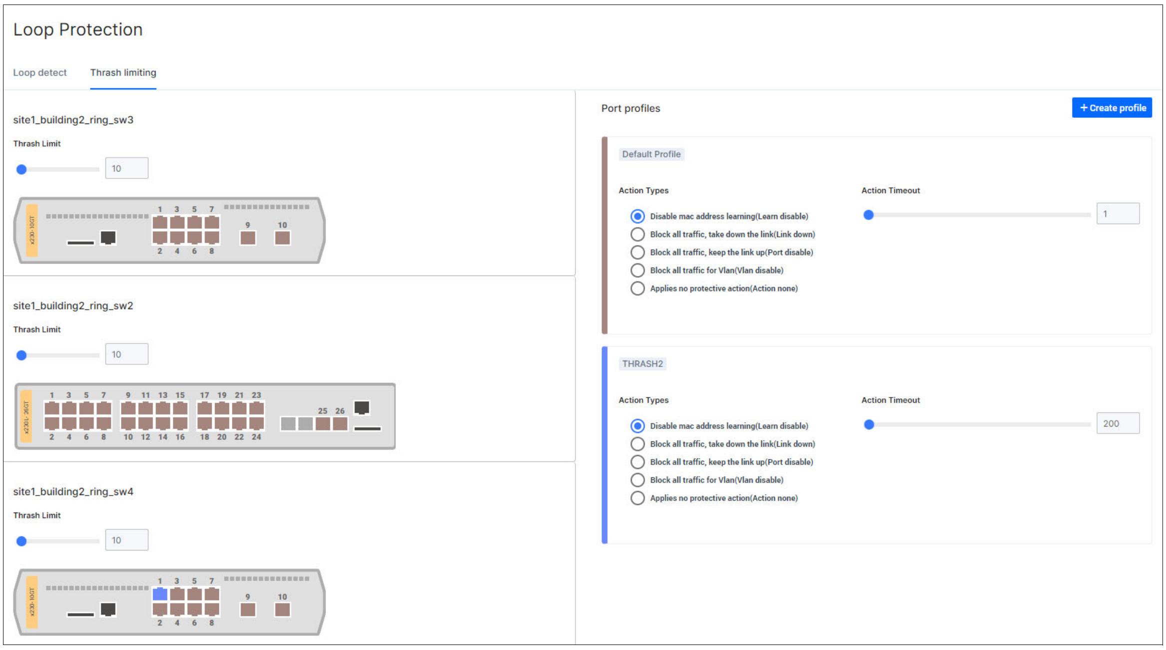
Action Types

- ○ Block all traffic, take down the link(Link down)
- ○ Details are logged, no action is applied(Log only)
- ○ Block all traffic, keep the link up(Port disable)
- ● Block all traffic for Vlan(Vlan disable)
- ○ Applies no protective action(Action none)

Action Timeout 7

Action Delay Time 0

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.



Loop Protection

site1_building2_ring_sw3

Thrash Limit: 10

site1_building2_ring_sw2

Thrash Limit: 10

site1_building2_ring_sw4

Thrash Limit: 10

Default Profile

Action Types

- ● Disable mac address learning(Learn disable)
- ○ Block all traffic, take down the link(Link down)
- ○ Block all traffic, keep the link up(Port disable)
- ○ Block all traffic for Vlan(Vlan disable)
- ○ Applies no protective action(Action none)

Action Timeout: 1

THRASH2

Action Types

- ● Disable mac address learning(Learn disable)
- ○ Block all traffic, take down the link(Link down)
- ○ Block all traffic, keep the link up(Port disable)
- ○ Block all traffic for Vlan(Vlan disable)
- ○ Applies no protective action(Action none)

Action Timeout: 200

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

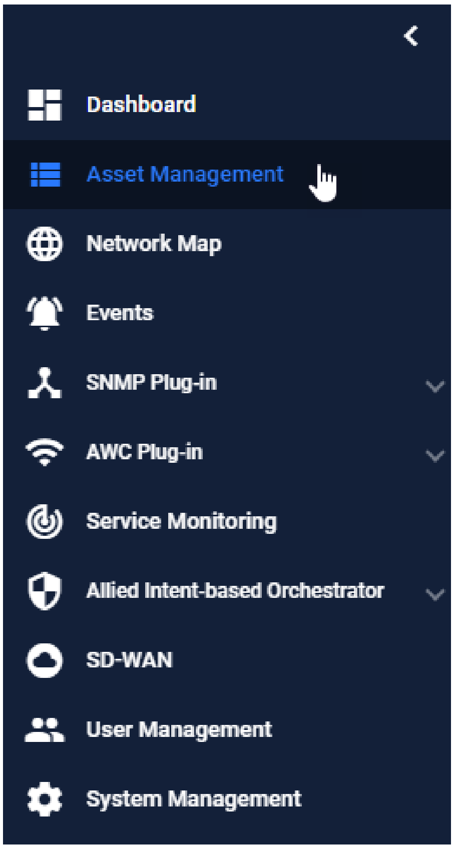
You can use the Asset Management screen to manage the assets in your network. It is made up of several components.

- **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.

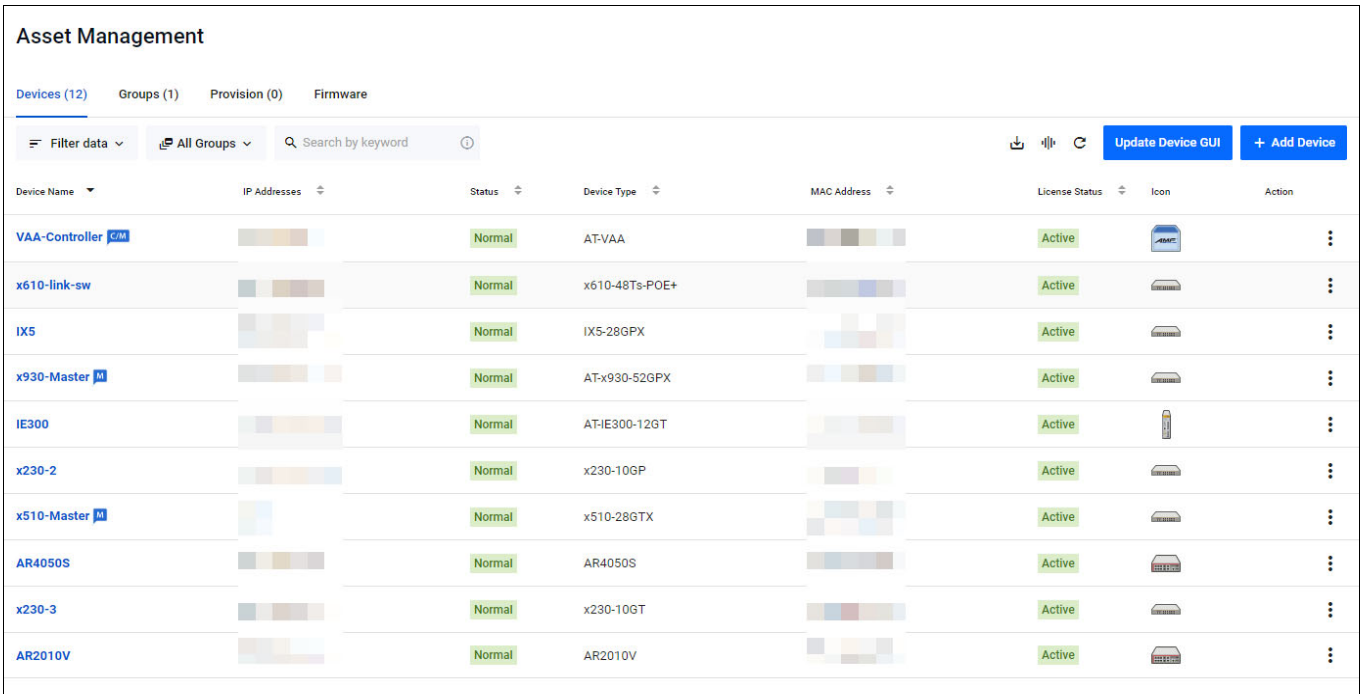
You can use Asset Management to:

- 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 is accessed from the sidebar menu.



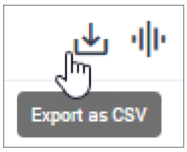
The Asset Management screen shows you the details of the items in your network. It also allows you to search for particular devices.



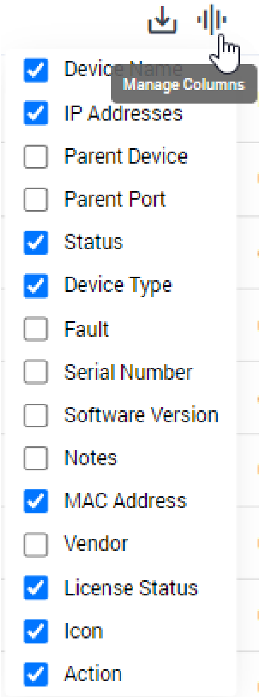
Asset Management

Device Name	IP Addresses	Status	Device Type	MAC Address	License Status	Icon	Action
VAA-Controller C/M	[redacted]	Normal	AT-VAA	[redacted]	Active		⋮
x610-link-sw	[redacted]	Normal	x610-48Ts-POE+	[redacted]	Active		⋮
IX5	[redacted]	Normal	IX5-28GPX	[redacted]	Active		⋮
x930-Master M	[redacted]	Normal	AT-x930-52GPX	[redacted]	Active		⋮
IE300	[redacted]	Normal	AT-IE300-12GT	[redacted]	Active		⋮
x230-2	[redacted]	Normal	x230-10GP	[redacted]	Active		⋮
x510-Master M	[redacted]	Normal	x510-28GTX	[redacted]	Active		⋮
AR4050S	[redacted]	Normal	AR4050S	[redacted]	Active		⋮
x230-3	[redacted]	Normal	x230-10GT	[redacted]	Active		⋮
AR2010V	[redacted]	Normal	AR2010V	[redacted]	Active		⋮

- Click on the **Export as CSV** icon at the top right corner to download a CSV file list of assests.



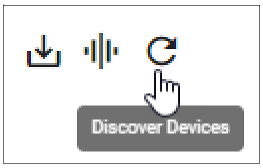
- Click on the **Manage Columns** icon to change the column display.



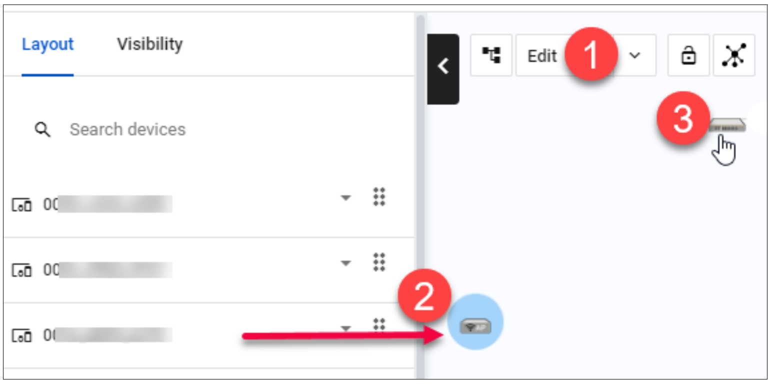
☑ Device Name
☑ IP Addresses
□ Parent Device
□ Parent Port
☑ Status
☑ Device Type
□ Fault
□ Serial Number
□ Software Version
□ Notes
☑ MAC Address
□ Vendor
☑ License Status
☑ Icon
☑ Action

- Click on the **Discover Devices** icon to discover devices from the Asset Management screen.

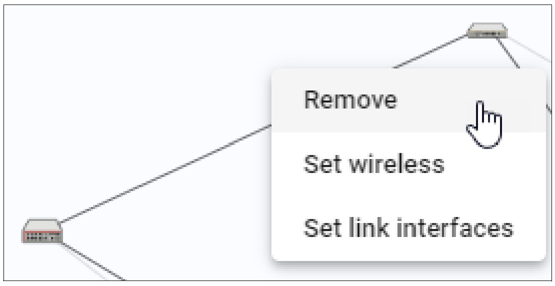
Vista Manager will use ARP to discover any new devices, and return a list to you. A message will appear indicating the number of new devices found.



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 devices or links between devices. (1) On Edit mode on the map, (2) select and drag a device from the side panel to the map. (3) Click on a second device, and a link will automatically be drawn between the devices.



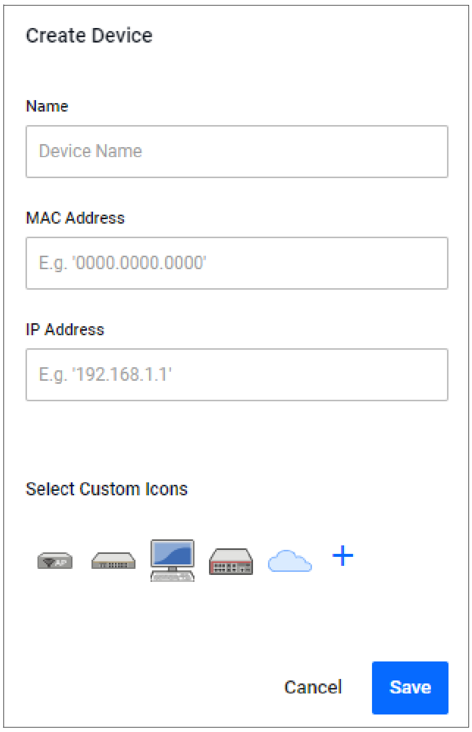
- To remove a link, right-click on the link and click **Remove**.



Detected devices that fall into a user defined inventory group will inherit the assigned custom icon.

- You can add a new device by clicking on the **+ Add Device** button.

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



Create Device

Name

Device Name

MAC Address

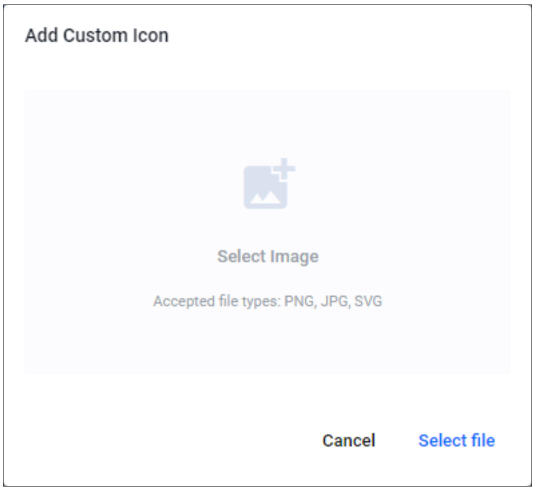
E.g. '0000.0000.0000'

IP Address

E.g. '192.168.1.1'

Select Custom Icons

- Click on the '**+**' button, to upload a custom icon for the device. The custom icon dialog supports PNG, JPG, and SVG image files. Only administrators have the permission to upload and change custom icons.



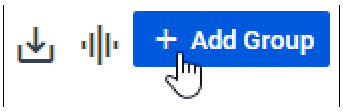
Add Custom Icon

Select Image

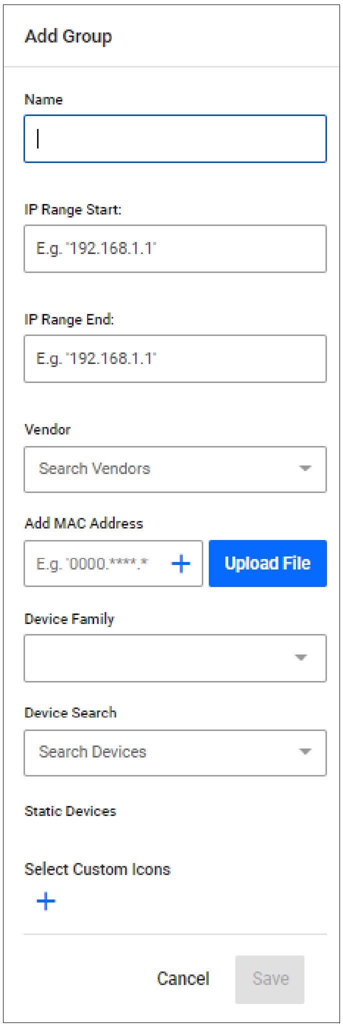
Accepted file types: PNG, JPG, SVG

Note: An AMF device cannot have its default icon changed.

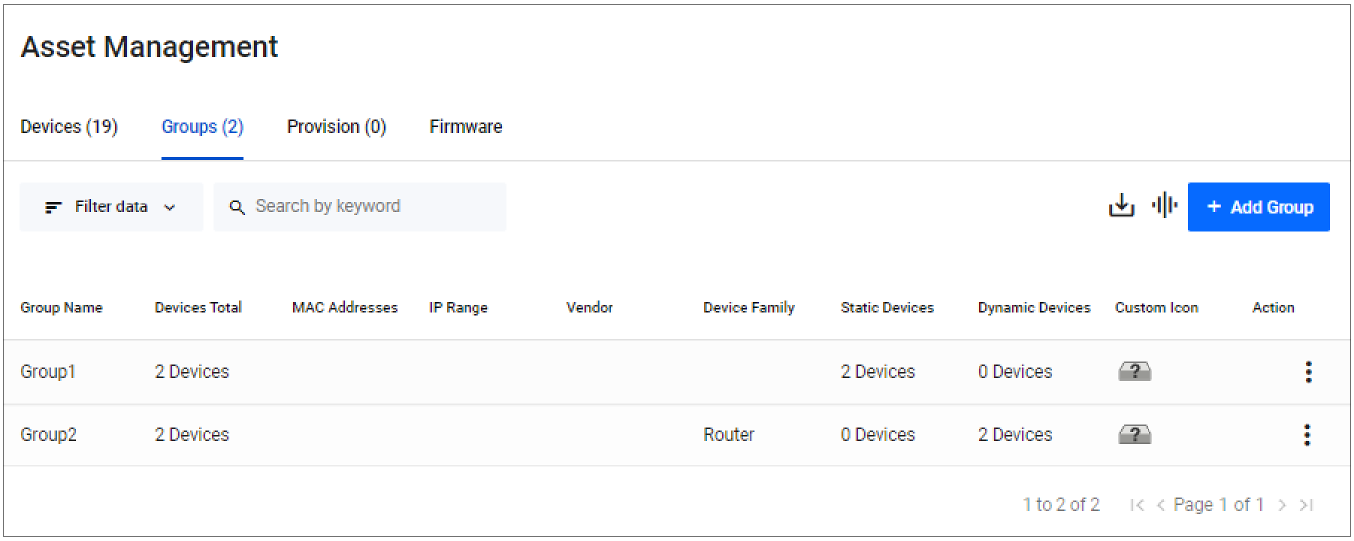
Asset Management also allows you to create groups to organize your inventory. To create a group, click on the Groups tab, and then click on the **+ Add Group** button.



You will be prompted to name the group. You can also specify which devices 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.

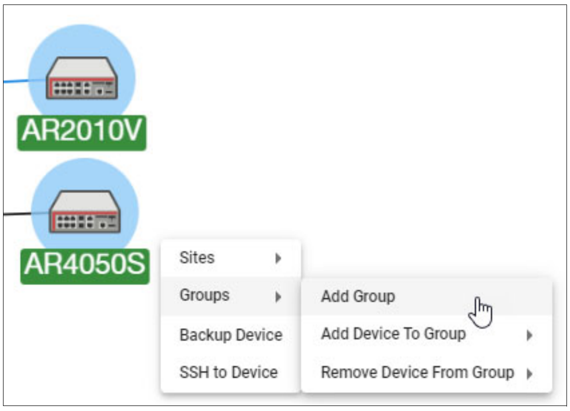


Group Name	Devices Total	MAC Addresses	IP Range	Vendor	Device Family	Static Devices	Dynamic Devices	Custom Icon	Action
Group1	2 Devices					2 Devices	0 Devices	?	⋮
Group2	2 Devices				Router	0 Devices	2 Devices	?	⋮

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 devices on the Network Map page. From the map itself, you may add/remove manually assigned devices 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:

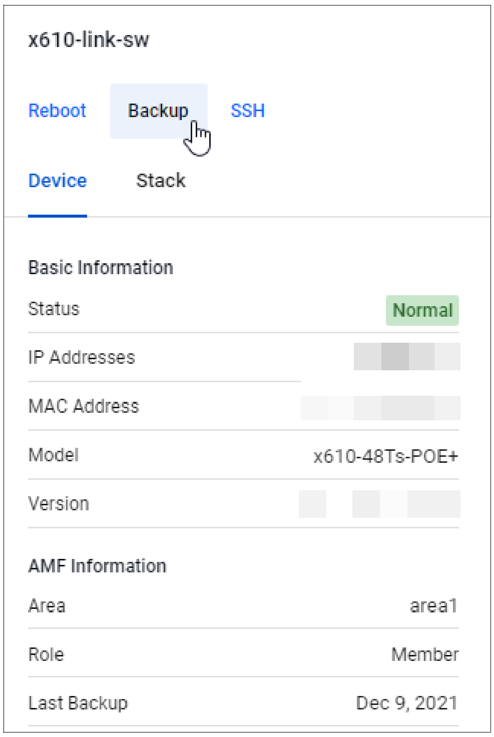
- Supported file formats are **.txt** and **.csv**.
- Commas, spaces, and new lines can be used to separate the MAC addresses.
- Supported MAC address formats are:
  - 000000000000
  - 0000.0000.0000
  - 0000:0000:0000
  - 0000-0000-0000
  - 00:00:00:00:00:00
  - 00-00-00-00-00-00
  - wildcard with asterisk (*)
- Any unrecognisable 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 devices, restore the network from back up, reboot devices, and manage devices by using SSH to access their command line.

Backup a device

Select the device that you want to back up:



x610-link-sw

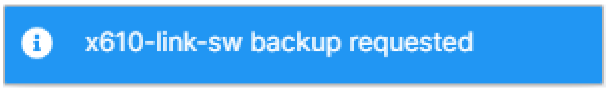
Basic Information

Status	Normal
IP Addresses	[redacted]
MAC Address	[redacted]
Model	x610-48Ts-POE+
Version	[redacted]

AMF Information

Area	area1
Role	Member
Last Backup	Dec 9, 2021

- Click on the **Backup** button.
- An information message is displayed showing that the backup has occurred:

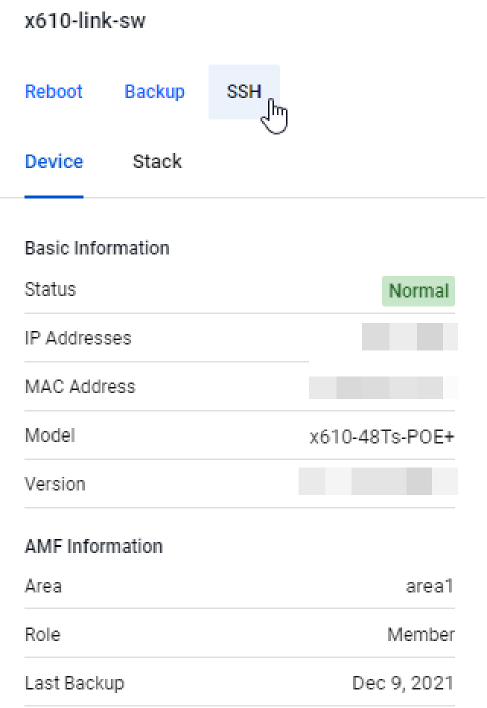


x610-link-sw backup requested

SSH/Shell to a device

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:



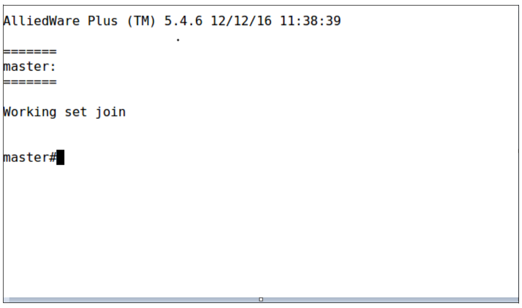
Basic Information

Status	Normal
IP Addresses	[redacted]
MAC Address	[redacted]
Model	x610-48Ts-POE+
Version	[redacted]

AMF Information

Area	area1
Role	Member
Last Backup	Dec 9, 2021

- Click the **SSH** button to start a CLI session.
- The following window is displayed:

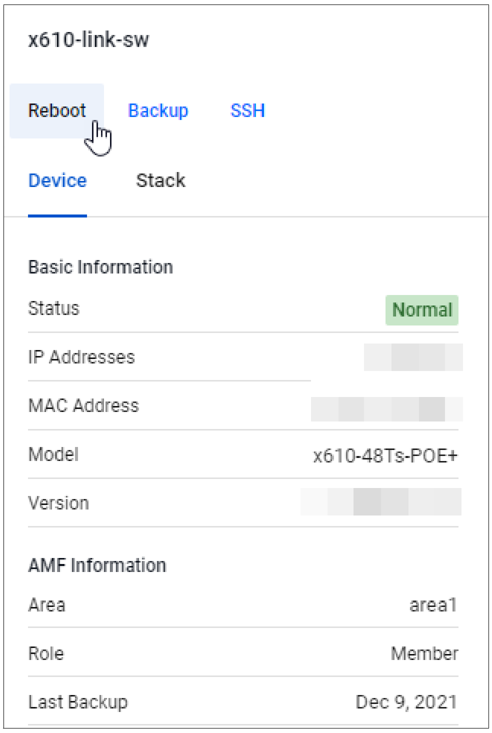


```
AlliedWare Plus (TM) 5.4.6 12/12/16 11:38:39

=======
master:
=======

Working set join


master#█
```

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

Reboot a device

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



x610-link-sw

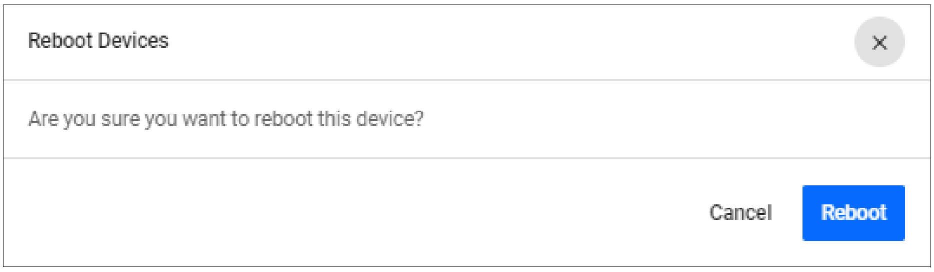
Basic Information

Status	Normal
IP Addresses	[redacted]
MAC Address	[redacted]
Model	x610-48Ts-POE+
Version	[redacted]

AMF Information

Area	area1
Role	Member
Last Backup	Dec 9, 2021

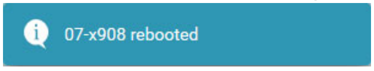
- Click the **Reboot** button.



Reboot Devices

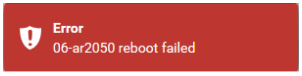
Are you sure you want to reboot this device?

- 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:



07-x908 rebooted

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



Error
06-ar2050 reboot failed

Intelligent device grouping

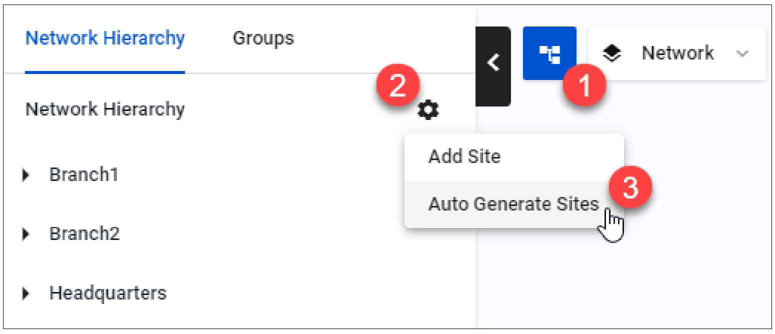
By selecting a Network Hierarchy preference, you can organize your network easily. When a new device is added into the network, it can be automatically assigned to a site based on its hostname. Intelligent device grouping comes with a range of functionalities:

- 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

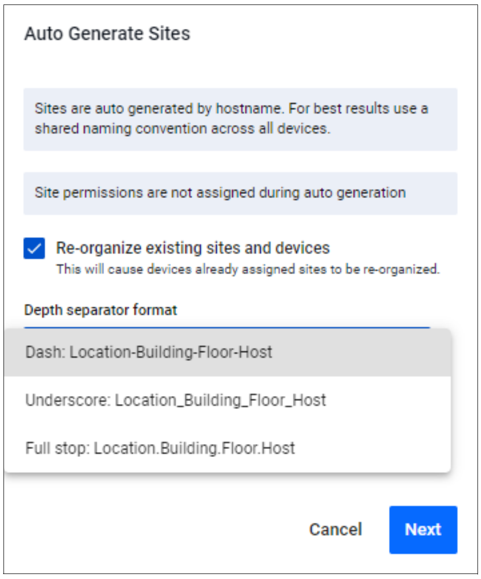
Note: Removing a site only stops the automatic assignment, it does not remove the site from Vista Manager EX.

To use this feature, navigate to the **Network Map** page.

1. Click on the **Network Hierarchy** icon at the top left of the map screen to display the side panel list of sites.
2. Click on the cogwheel.
3. 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.



Auto Generate Sites

Sites are auto generated by hostname. For best results use a shared naming convention across all devices.

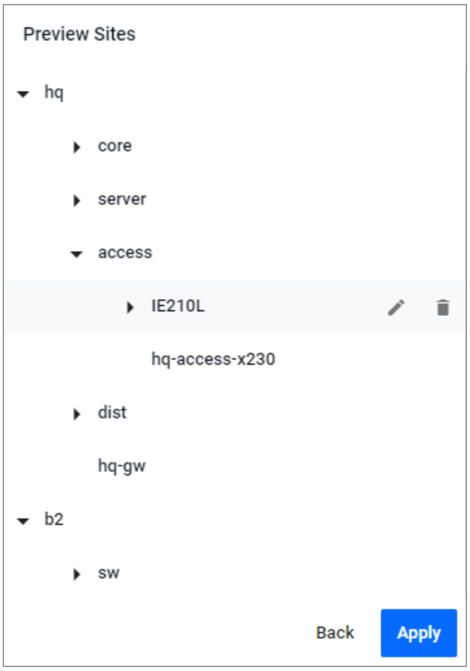
Site permissions are not assigned during auto generation

☑ Re-organize existing sites and devices
This will cause devices already assigned sites to be re-organized.

Depth separator format

Dash: Location-Building-Floor-Host
Underscore: Location_Building_Floor_Host
Full stop: Location.Building.Floor.Host
Cancel
Next

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



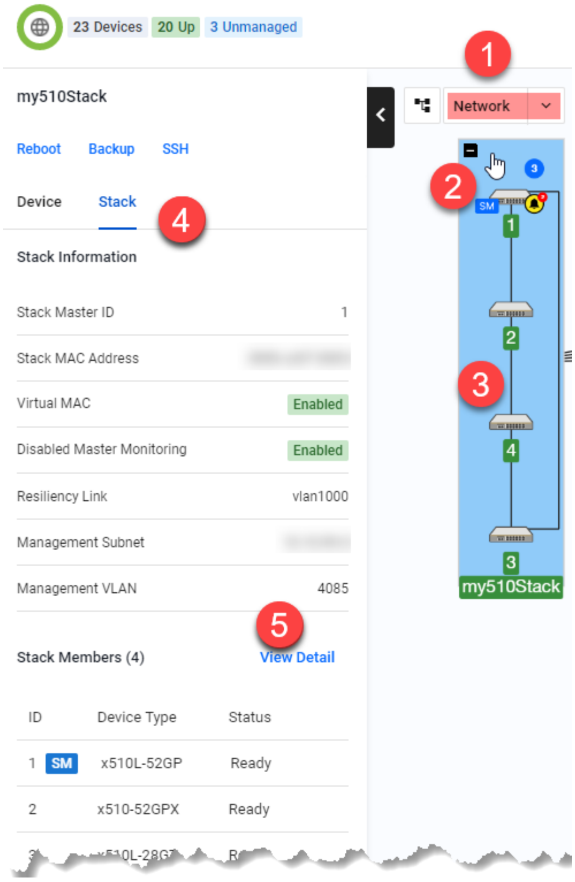
All devices will be automatically grouped into an appropriate Network Hierarchy group. You can manually collapse other devices on the integrated map, which allows you to focus only on the high-level networks.

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 devices 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.

Enhanced information display for stacked devices

You can use the **View Detail** link to monitor the state of stacked devices in your network.



my510Stack

Stack Information

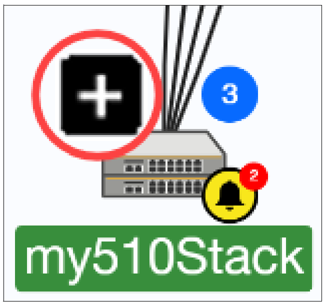
Stack Master ID	1
Stack MAC Address	[redacted]
Virtual MAC	Enabled
Disabled Master Monitoring	Enabled
Resiliency Link	vlan1000
Management Subnet	[redacted]
Management VLAN	4085

Stack Members (4) View Detail

ID	Device Type	Status
1 SM	x510L-52GP	Ready
2	x510-52GPX	Ready
3	x510L-28GT	R

1. Navigate to the **network layer** of the integrated map.

2. Hover over a stack to see the ‘+’ symbol. Click on ‘+’ to expand it. This lets you view all stack members and associated stacking links. If a stack is fully-formed, you will also see an outer link completing the stacking loop.



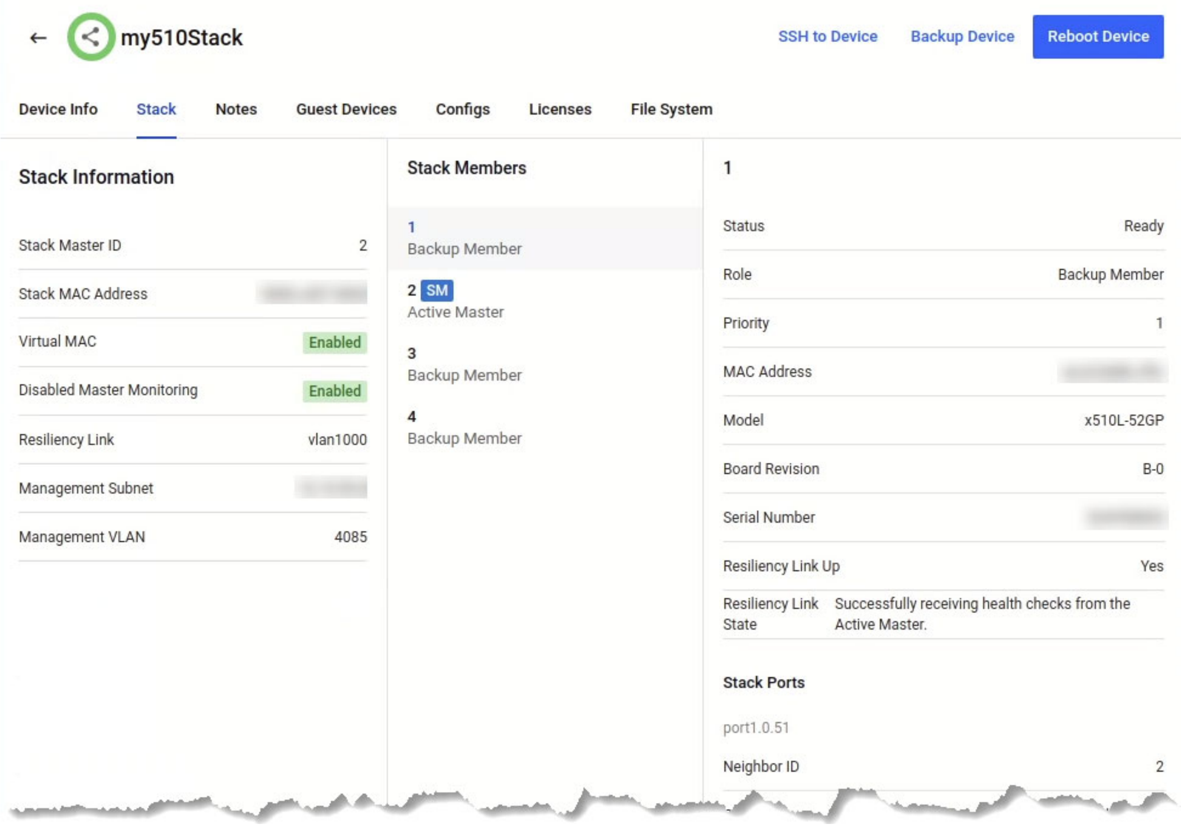
3. Click on the stack in the map (blue highlighted area) to see its information.

4. The side panel pops out. The Stack tab will display some basic stack-wide information such as:

   - a list of stack members
   - current status of each stack member
   - which stack member is the master

5. Click **View Detail** to see detailed information about the stack. This opens up the device details page showing:

   - **Stack Information:** Stack Master ID, stack MAC Address, virtual MAC, disabled master monitoring, resiliency link, management subnet, management VLAN
   - **Stack Members:** Stack ID, status, role, priority, MAC address, product type, revision, serial number, resiliency links, state, stack ports



Stack Information

Stack Master ID	2
Stack MAC Address	[redacted]
Virtual MAC	Enabled
Disabled Master Monitoring	Enabled
Resiliency Link	vlan1000
Management Subnet	[redacted]
Management VLAN	4085

Stack Members

1
Backup Member

2 SM
Active Master

3
Backup Member

4
Backup Member

1

Status	Ready
Role	Backup Member
Priority	1
MAC Address	[redacted]
Model	x510L-52GP
Board Revision	B-0
Serial Number	[redacted]
Resiliency Link Up	Yes
Resiliency Link State	Successfully receiving health checks from the Active Master.

Stack Ports

port1.0.51

Neighbor ID	2

When a stack is expanded:

- All stack members and associated stacking links will be displayed.
- Click on each link to see which device type and interface is on each end of the link.
- The stack master has an ‘SM’ badge indicating that it is the stack master.
- When a stack master leaves the stack, the stack master badge will update to show next to the new stack master.
- Each stack member will have an icon showing its stack member ID.
- If a stack member goes down, its position will move to the bottom of the stack to indicate its current down status.
- An event bell icon indicating any network events will still be displayed on the stack master.
- The stack remains expanded when you leave and navigate back to the map later.

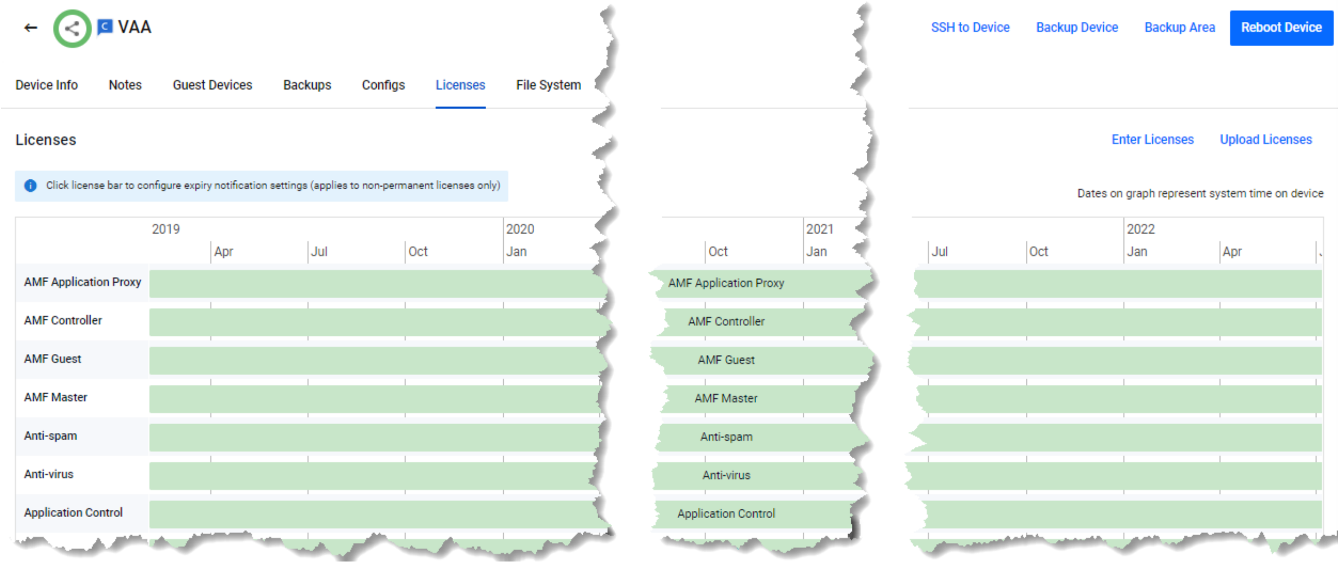
There are some limitations to this feature:

- If a stack member goes down, the hostname/member ID will stay green and not change to red.
- Individual stack members cannot be moved.

This feature requires AlliedWare Plus version 5.4.7-2.1 or later.

AMF device licenses

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



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

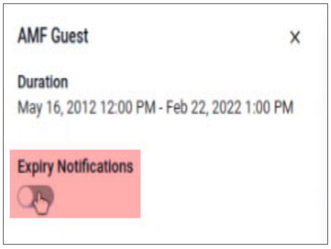
Dates on graph represent system time on device

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

Click on a license bar to display a pop-up panel with additional information about that license.

Disable license expiry notifications

By default, all license expiry notifications are set to enabled. As an administrator, you will have the option to disable them.



AMF Guest ×

Duration
May 16, 2012 12:00 PM - Feb 22, 2022 1:00 PM

Expiry Notifications

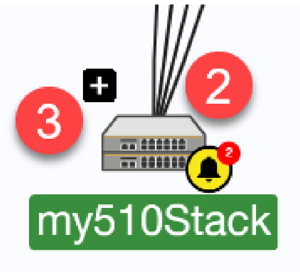
Click on a license bar that you wish to disable notifications for. A side panel will appear. Turn off the **Expiry Notifications** settings. A success message will pop up at the bottom of the side panel. A crossed-out bell now appears on the license bar.

Note: This feature applies to non-permanent licenses only.

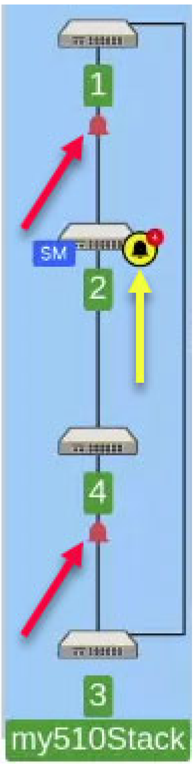
Active Fiber Monitoring (AFM) display

With enhanced information display possible for stacked devices, support has been added to display Active Fiber Monitoring (AFM). You will be able to see links between members and fiber tamper alarms (red bell icons) when a link has been tampered with. As an administrator, you can use this information to check on the physical links, dismiss the fiber tamper alarms and/or change AFM settings on specific links.

1. Navigate to the **network layer** of the integrated map.
2. Identify a stack with an event bell icon. This means there has been an event on the stack, for example, tampered links.

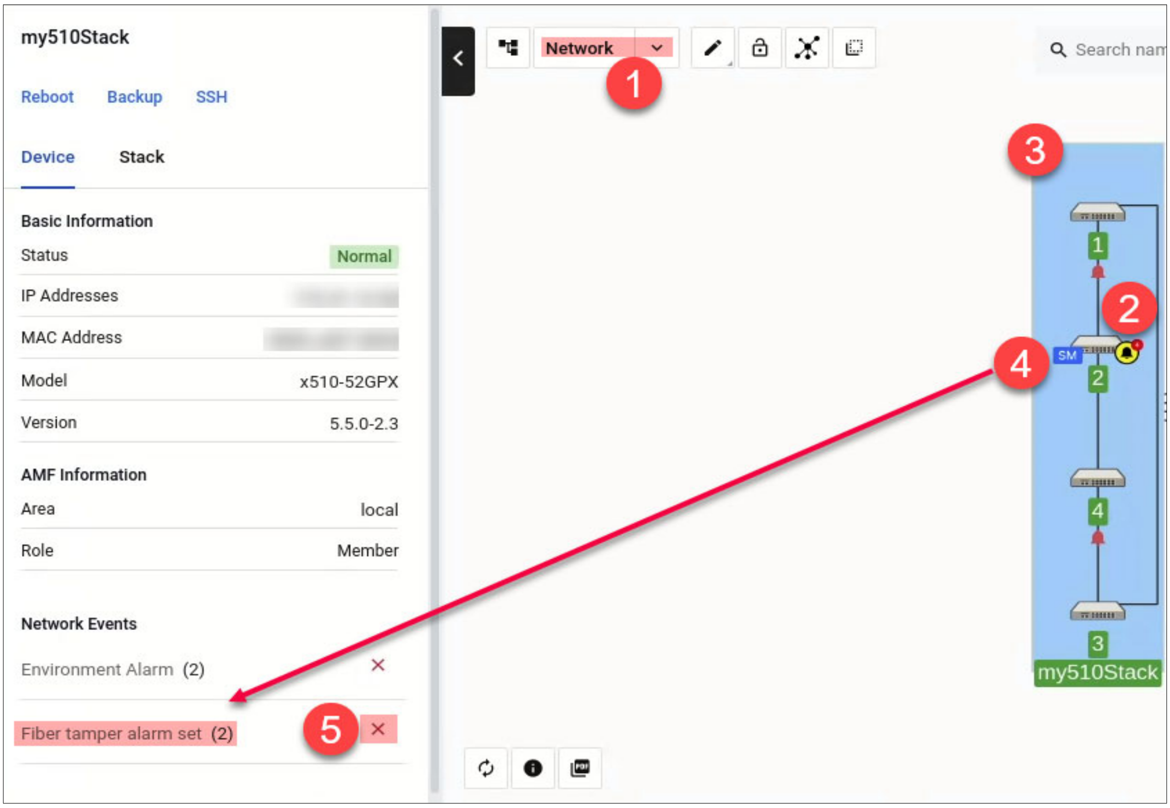


3. Hover over a stack to see the '+' symbol. Click on '+' to expand it. You will see the stack master showing the yellow and black event bell icon, and fiber tamper alarms on stacking links (red bell icons) that have been tampered with.



4. Click on the stack (blue highlighted area) to enable the side panel. Fiber tamper alarms are shown at the bottom of the side panel, under Network Events.

Note: Fiber tamper alarms will remain until you have dismissed them. This removes the red bell icon and reduces the event bell count on the device stack.



my510Stack

Reboot Backup SSH

Device Stack

Basic Information

Status	Normal
IP Addresses	[redacted]
MAC Address	[redacted]
Model	x510-52GPX
Version	5.5.0-2.3

AMF Information

Area	local
Role	Member

Network Events

Environment Alarm (2) ×

Fiber tamper alarm set (2) ×

5. You can dismiss a fiber tamper alarm in 3 ways:

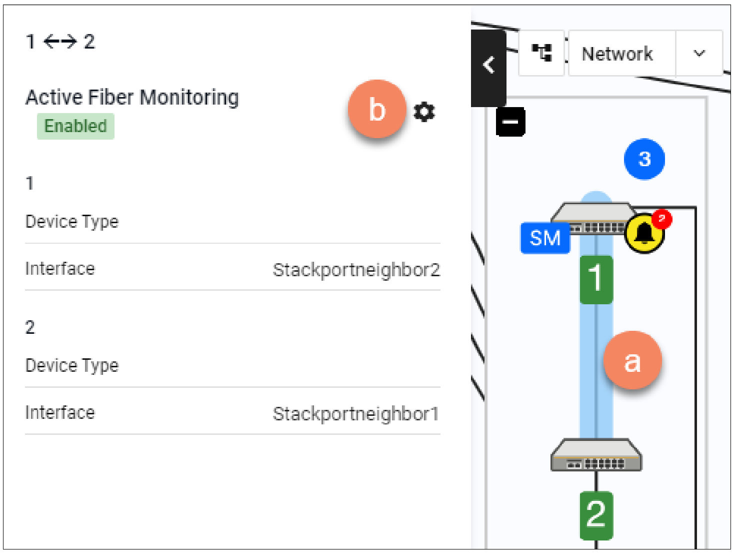
   - Click on the stack, like in Step 4. Dismiss the **Fiber tamper alarm set** event under **Network Events** on the side panel.
   - Click on the red bell icon. Dismiss the **Fiber tamper alarm set** event under **Network Events** on the side panel.
   - Dismiss either the stack event or stack member event in the **Event Log**.

6. To change settings for AFM:

   a. With the stack still expanded, click on a link inside the stack that you wish to disable AFM for. This highlights the link.

   b. On the side panel, click on the AFM settings icon to disable AFM.

   c. Disable AFM.



1 ←→ 2

Active Fiber Monitoring

Enabled

1

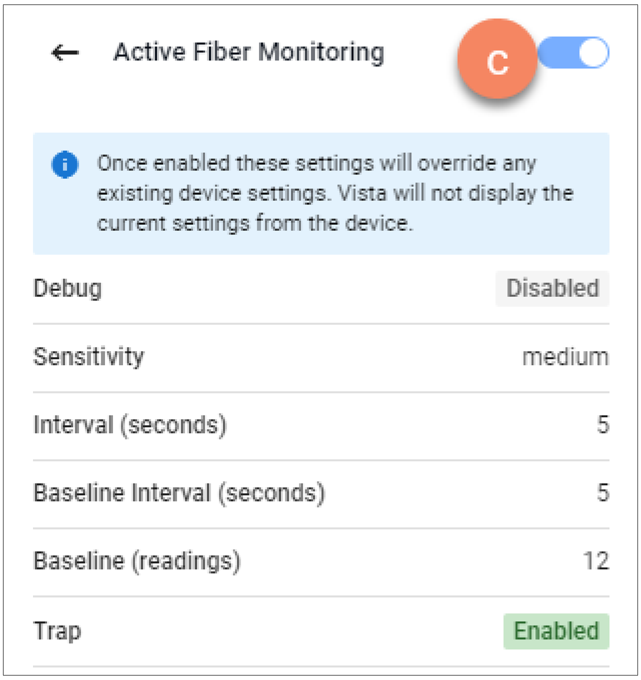
Device Type

Interface Stackportneighbor2

2

Device Type

Interface Stackportneighbor1



← Active Fiber Monitoring

Once enabled these settings will override any existing device settings. Vista will not display the current settings from the device.

Debug	Disabled
Sensitivity	medium
Interval (seconds)	5
Baseline Interval (seconds)	5
Baseline (readings)	12
Trap	Enabled

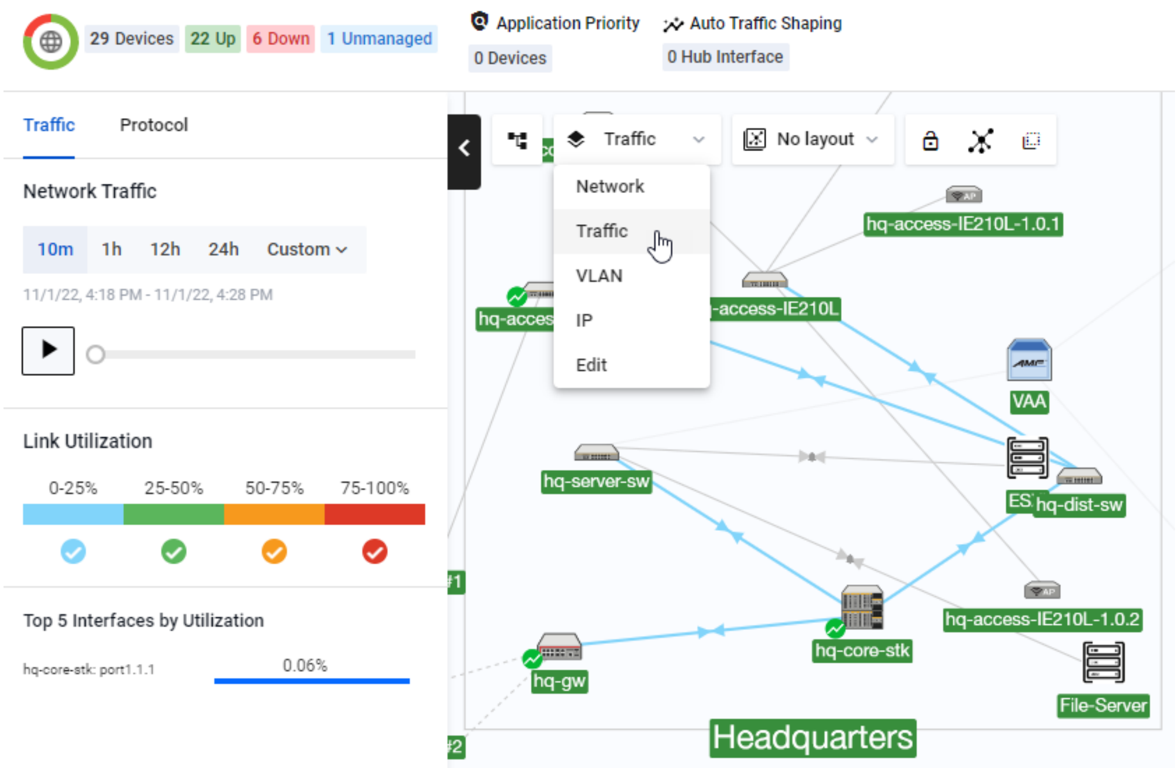
Note: Only links inside a Virtual Chassis Stack are supported for viewing and editing AFM settings in Vista Manager EX.

Note: If AFM has already been enabled from the CLI, the AFM settings icon will not be visible on the side panel of Vista Manager EX.

- This feature requires AlliedWare Plus version 5.5.0-0.3 or later.
- Detecting tampered link events requires AlliedWare Plus version 5.4.8-1 or later.

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.

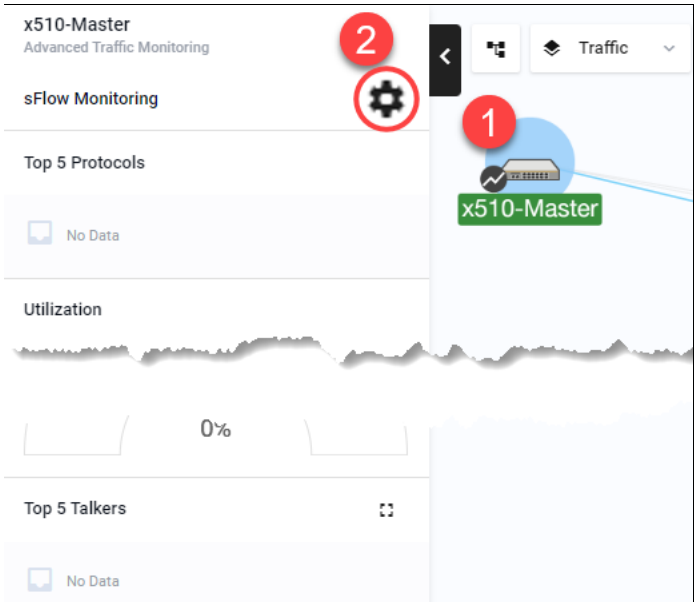
For additional information and to see how to use the traffic monitoring functionality, refer to the Traffic Monitoring video on the Allied Telesis website.

Advanced traffic monitoring with sFlow

You can monitor network traffic using Vista Manager's sample Flow (sFlow) feature. After configuring sFlow on your network devices, use can use advanced traffic monitoring to view information about network traffic, protocols, and applications.

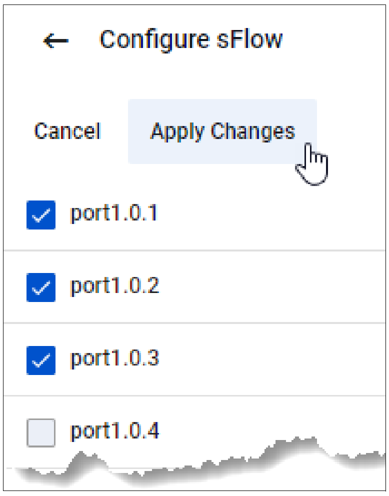
Advanced traffic monitoring can be accessed from the network map menu. Click on the dropdown, then select Traffic. This opens the Traffic sidebar. Advanced Traffic Monitoring will appear at the bottom of the sidebar. When you first open it, there will be no data, since you will not have configured any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

(1) Select a device from your network map, and (2) click on the settings cogwheel to configure it.



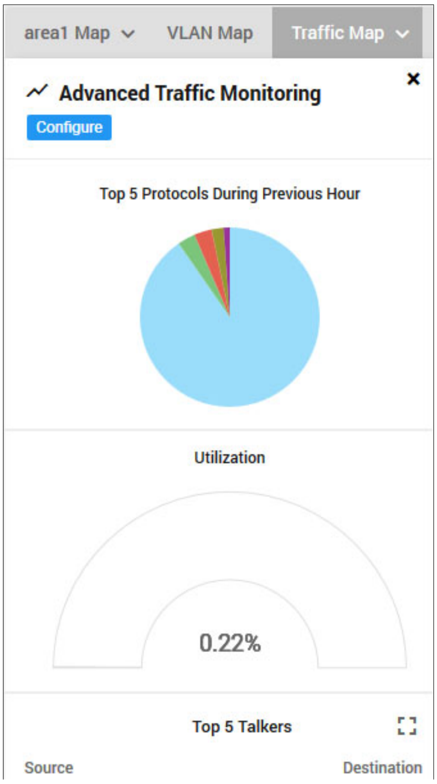
The side panel will show a list of the ports on the device. Tick on a port to enable or disable sFlow on the port.

Click **Apply Changes** to save.



☑ port1.0.1
☑ port1.0.2
☑ port1.0.3
□ port1.0.4

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



Advanced Traffic Monitoring

Top 5 Protocols During Previous Hour

Utilization

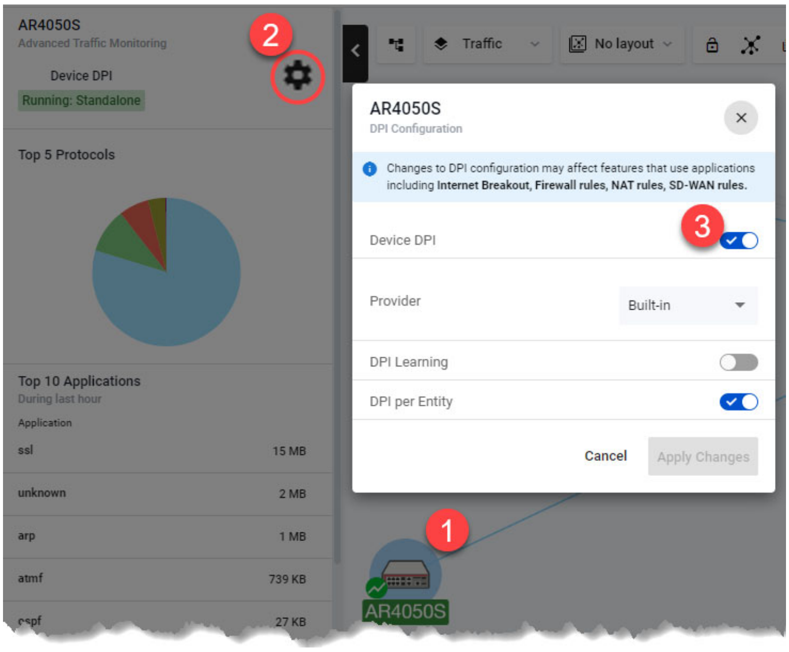
0.22%

Top 5 Talkers

Source	Destination

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

(1) Select a device from your network map, and (2) click on the cogwheel to configure it. (3) Click Device DPI to enable it.



AR4050S
Advanced Traffic Monitoring

Device DPI
Running: Standalone

Top 5 Protocols

Top 10 Applications
During last hour

Application	
ssl	15 MB
unknown	2 MB
arp	1 MB
atmf	739 KB
ospf	27 KB

AR4050S
DPI Configuration

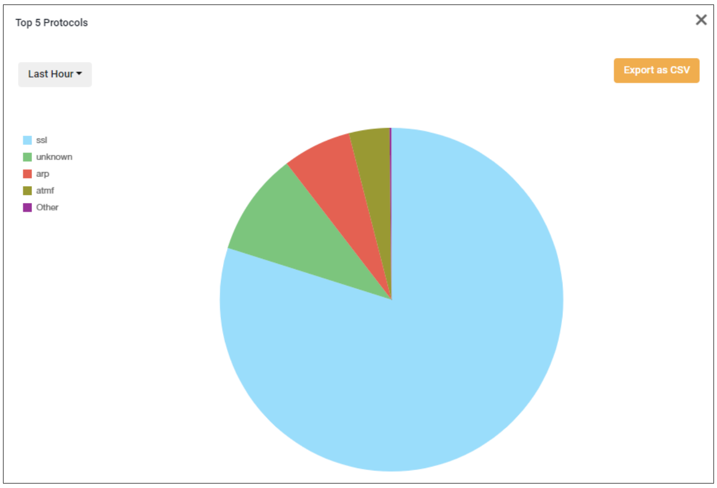
Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.**

Device DPI	✓
Provider	Built-in
DPI Learning	○
DPI per Entity	✓

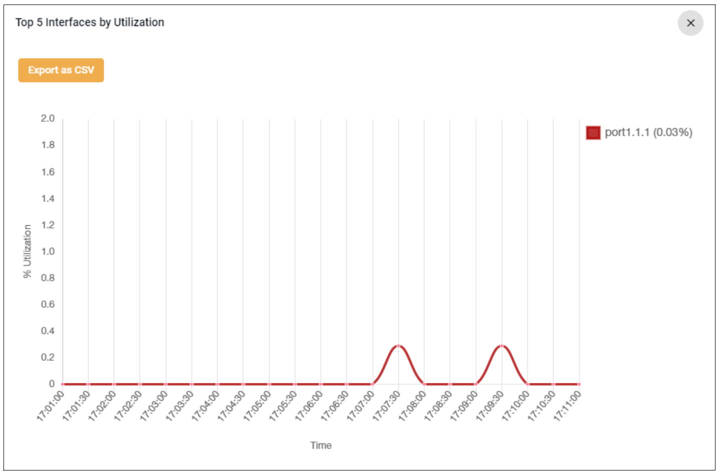
Cancel Apply Changes

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.

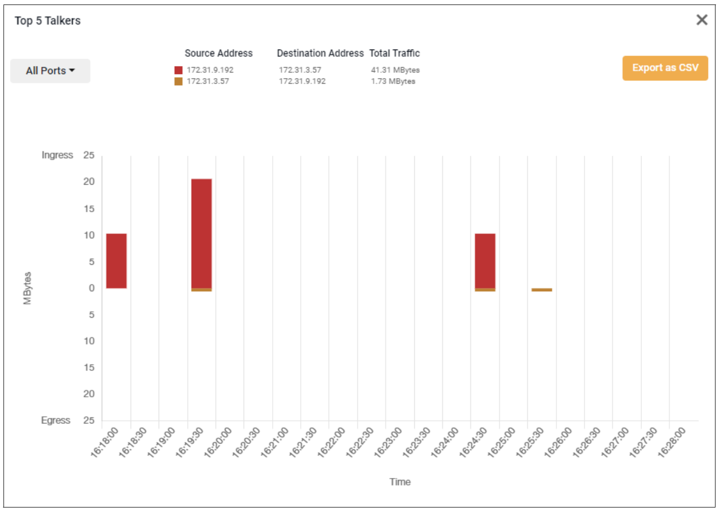
Top 5 Protocols:



Top 5 Interfaces by Utilization:



Top 5 Talkers:



	Source Address	Destination Address	Total Traffic
🟥	172.31.9.192	172.31.3.57	41.31 MBytes
🟧	172.31.3.57	172.31.9.192	1.73 MBytes

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

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.

AlliedWare Plus configuration can support multiple collectors. However, only the first collector will allow Vista Manager sFlow to connect to the device correctly. If there are multiple collectors, please ensure that the first collector is the IP address of Vista Manager. For example, the following sFlow configuration is correct if Vista Manager is using the IP of 10.33.25.48:

```
sflow agent ip 172.31.1.102
sflow collector id 1 ip 10.33.25.48
sflow collector id 2 ip 10.36.150.103
sflow collector id 3 ip 10.33.25.92
sflow enable
```

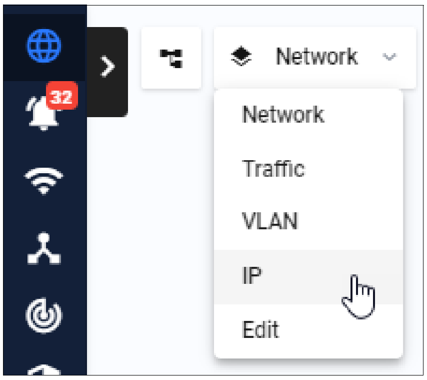
IP map layer: Tracepath and Walk path

From the IP map layer, you can access both the Tracepath and Walk path features.

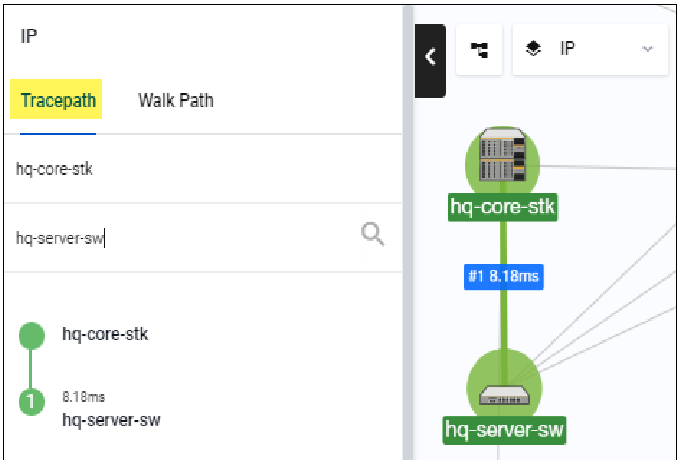
Tracepath allows you to determine where traffic is flowing. You can click on two devices in the Vista Manager network map, the source and destination. Vista Manager will display the path between them and show RTT (round trip time) information.

Walk path lets you determine if there are any configured routing paths from one device to a destination IP within the network known to Vista Manager. This is usually performed for installation or diagnostic purposes.

To first access the IP map layer, open the network map in Vista Manager. Click on the dropdown and select **IP**.



To use Tracepath or Walk path, navigate to the relevant tabs on the side panel.

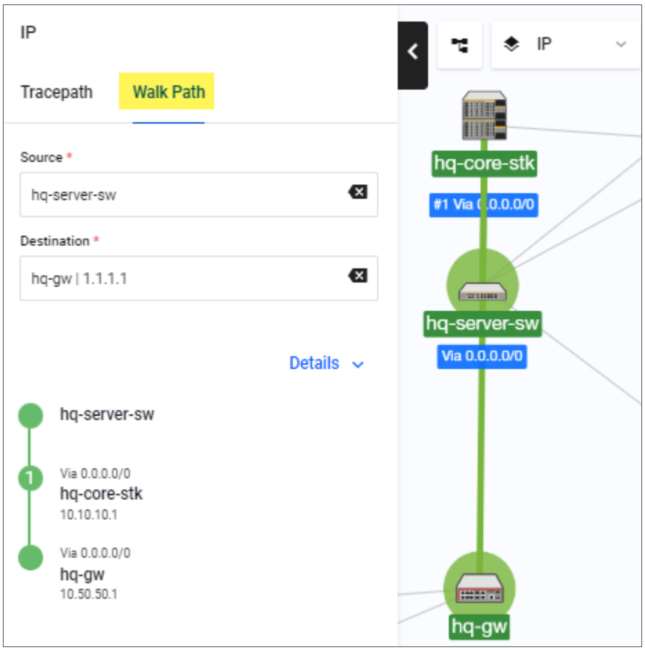


hq-core-stk

hq-server-sw

hq-core-stk

1 8.18ms
hq-server-sw



Source *

hq-server-sw

Destination *

hq-gw | 1.1.1.1

hq-server-sw

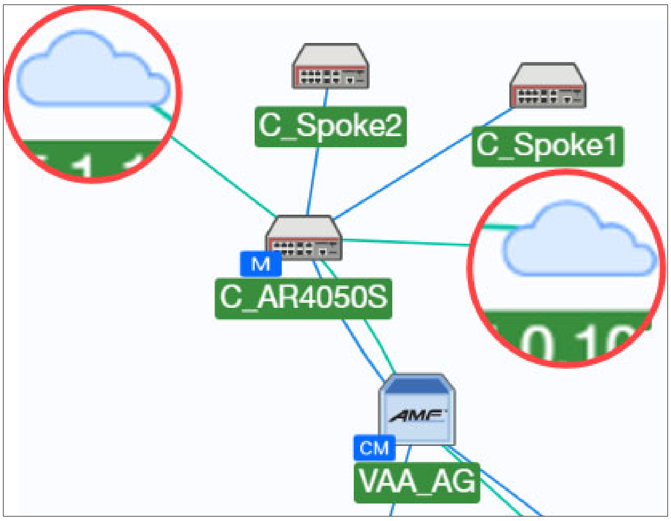
1 Via 0.0.0.0/0
hq-core-stk
10.10.10.1

Via 0.0.0.0/0
hq-gw
10.50.50.1

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

Detecting non-AMF devices: Improved WAN visibility

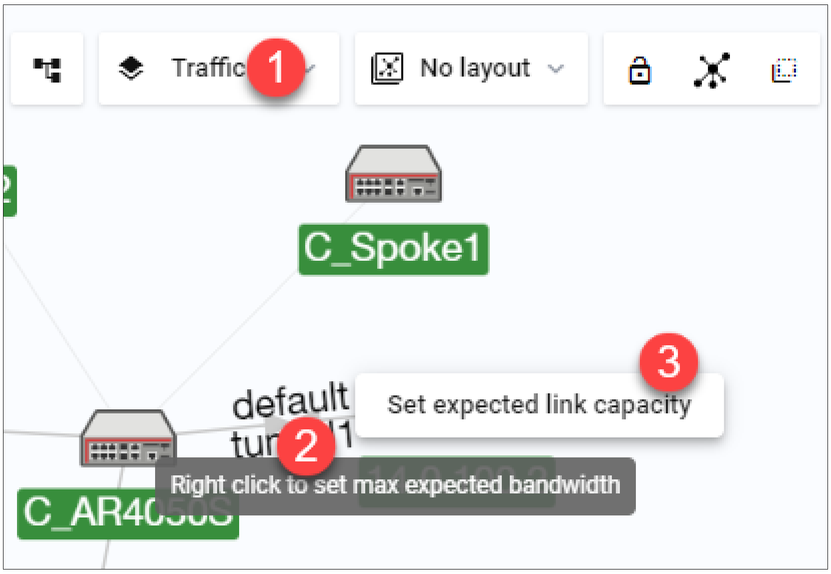
The integrated map can detect non-AMF devices that have an AlliedWare Plus device connected to them by a tunnel. The non-AMF device is represented as a cloud icon. The hostname is the IP address of the tunnel destination.



After manually adding non-AMF devices, you can also monitor link utilization and see related information using the following steps:

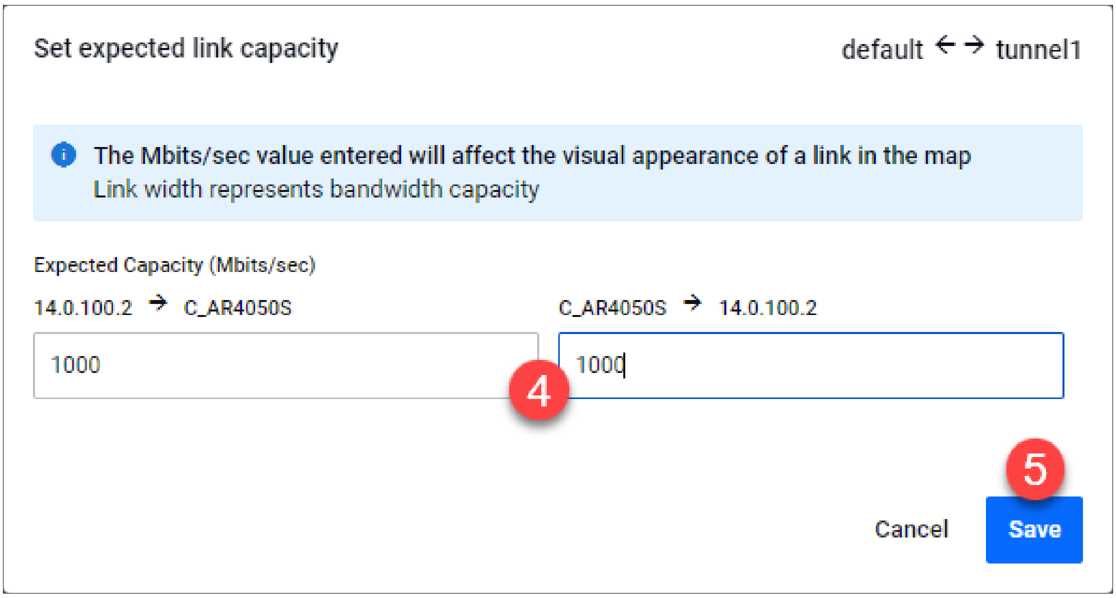
1. Navigate to the **Traffic map** mode.
2. Right-click on a tunnel link you want to monitor.
3. Set the expected link capacity.
4. Enter the maximum bandwidth in Mbits/sec.
5. Click on the **Save** button.
6. Click on the tunnel link to view its link utilization information.
7. The side panel pops out showing the link utilization and its related information.

See the following screenshot for details.



Set expected link capacity

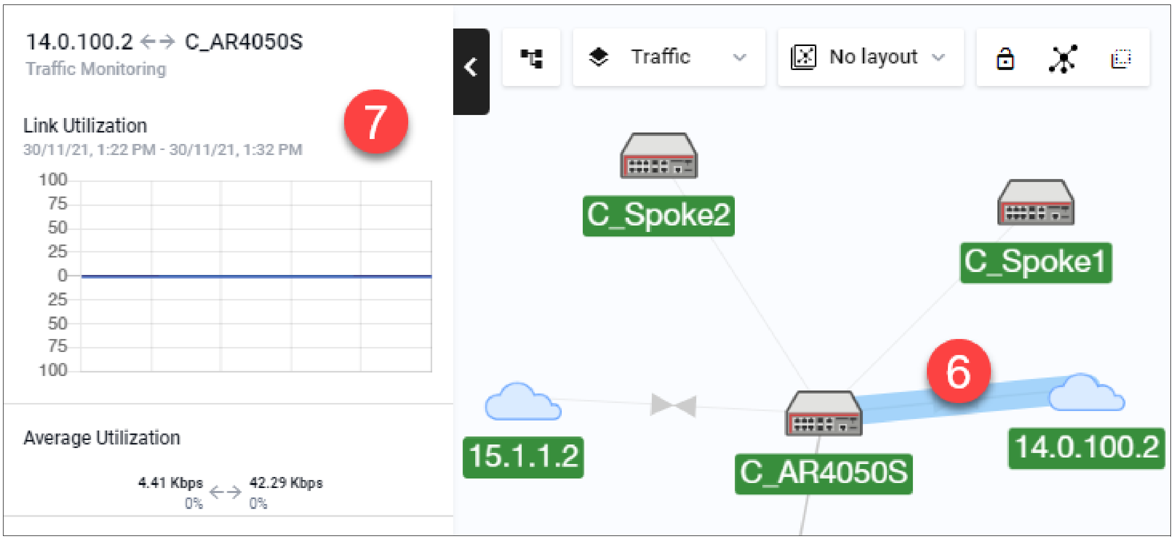
Right click to set max expected bandwidth


Set expected link capacity default ← → tunnel1

ⓘ The Mbits/sec value entered will affect the visual appearance of a link in the map
Link width represents bandwidth capacity

Expected Capacity (Mbits/sec)

14.0.100.2 → C_AR4050S	C_AR4050S → 14.0.100.2
1000	1000


14.0.100.2 ← → C_AR4050S
Traffic Monitoring

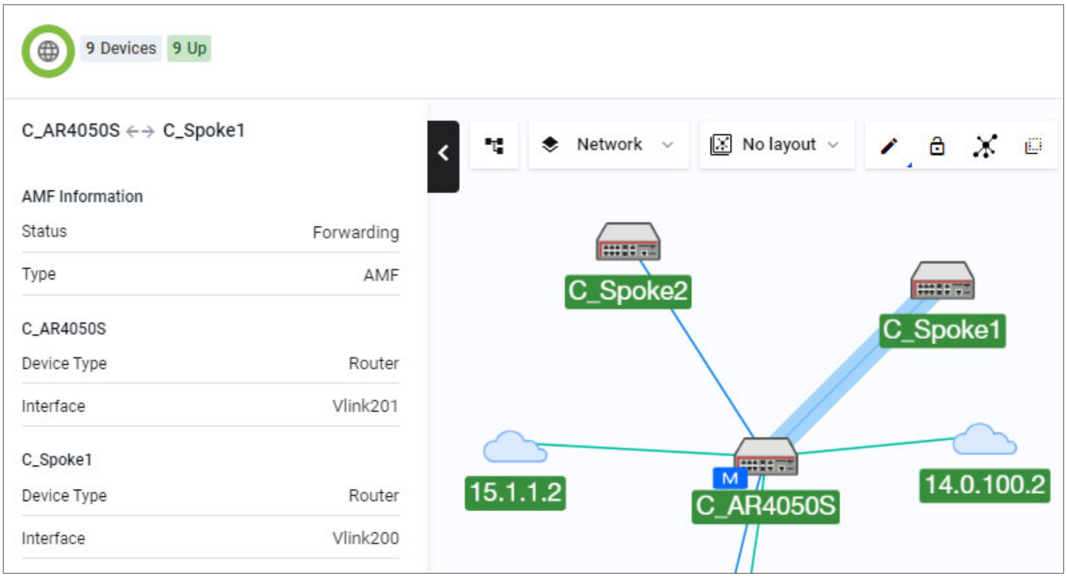
Link Utilization
30/11/21, 1:22 PM - 30/11/21, 1:32 PM

Average Utilization

4.41 Kbps 0% ← → 42.29 Kbps 0%

There are multiple functionalities to this feature:

- automatically detect supported tunnels between an AlliedWare Plus device and a remote device that is not part of the network
- automatically create custom devices represented by cloud icons on the remote end of the tunnel and add them to the map
- automatically update map if there are any changes to an existing tunnel or when a new tunnel is configured
- detect IPv4 PPPoE configuration and display these links and devices on the map similar to the tunnels
- display read-only information about the tunnel on the map side panel



C_AR4050S <-> C_Spoke1

AMF Information

Status	Forwarding
Type	AMF

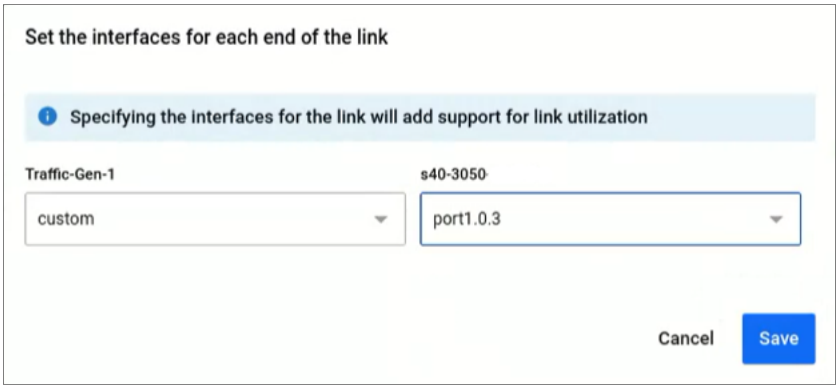
C_AR4050S

Device Type	Router
Interface	Vlink201

C_Spoke1

Device Type	Router
Interface	Vlink200

- configure interfaces and bandwidth on a custom link so that the link utilization data is available



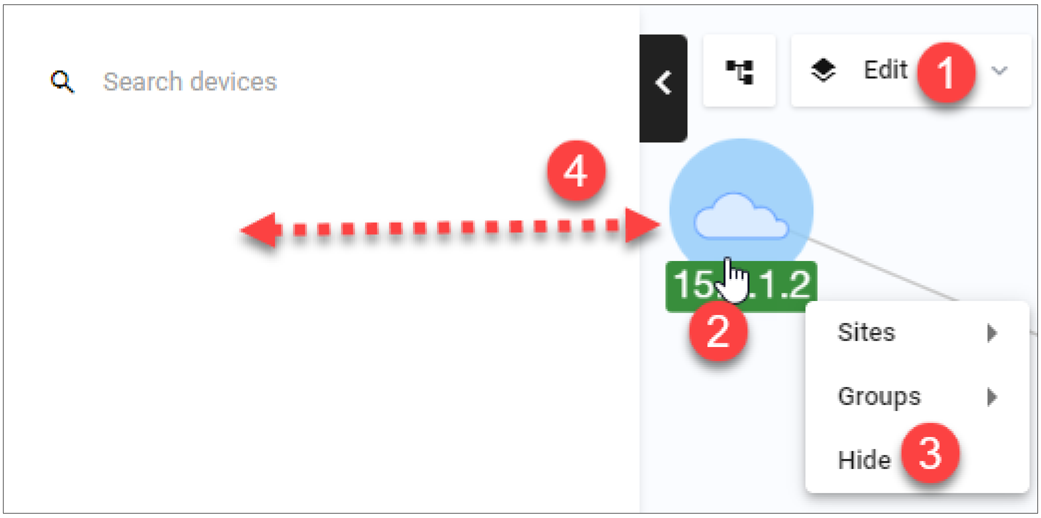
Set the interfaces for each end of the link

Specifying the interfaces for the link will add support for link utilization

Traffic-Gen-1: custom

s40-3050: port1.0.3

- display link utilization statistics for tunnels on the traffic map
- hide/display non-AMF (remote) devices and their associated WAN tunnels via the Edit layer of the map



- enhance custom links to allow you to specify the associated interfaces of the link

There are some limitations to take note of:

- This feature is unable to detect the up/down status of a remote device.
- If two WAN tunnels are connecting to the same device, two cloud icons will show instead of one. Vista Manager is unable to discover if two IPs are on the same device.
- Removing or configuring interfaces on automatically discovered tunnels are not possible. You can only hide a remote device and its associated links.
- Link utilization data of a port connected to a server is not supported unless the connection is via a tunnel. Manually adding a remote device and a custom link, and specifying the associated interface will display its link utilization data.

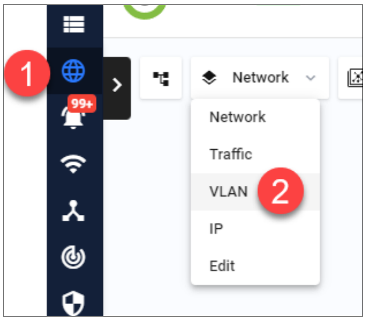
VLAN management

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

To configure VLANs, navigate to the VLAN Map:

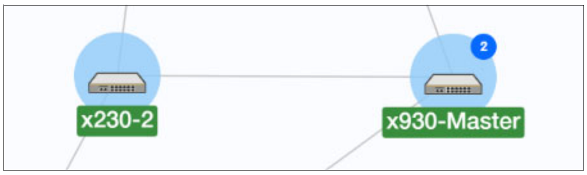
1. In the lefthand menu, select **Network Map**.
2. Select **VLAN** from the Network dropdown list.



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.

To create a VLAN, select the device or devices you want to add the VLAN to. Click to select one device, and Shift-click to select more devices.



EPSR ports are disabled on the VLAN editing page. You can easily identify EPSR ports when editing VLANs, and avoid misconfigurations.

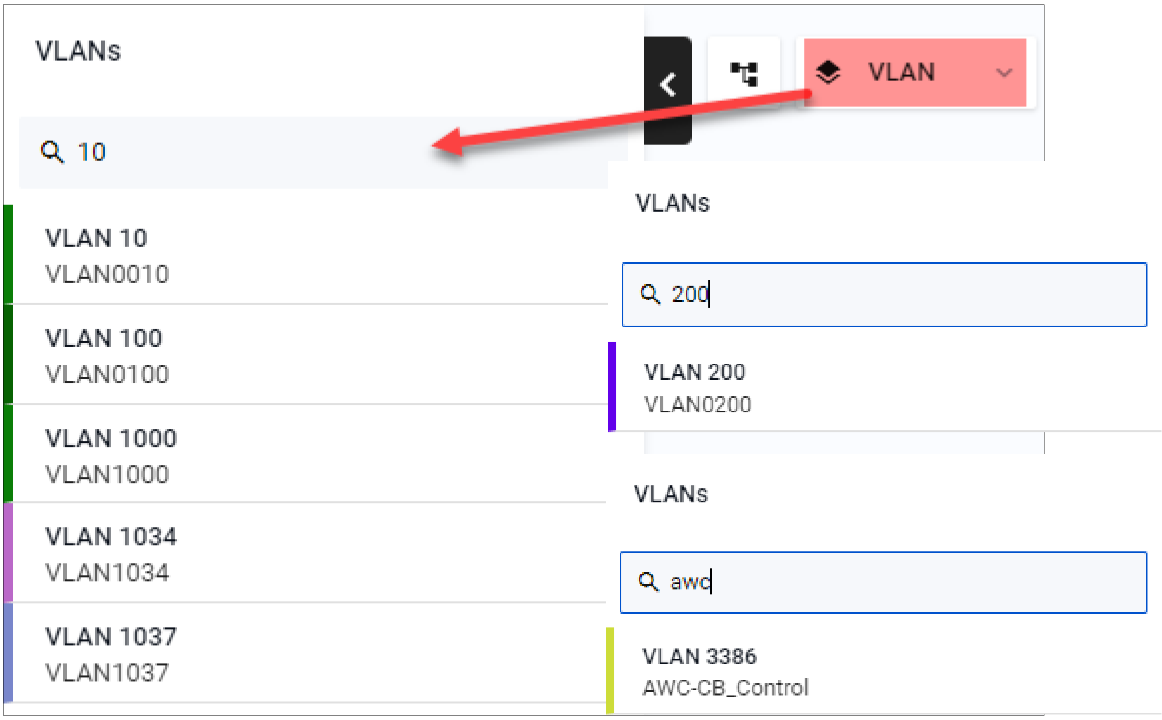
To see more about how to use the VLAN management functionality, refer to the VLAN Management video on the Allied Telesis website.

VLAN search

The search box supports almost instant filtering by **VLAN ID** and **VLAN name**.

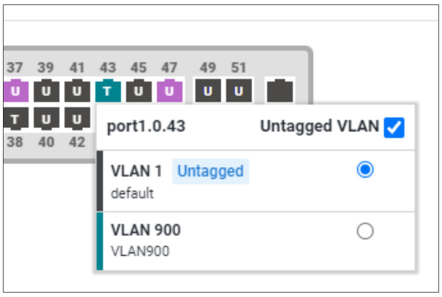
When searching by **VLAN ID**, the filter performs an exact match to narrow down search results and ensure higher accuracy. When searching for **VLAN names**, the filter is not case-sensitive and performs partial matching only.

For example, a user tries to search for ‘VLAN 10’ in a network that also has VLAN 50 named Building 100. Typing ‘10’ will return results of ‘VLAN 10’ being top of the list, because it is a direct match on the VLAN ID. Other VLANs containing 10 in their names will appear after, such as VLAN 100, 1000, 1034, etc..



VLAN 1 port reconfiguration

If a port is assigned to VLAN 1 in Access mode, a different VLAN can be reassigned without first having to remove VLAN 1. The VLAN 1 states of ports are treated the same as all other VLANs. Every port will have a ‘U’ (Access) or a ‘T’ (Trunk) displayed. When VLAN 1 is selected, ports with VLAN 1 assigned can only be changed between Access and Trunk modes. There is no ‘blank’ state.



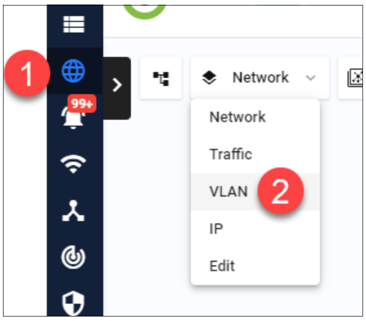
Native VLAN configuration

You can use the VLAN map to assign native VLANs to switchports on devices.

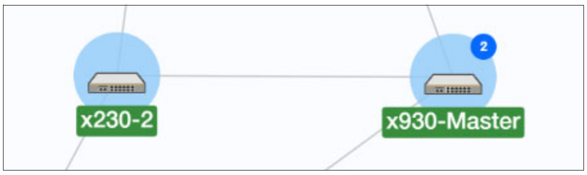
Once a port has a native VLAN, any packets received on the switchport without a VLAN tag are placed into the native VLAN. Packets leaving a switchport on the native VLAN will not be tagged. Different native VLANs can be assigned to different switchports on a device. Only one native VLAN can exist per switchport.

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

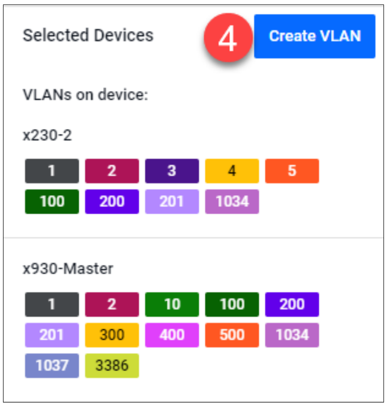
1. In the lefthand menu, select **Network Map**.
2. Select **VLAN** from the Network dropdown list.



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



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



Selected Devices Create VLAN

VLANs on device:

x230-2

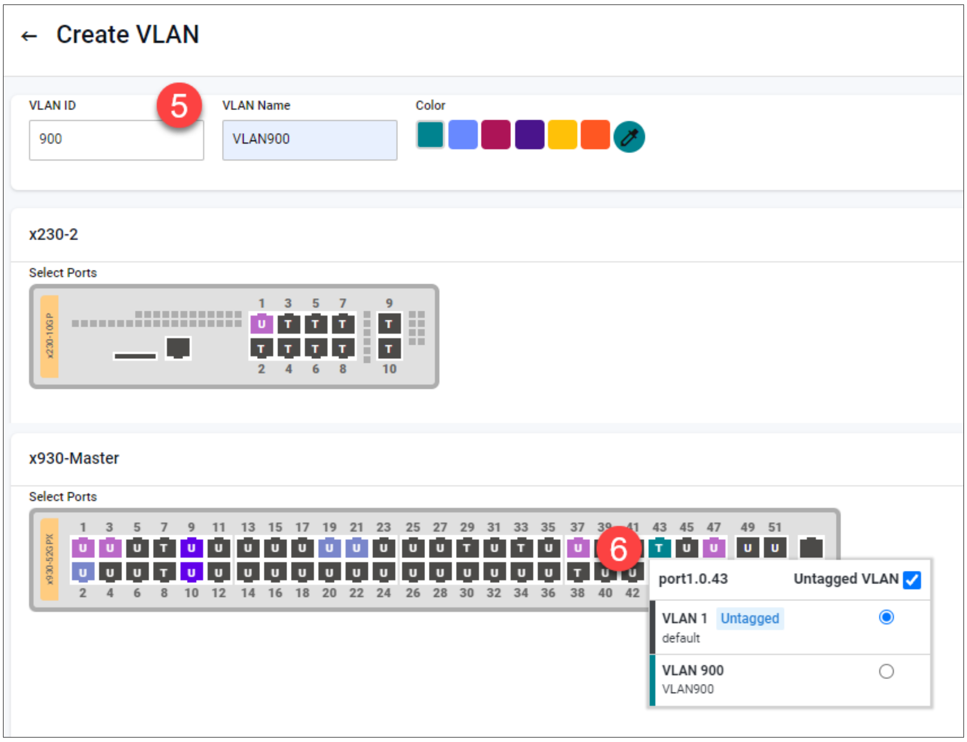
1 2 3 4 5
100 200 201 1034

x930-Master

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

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

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



← Create VLAN

VLAN ID: 900

VLAN Name: VLAN900

Color

x230-2

Select Ports

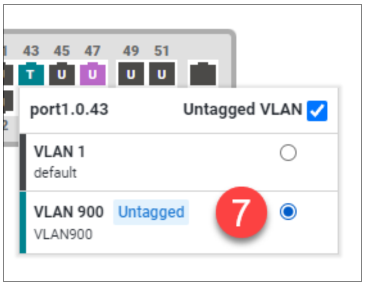
x930-Master

Select Ports

port1.0.43 Untagged VLAN ☑

- VLAN 1 Untagged ● default
- VLAN 900 ○ VLAN900

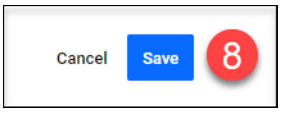
7. A pop-up will appear, showing the current native VLAN (probably VLAN 1) and the port's other VLANs, including the new VLAN. In the pop-up, select the VLAN that you want to make the native VLAN.



port1.0.43 Untagged VLAN ☑

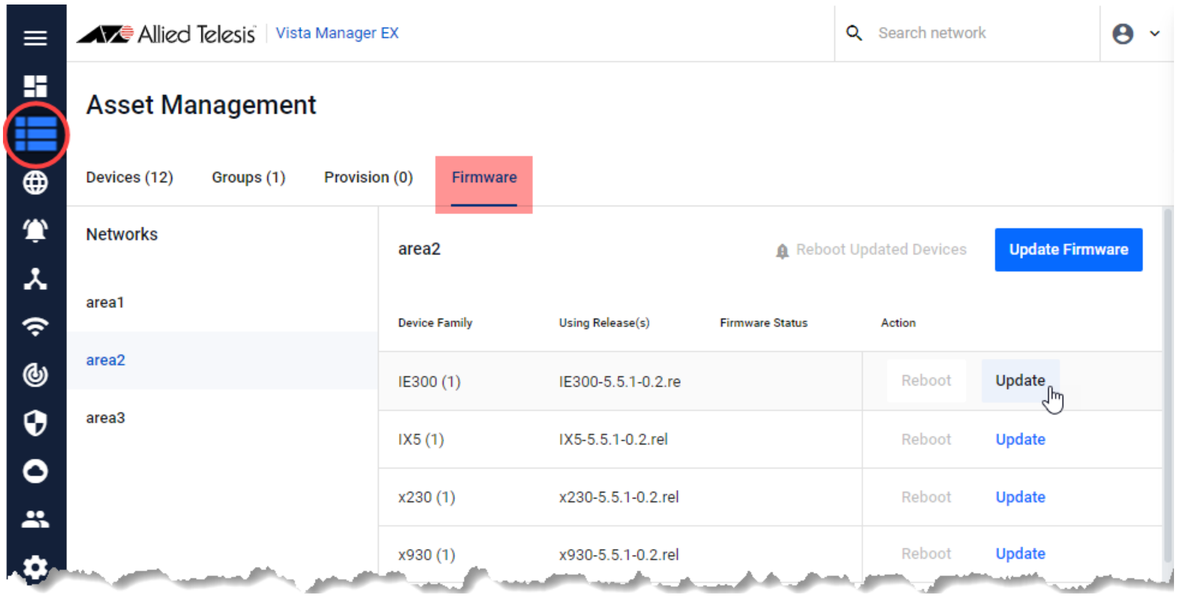
- VLAN 1 ○ default
- VLAN 900 Untagged ● VLAN900

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



Firmware management

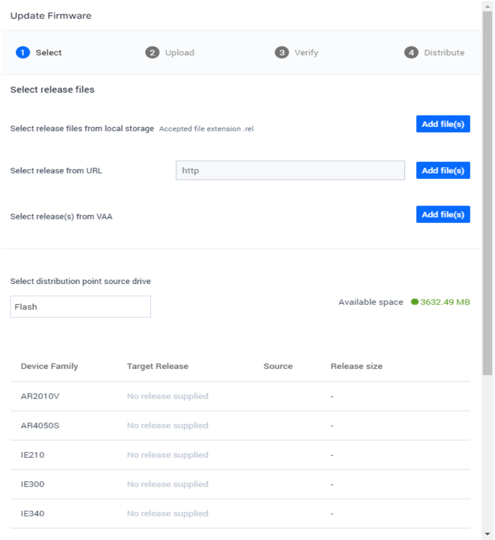
This feature provides you with the ability to update firmware across a device or family of devices on a network (AMF area), and then schedule a time when the devices will reboot to install the firmware release.



Device Family	Using Release(s)	Firmware Status	Action
IE300 (1)	IE300-5.5.1-0.2.re		Reboot Update
IX5 (1)	IX5-5.5.1-0.2.rel		Reboot Update
x230 (1)	x230-5.5.1-0.2.rel		Reboot Update
x930 (1)	x930-5.5.1-0.2.rel		Reboot Update

1. From the left-hand menu, navigate to Asset Management and click on the **Firmware** tab.
2. To the right, you will see buttons to update a family of devices, or an **Update Firmware** button to update **all** families in an AMF area. Click on any of the blue **Update** action buttons.
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 devices.



Select release files

Select release files from local storage Accepted file extension .rel

Select release from URL: http

Select release(s) from VAA

Select distribution point source drive: Flash

Available space ● 3632.49 MB

Device Family	Target Release	Source	Release size
AR2010V	No release supplied		-
AR4050S	No release supplied		-
IE210	No release supplied		-
IE300	No release supplied		-
IE340	No release supplied		-

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 (firmware distribution)

Note: Users also have the option to copy the file to a USB drive if their Flash drive is full on the firmware 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 devices failed. If any failed, click More info to see exactly which devices failed and why. Assuming that some succeeded, click Update device.**

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

4. AlliedWare Plus software versions require a release license for SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a suitable license certificate. For details, see the ***“Licensing this Version...”*** sections of the relevant AlliedWare Plus release note.

5. Click **Reboot Updated Devices**, then select the date and time for the reboot. After the reboot, those devices will be running the release file provided.

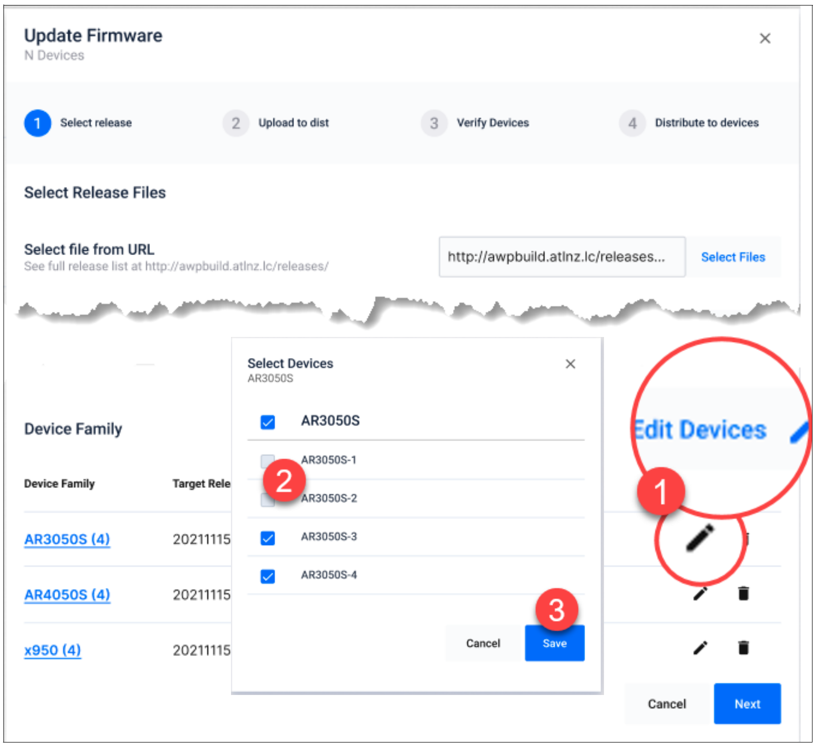
Note: If you use firmware distribution to copy a firmware file to devices, and that file already exists on a device, then firmware distribution will overwrite the existing file. This makes it possible to use firmware distribution to repair a corrupted firmware file on a device.

Selective firmware upgrade

You can exclude selected devices from a given family when you perform a firmware upgrade.

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

1. Select the release files from your desired location. Then click on the **Edit Devices** button or the pencil **Edit** icon in the **Action** column.
    - Edit Devices - to select devices per family
    - Edit action - to select devices for specific families in the same area
2. A pop-up then appears listing all devices under the device family. This allows you to deselect specific devices before upgrading the firmware.
3. Click **Save** when you have finished. The number of target devices are updated after you save the changes.



Select file from URL
See full release list at http://awpbuild.atlnz.lc/releases/
http://awpbuild.atlnz.lc/releases...

Device Family

Device Family	Target Rele
AR3050S (4)	20211115
AR4050S (4)	20211115
x950 (4)	20211115

Select Devices
AR3050S

☑ AR3050S
□ AR3050S-1
□ AR3050S-2
☑ AR3050S-3
☑ AR3050S-4

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

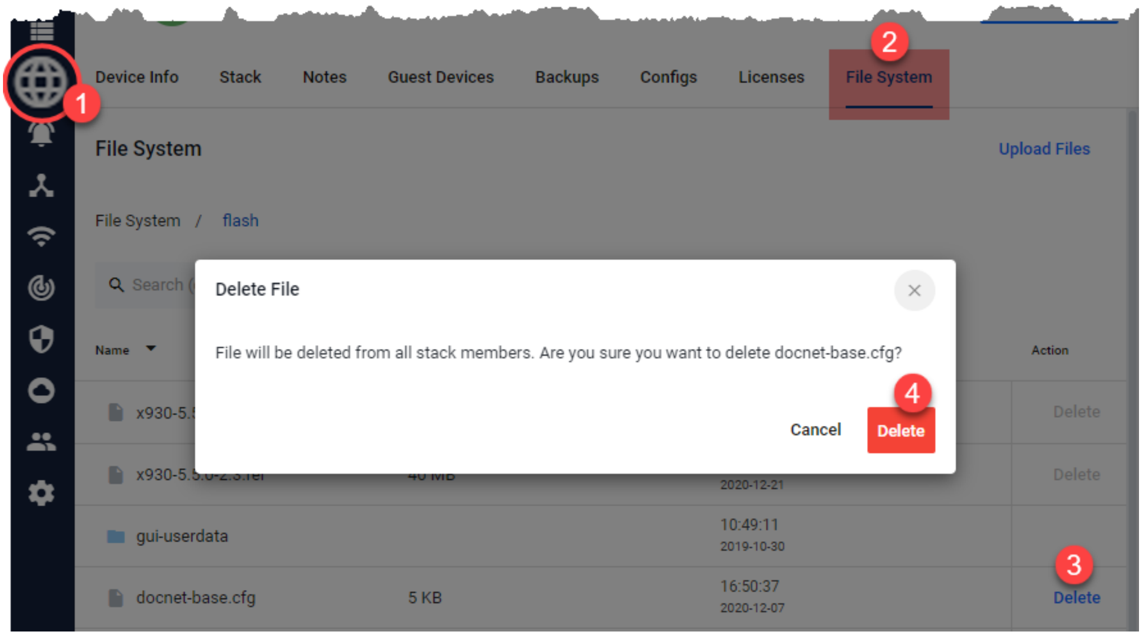
Zip folder support

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.

Searching and deleting files from the file system

Users with write permissions will be able to delete supported files from the file system of a device. The ability to search for files has also been added. This makes it easier to find which files to delete. You may use this feature to free up space on a device before upgrading its firmware. To delete a file:



Delete File

File will be deleted from all stack members. Are you sure you want to delete docnet-base.cfg?

1. Select a device from your network map. Double-click on it.
2. On the device details page, navigate to the **File System** tab.
3. You will see an **Action** column with delete buttons on the right. Click **Delete** for the file(s) that you wish to delete.
4. A confirmation message appears. Click **Delete** to proceed. A success notification then appears on the bottom right.

Note: File(s) selected for deletion on a stacked device will be deleted from all stack members.

There are some limitations to take note of:

- Protected files cannot be deleted:
  - boot firmware release files
  - backup boot firmware release files
  - boot configuration files
  - backup boot configuration files
- Directories cannot be deleted.
- Wildcard characters (*) are not supported in the file search.

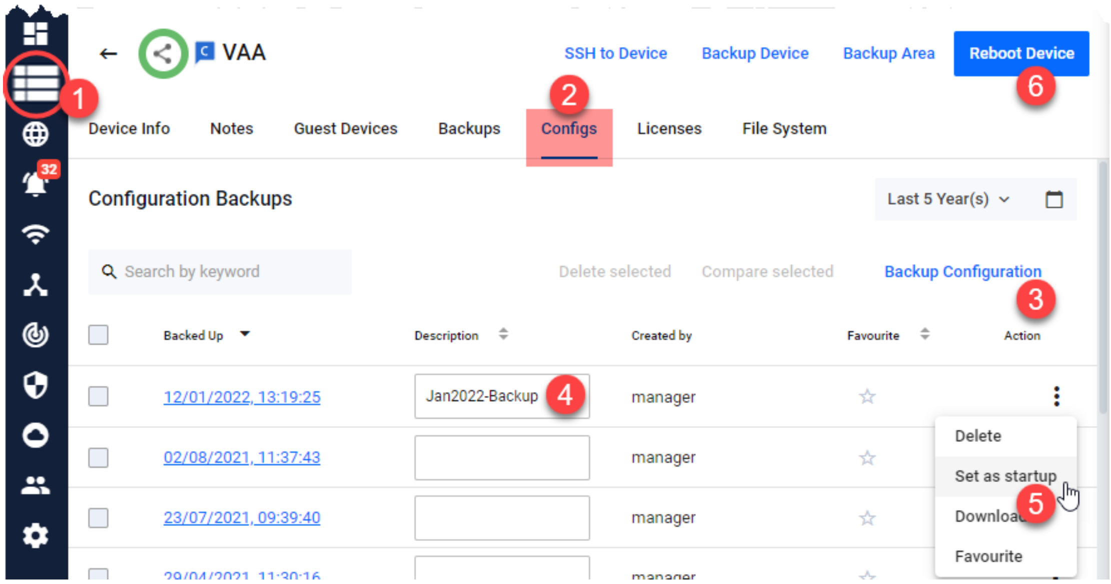
This feature requires firmware version AlliedWare Plus v5.4.9-0.1 or later.

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.



□	Backed Up	Description	Created by	Favourite	Action
□	12/01/2022, 13:19:25	Jan2022-Backup	manager	☆	⋮
□	02/08/2021, 11:37:43		manager	☆	
□	23/07/2021, 09:39:40		manager	☆	
□	29/04/2021, 11:30:16		manager	☆	

1. From the left-hand menu, navigate to **Asset Management** and select the device you wish to work with.

2. Click on the **Configs** tab.

3. Click on the **Backup Configuration** 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. A bell icon will appear on the Reboot Device indicating further action is required. Click the **Reboot Device** button immediately, or schedule a time for it.

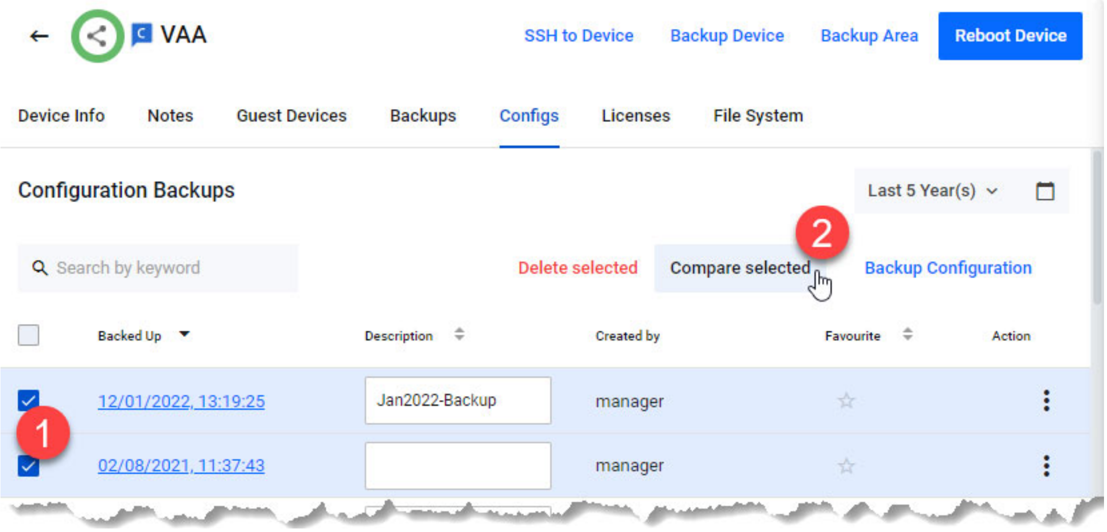
Note: Restoring a config overwrites the contents of the current startup-config only. The original filename and location of the backup config will not be used during the restore.

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

1. Click on the check box on the left-hand side of each configuration file you wish to compare. Select up to two files.

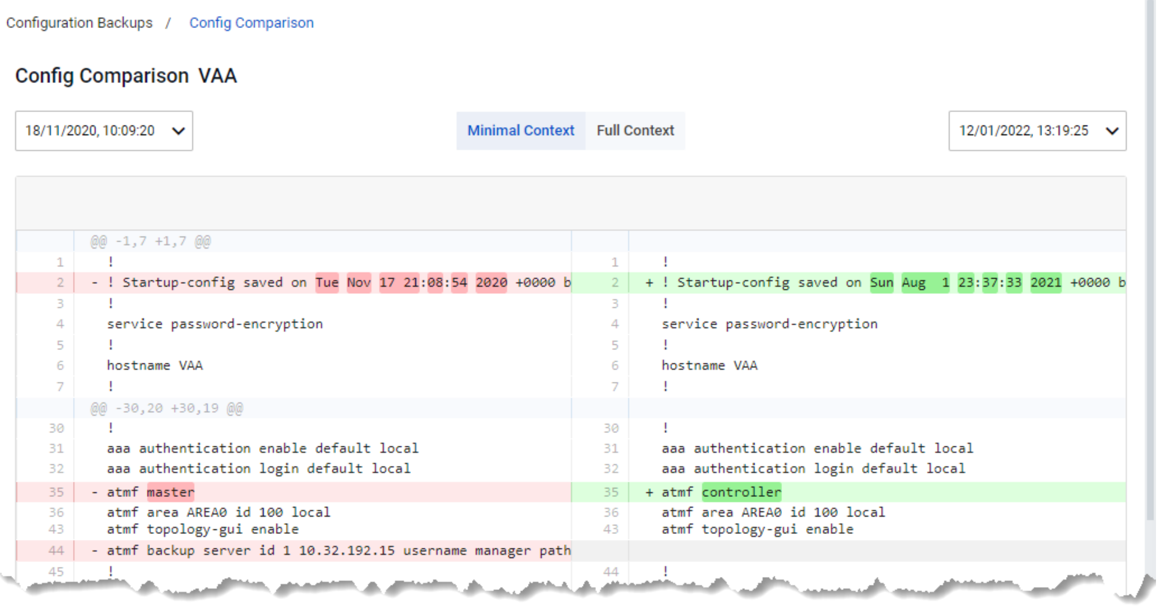
2. Click on the **Compare selected** button.



☐	Backed Up	Description	Created by	Favourite	Action
☑	12/01/2022, 13:19:25	Jan2022-Backup	manager	☆	⋮
☑	02/08/2021, 11:37:43		manager	☆	⋮

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.

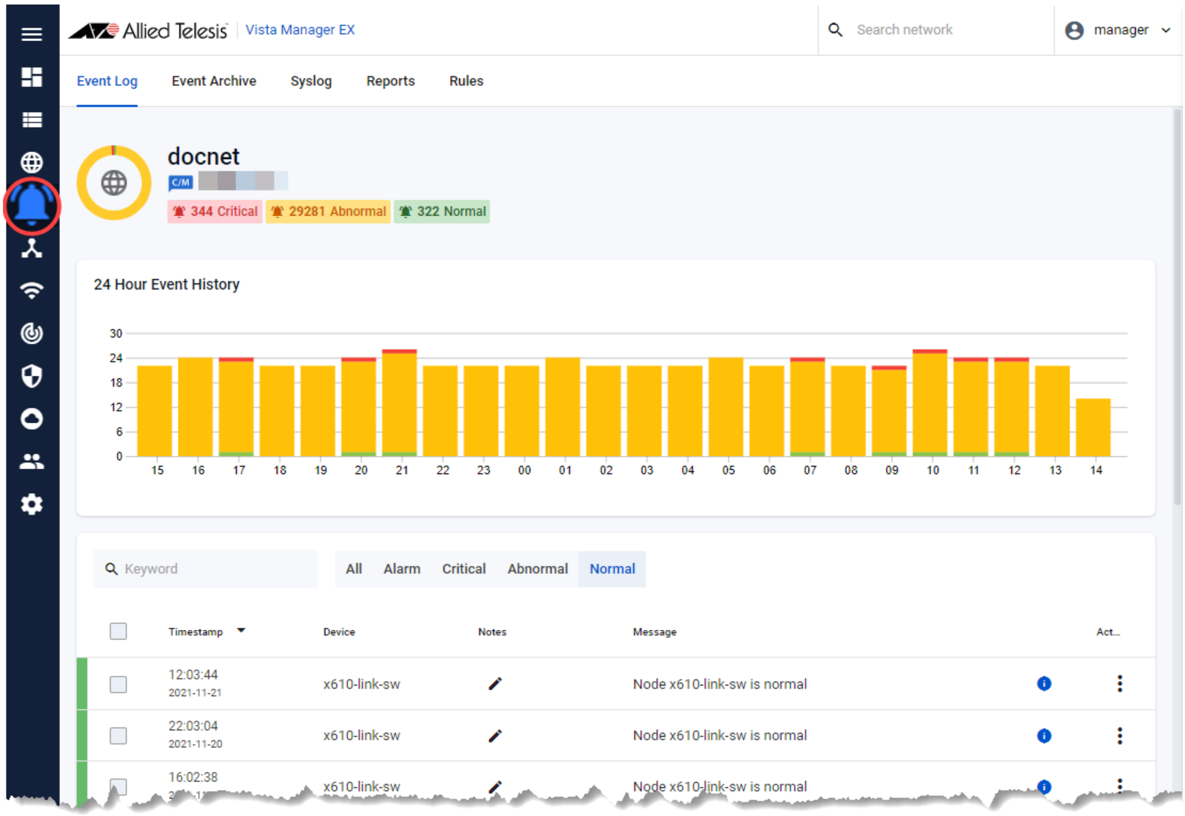


Config Comparison VAA

```
@@ -1,7 +1,7 @@
  !                                                          !
- ! Startup-config saved on Tue Nov 17 21:08:54 2020 +0000 b  + ! Startup-config saved on Sun Aug  1 23:37:33 2021 +0000 b
  !                                                          !
  service password-encryption                                service password-encryption
  !                                                          !
  hostname VAA                                               hostname VAA
  !                                                          !
@@ -30,20 +30,19 @@
  !                                                          !
  aaa authentication enable default local                    aaa authentication enable default local
  aaa authentication login default local                     aaa authentication login default local
- atmf master                                                + atmf controller
  atmf area AREA0 id 100 local                               atmf area AREA0 id 100 local
  atmf topology-gui enable                                   atmf topology-gui enable
- atmf backup server id 1 10.32.192.15 username manager path
  !                                                          !
```

Using the event log

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



□	Timestamp ▾	Device	Notes	Message	Act...
□	12:03:44 2021-11-21	x610-link-sw	✎	Node x610-link-sw is normal	ⓘ ⋮
□	22:03:04 2021-11-20	x610-link-sw	✎	Node x610-link-sw is normal	ⓘ ⋮
□	16:02:38	x610-link-sw	✎	Node x610-link-sw is normal	ⓘ ⋮

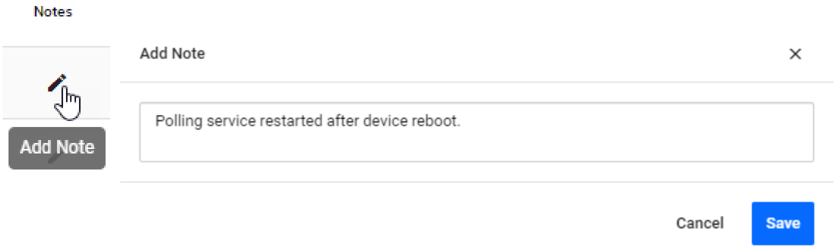
The event log shows currently uncleared events. Critical events have a red background, abnormal events are yellow, and normal events are green.

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.



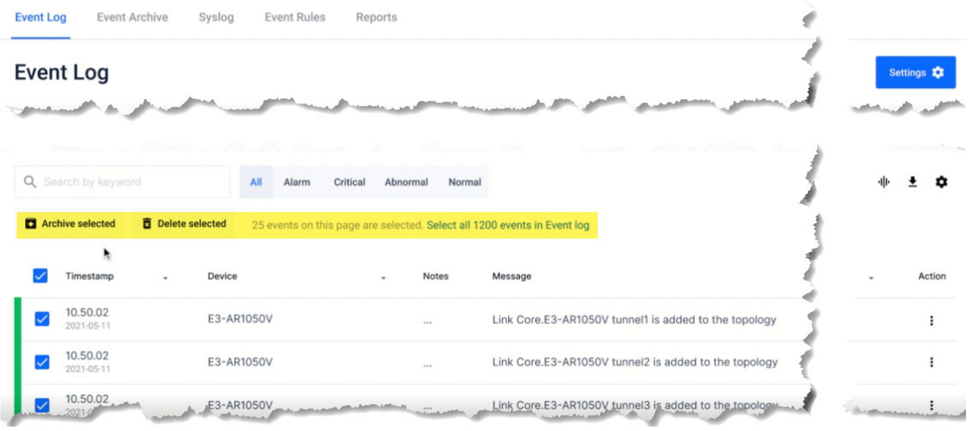
Polling service restarted after device reboot.

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.

You can also:

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

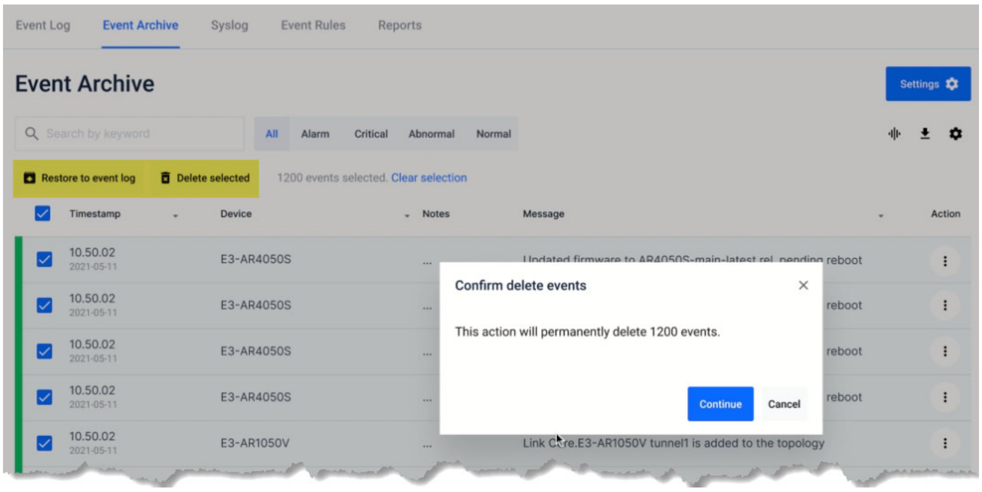


25 events on this page are selected. Select all 1200 events in Event log

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

You can also:

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



1200 events selected. Clear selection

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

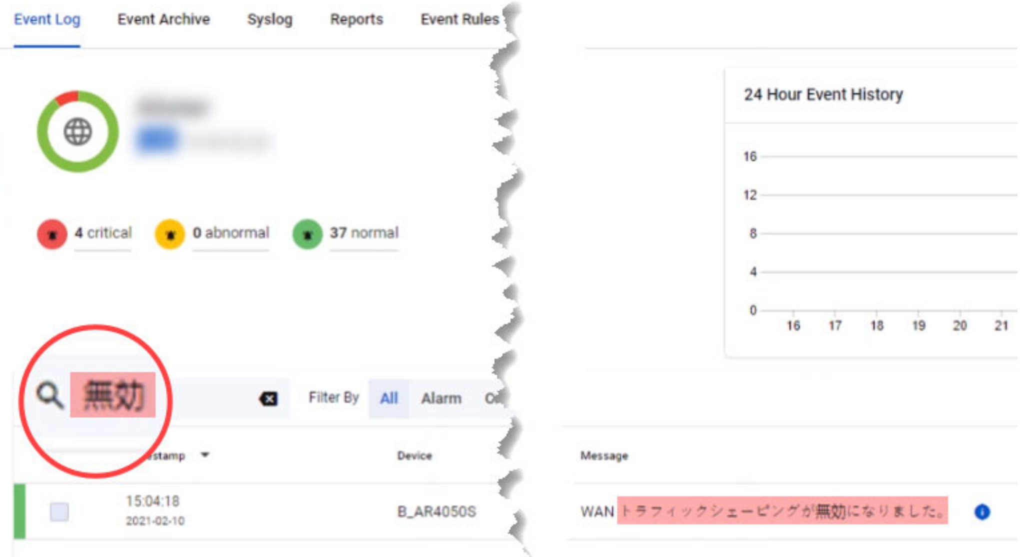
Confirm delete events

This action will permanently delete 1200 events.

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

Japanese event language support

By upgrading to Vista Manager EX version 3.7.0 and later, you will be able to search for events in Japanese. A large number of English-only events now have Japanese translations, where they did not previously.



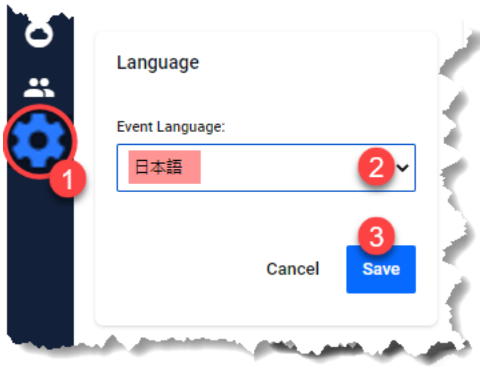
stamp	Device	Message
15:04:18 2021-02-10	B_AR4050S	WAN トラフィックシェーピングが無効になりました。

Most event messages now have a translation key. Event rules have been improved to store both the **translation key** and **translated value**. The translated value of an event rule is used to match translation keys of event messages. Because of this, the match becomes highly specific as each event rule applies to only one event message.

Note: We recommend using the **title field** instead of the message field when creating event rules so that broader search results can be achieved.

Changing the event language initiates the background process of translating past events. Once past events have been translated, event rule messages will then be translated to the new language. An event log is created when the translation completes.

Administrators will have the ability to change the event language from the System Management page.


Language

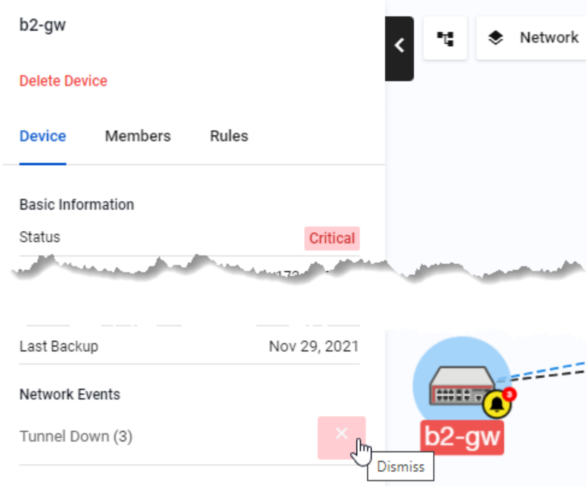
Event Language: 日本語

Note: This language support functionality is only applicable to the Event Log, SD-WAN table of events, and Event Rules. Plug-in events will not be translated.

This feature has been designed to support more languages in the future.

High priority events

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


b2-gw

Basic Information

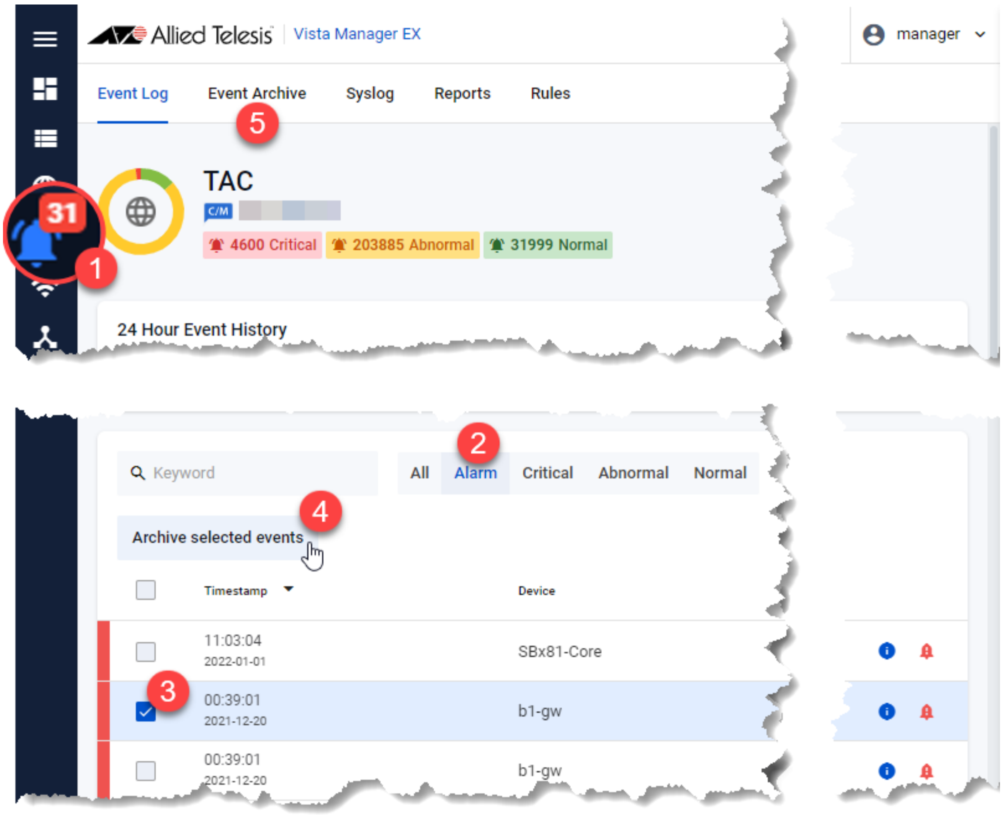
Status: Critical

Last Backup: Nov 29, 2021

Network Events

Tunnel Down (3)

Events can also be archived on the Event Log page. Archiving an event moves the log entry to the Event Archive tab and decreases the alarm icon’s event count on the side bar.



AMF Security block actions

AMF Security (AMF-Sec) blocking actions, configured using AMF application proxy, are displayed as high priority events. AMF-Sec blocking actions configured using OpenFlow are not yet supported.

The following AMF-Sec blocks will be shown on the Area Map and in the Event Log:

- Drop
- Quarantine
- Link Down

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

- IP Filter

See the AMF Security (AMF-Sec) Technical Documents for more information on configuring AMF-Sec and the AMF application proxy.

SNMP traps

SNMP trap events require the SNMP plug-in. If they are configured, the following SNMP traps will appear as high priority events:

- SNMP loop detection traps
- SNMP active fiber monitoring traps.

Creating event filter rules

Applicable to all Vista Manager installations - For Admin users

You can create event rules to notify you whenever certain events occur, such as a port goes up/down, configuration on a device is changed or a fan or power supply failure occurs.

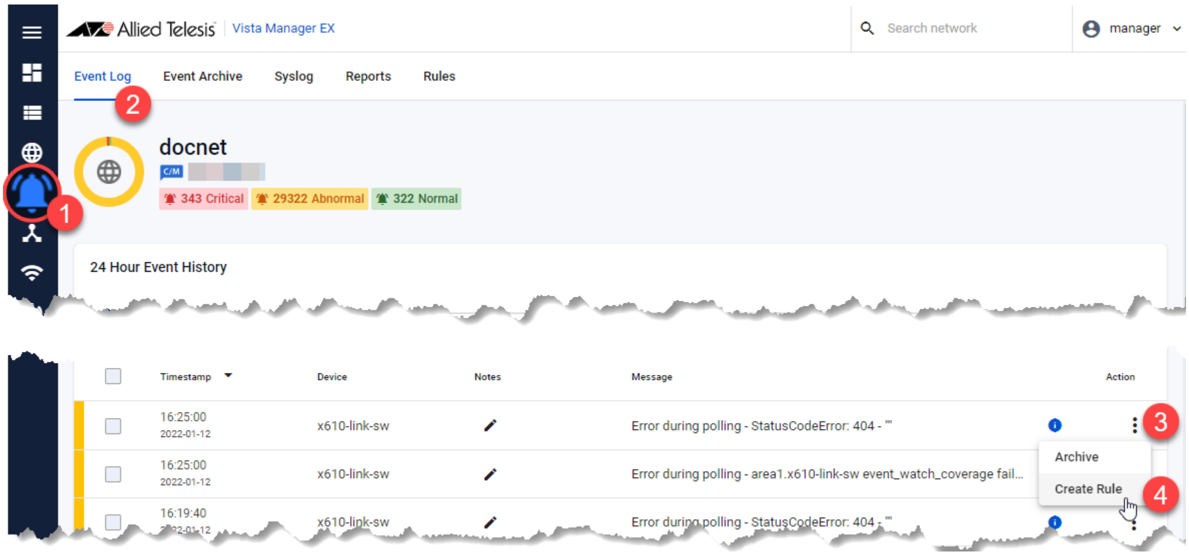
Previously, you had to be actively looking at Vista Manager to notice these things. Now you can simply check your emails.

You can also place an alarm on an event rule to identify it as a critical event. Critical events have a dismissible red alarm icon showing next to them in the **Event Log** window. You can decide if the alarmed event requires immediate action or dismiss it as a normal alert.

Creating Event Rules

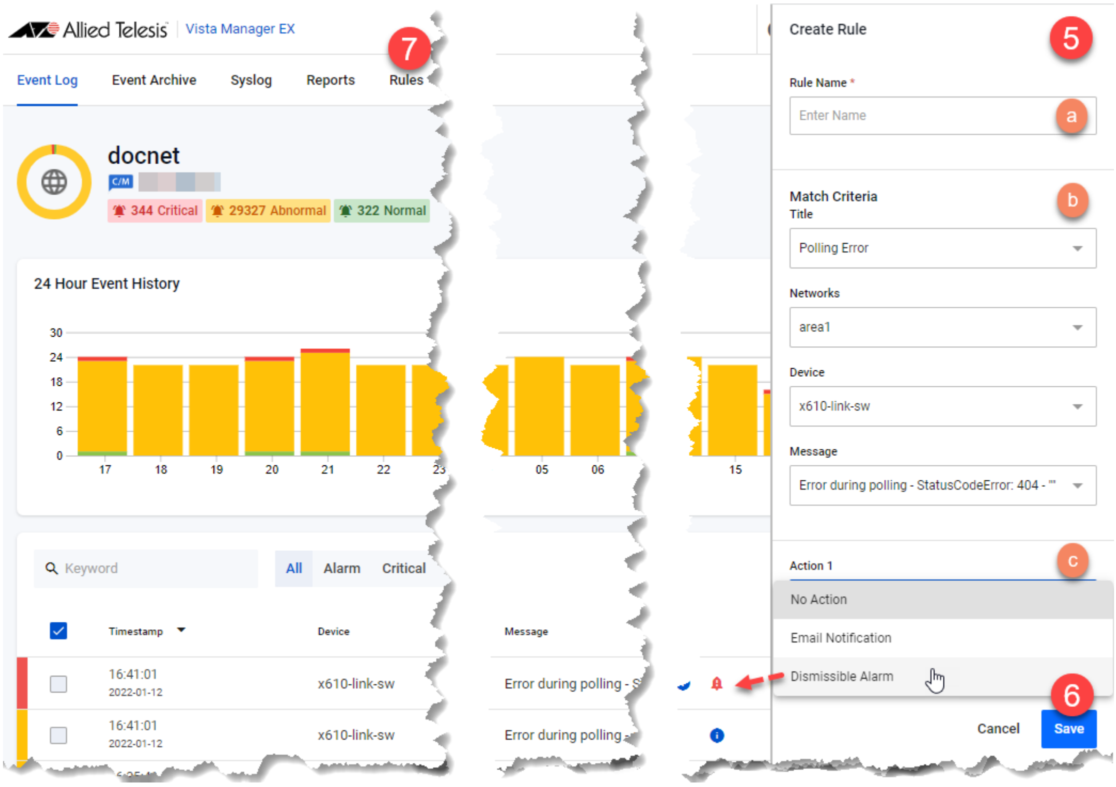
To create an event rule:

1. From the left-hand menu, navigate to **Events.**
2. From the **Event Log** tab, choose an existing event you wish to create a rule for.
3. In the **Action** column, click on the three vertical dots for more options.
4. Select **Create Rule**.



□	Timestamp	Device	Notes	Message	Action
□	16:25:00 2022-01-12	x610-link-sw		Error during polling - StatusCodeError: 404 - ""	
□	16:25:00 2022-01-12	x610-link-sw		Error during polling - area1.x610-link-sw event_watch_coverage fail...	
□	16:19:40 2022-01-12	x610-link-sw		Error during polling - StatusCodeError: 404 - ""	

5. The Create Rule side-panel opens. The criteria will be pre-filled based on the event that has been selected. Configure as required.



☐	Timestamp	Device	Message
☐	16:41:01 2022-01-12	x610-link-sw	Error during polling - S
☐	16:41:01 2022-01-12	x610-link-sw	Error during polling -

Create Rule

Rule Name *: Enter Name

Match Criteria

Title: Polling Error

Networks: area1

Device: x610-link-sw

Message: Error during polling - StatusCodeError: 404 - ""

Action 1: No Action / Email Notification / Dismissible Alarm

a. Enter a rule name.

b. Select **any** criteria to match on anything.

c. Select an **Action**: Email Notification, Dismissible Alarm, or No Action.

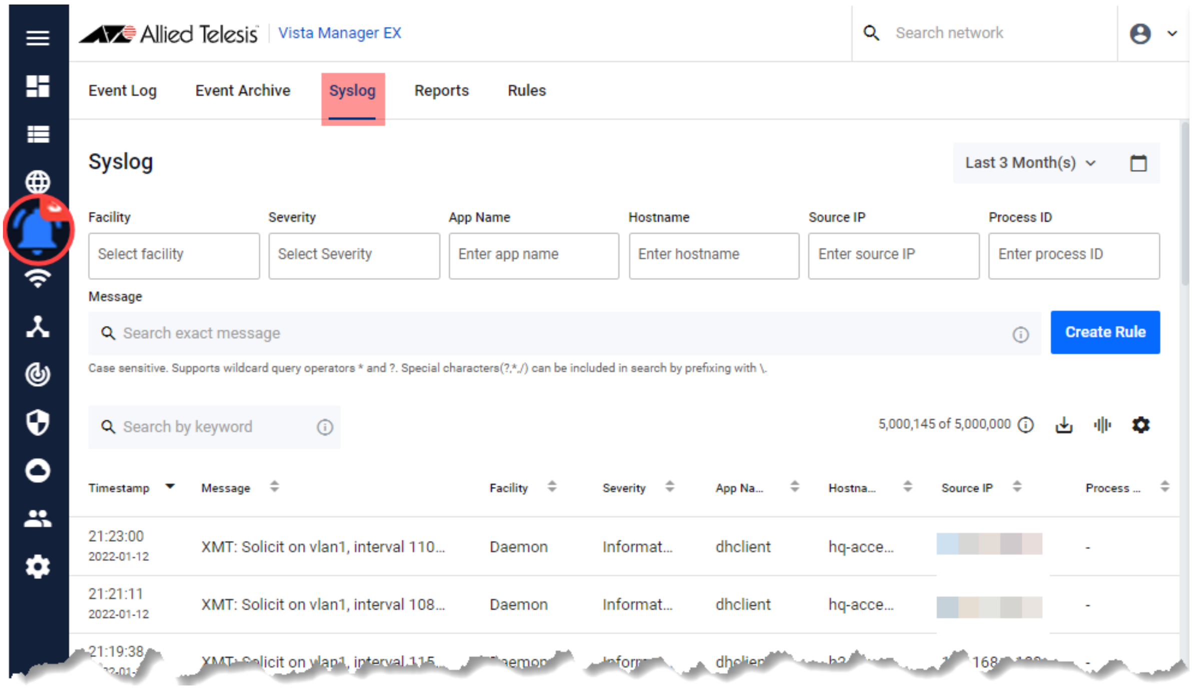
6. Click **Save**.

7. Use the **Rules** tab to view, edit, or delete existing rules.

Note: An SMTP server is required for email notifications to be sent. You can configure users' email addresses in the **User Management** window.

Using the syslog server

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



Syslog

Last 3 Month(s)

Facility	Severity	App Name	Hostname	Source IP	Process ID
Select facility	Select Severity	Enter app name	Enter hostname	Enter source IP	Enter process ID

Message: Search exact message

Case sensitive. Supports wildcard query operators * and ?. Special characters(?,*,/) can be included in search by prefixing with \.

Search by keyword

5,000,145 of 5,000,000

Timestamp	Message	Facility	Severity	App Na...	Hostna...	Source IP	Process ...
21:23:00 2022-01-12	XMT: Solicit on vlan1, interval 110...	Daemon	Informat...	dhclient	hq-acce...	[redacted]	-
21:21:11 2022-01-12	XMT: Solicit on vlan1, interval 108...	Daemon	Informat...	dhclient	hq-acce...	[redacted]	-
21:19:38	XMT: Solicit on vlan1, interval 115	Daemon	Inform	dhclien	h2	168	-

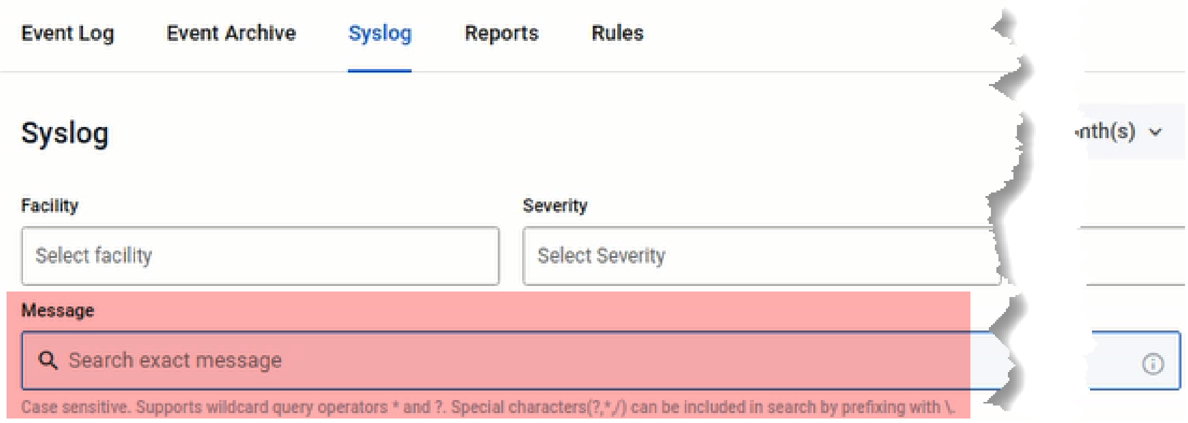
The syslog server shows messages from the network or for a specific device on the network. Depending on your level of access, Administrator access allows you to configure how long to store syslog messages. The default configuration is 365 days. Messages older than the default or configured length of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

Note: For the syslog server to display accurate timestamps and valid messages, it is highly recommended for the device to be running Alliedware Plus version 5.4.8 or later and have the **log date-format iso** command configured by the administrator.

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 device, 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.

Syslog message filtering



Syslog

Facility: Select facility

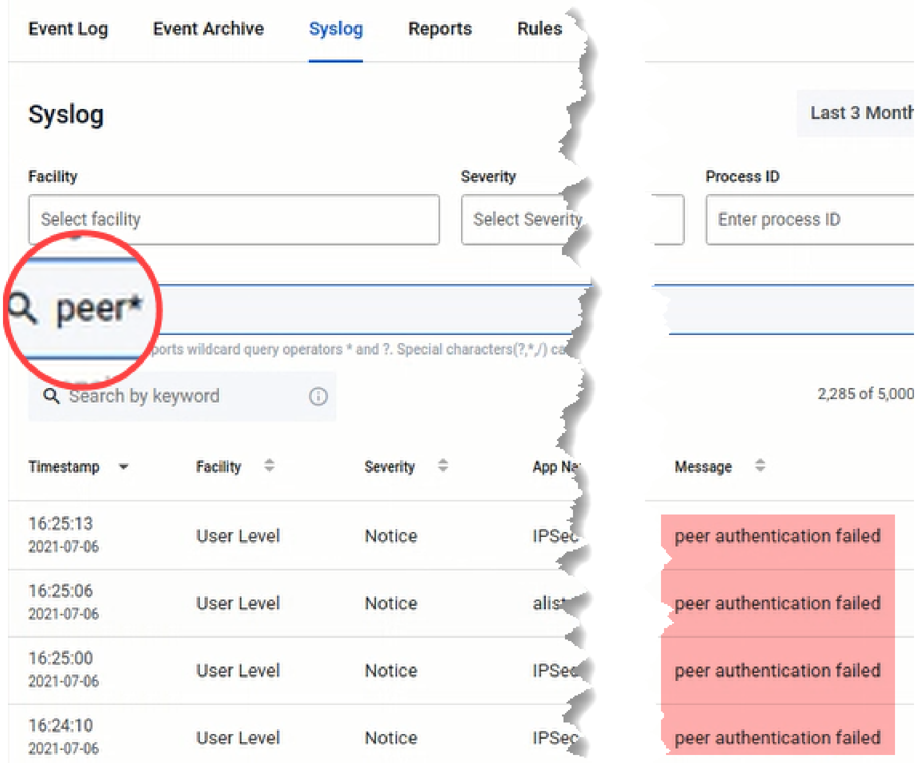
Severity: Select Severity

Message: Search exact message

Case sensitive. Supports wildcard query operators * and ?. Special characters(?,*,/) can be included in search by prefixing with \.

Filter syslog events by whole or partial message content, by using multiple wildcards. Details of supported wildcard query operators and special characters are as follows:

- A question mark (**?**) is used for a single character.
- An asterisk (*****) is used for multiple characters.



Syslog

Facility: Select facility

Severity: Select Severity

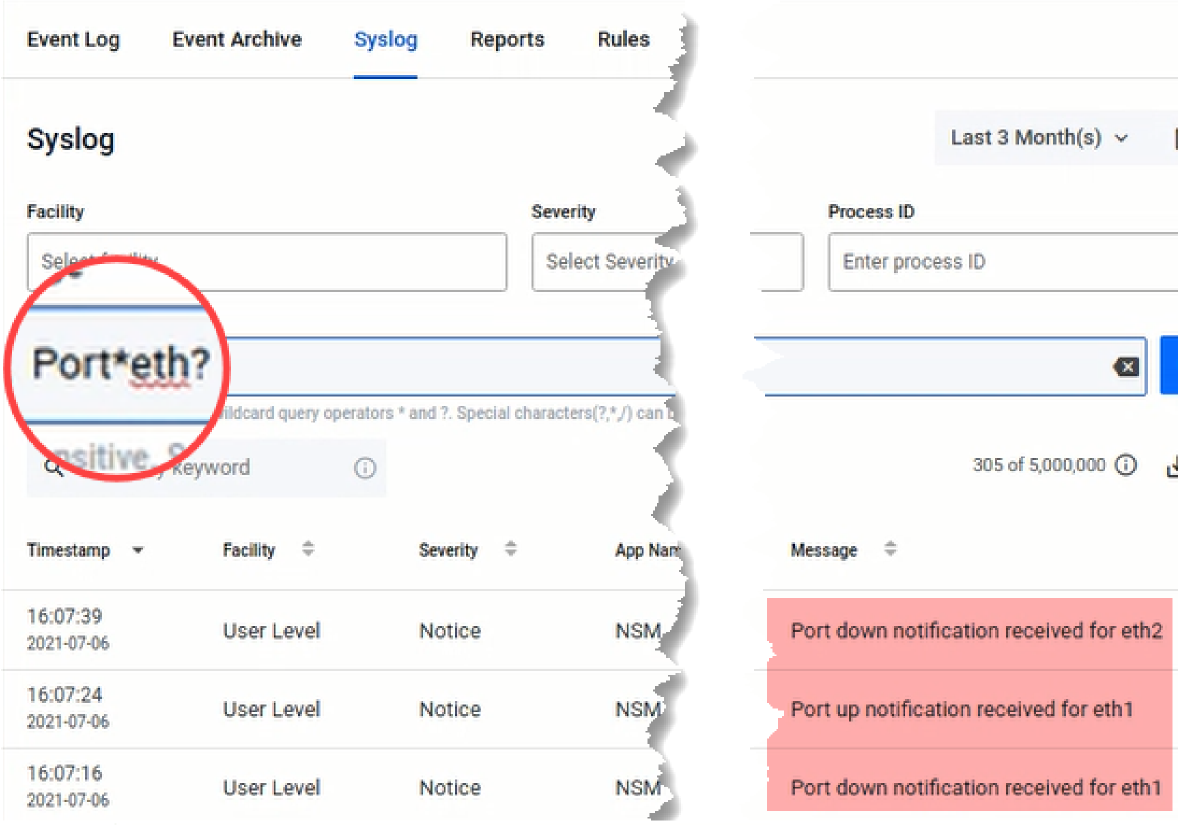
Process ID: Enter process ID

peer*

ports wildcard query operators * and ?. Special characters(?,*,/) ca

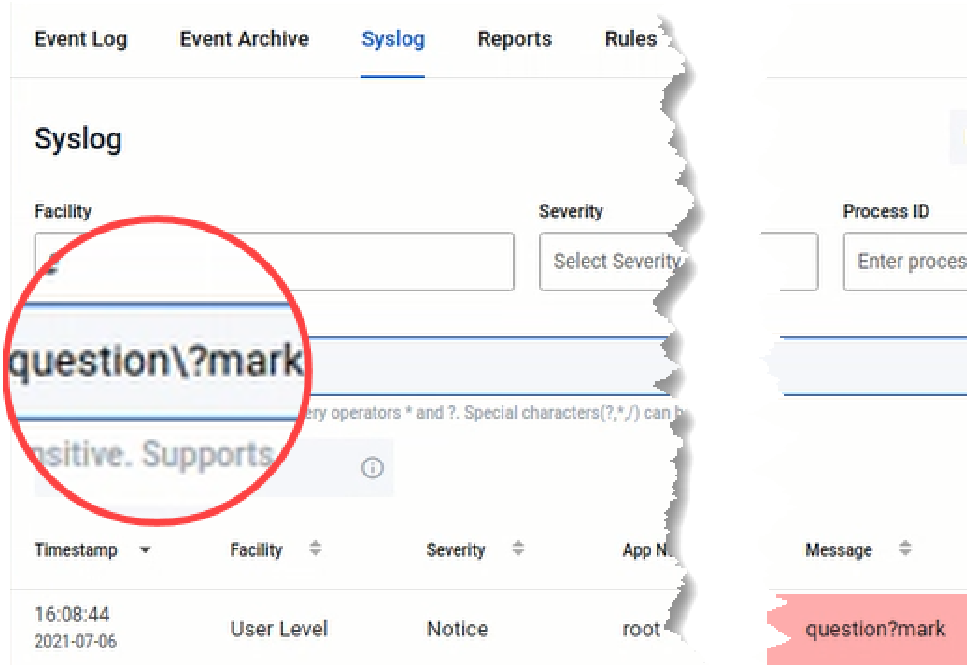
Timestamp	Facility	Severity	App Na	Message
16:25:13 2021-07-06	User Level	Notice	IPSec	peer authentication failed
16:25:06 2021-07-06	User Level	Notice	alis	peer authentication failed
16:25:00 2021-07-06	User Level	Notice	IPSec	peer authentication failed
16:24:10 2021-07-06	User Level	Notice	IPSec	peer authentication failed

- A backslash (\) is used to escape any special characters (**?**, *****, **/**) after it.
- When a backslash is expected to be part of the message to be matched on, escape it with an additional (preceding) backslash.
- When an asterisk is expected to be part of the message to be matched on, escape it with a preceding backslash.



Port*eth?

Timestamp	Facility	Severity	App Nam	Message
16:07:39 2021-07-06	User Level	Notice	NSM	Port down notification received for eth2
16:07:24 2021-07-06	User Level	Notice	NSM	Port up notification received for eth1
16:07:16 2021-07-06	User Level	Notice	NSM	Port down notification received for eth1



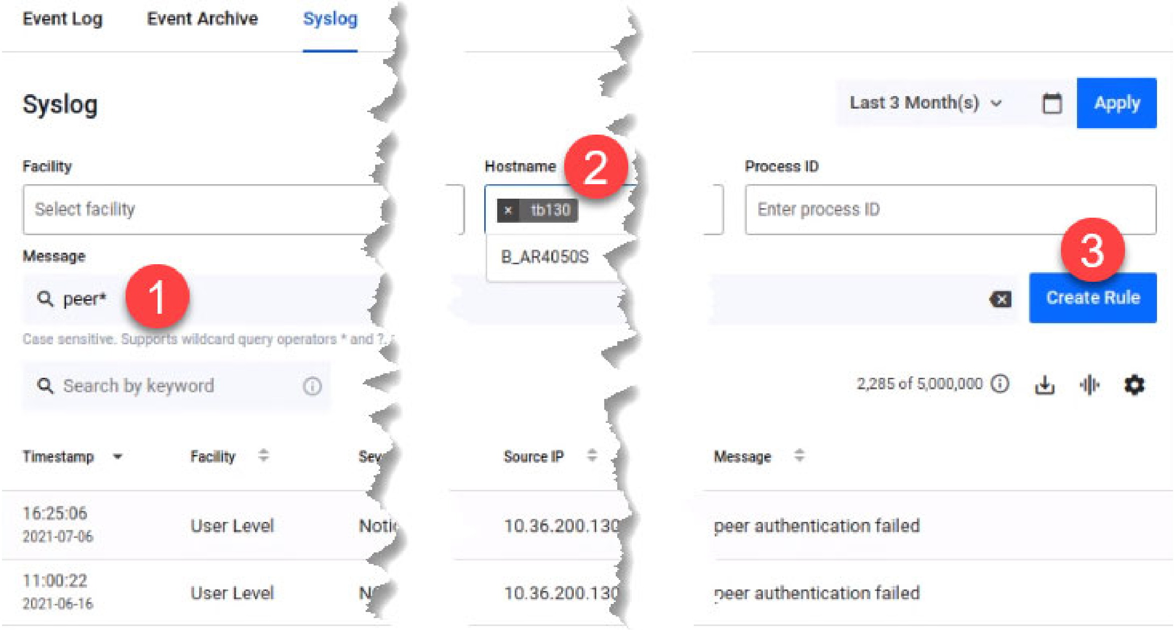
question\?mark

Timestamp	Facility	Severity	App N	Message
16:08:44 2021-07-06	User Level	Notice	root	question?mark

Syslog rules

Syslog rules work similarly as the existing event rules. Any received syslog that matches a rule will trigger the action associated with the rule. Create a syslog rule based on the syslog message filter from the syslog tab page. When creating a single rule, configure up to two of the following actions:

- email notification
- dismissible alarm
- no action



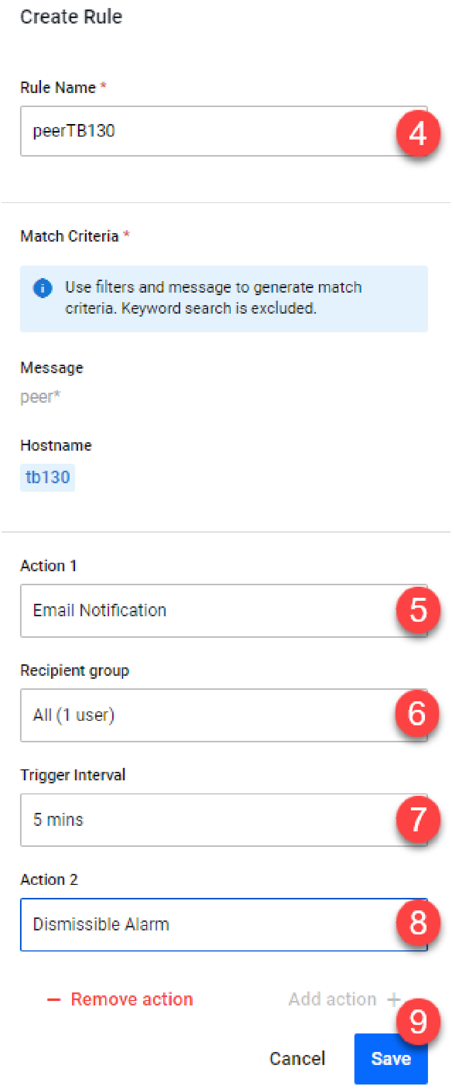
Message: peer*

Hostname: tb130

B_AR4050S

Timestamp	Facility	Sev	Source IP	Message
16:25:06 2021-07-06	User Level	Noti	10.36.200.130	peer authentication failed
11:00:22 2021-06-16	User Level	N	10.36.200.130	peer authentication failed

1. Use the syslog message filtering to search for messages of your choice.
2. Next, select a hostname.
3. Click **Create Rule**. This opens up a side panel.
4. Enter a rule name.
5. Configure a first action for **email notification**.
6. Select a recipient group.
7. Select a trigger interval time.
8. Configure a second action for **dismissible alarm**.
9. Click **Save**.



Create Rule

Rule Name *

peerTB130 4

Match Criteria *

Use filters and message to generate match criteria. Keyword search is excluded.

Message

peer*

Hostname

tb130

Action 1

Email Notification 5

Recipient group

All (1 user) 6

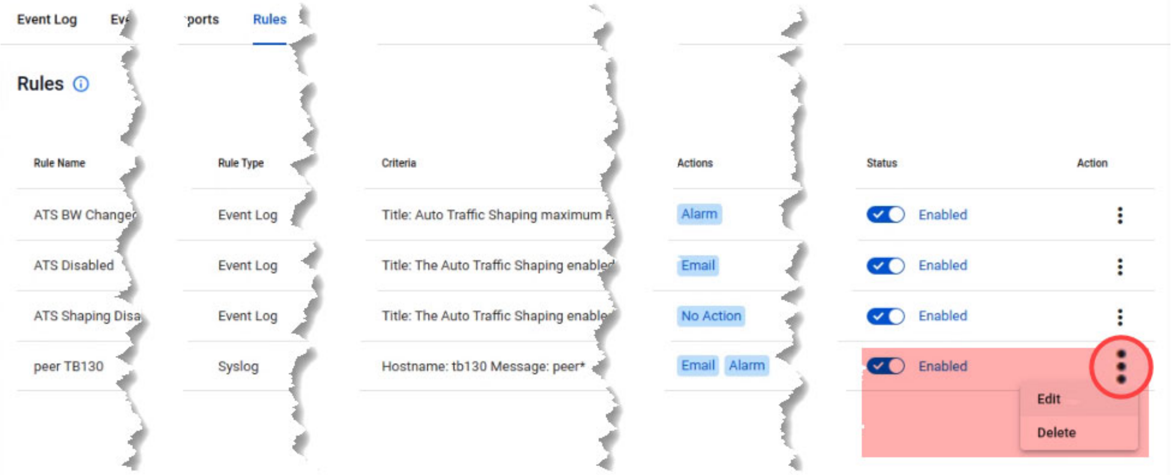
Trigger Interval

5 mins 7

Action 2

Dismissible Alarm 8

To view a list of syslog rules, navigate to the Rules tab page. Here, you can also disable a rule, update its settings, or delete it.

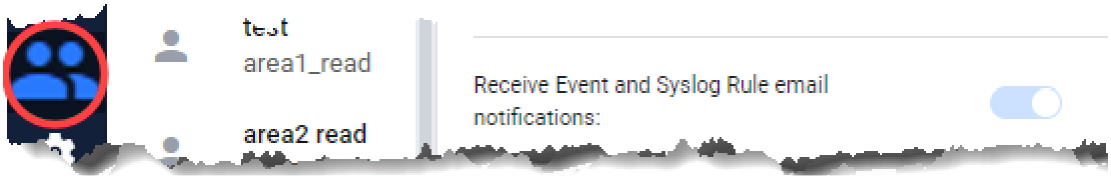


Rules

Rule Name	Rule Type	Criteria	Actions	Status	Action
ATS BW Change	Event Log	Title: Auto Traffic Shaping maximum	Alarm	Enabled	⋮
ATS Disabled	Event Log	Title: The Auto Traffic Shaping enabled	Email	Enabled	⋮
ATS Shaping Disa	Event Log	Title: The Auto Traffic Shaping enable	No Action	Enabled	⋮
peer TB130	Syslog	Hostname: tb130 Message: peer*	Email Alarm	Enabled	⋮

Syslog rule - email notification

On the **user management** page, a new toggle button enabled by default will be present for all users. This setting determines whether a user will receive an email when a syslog matches a syslog rule configured with email notification.



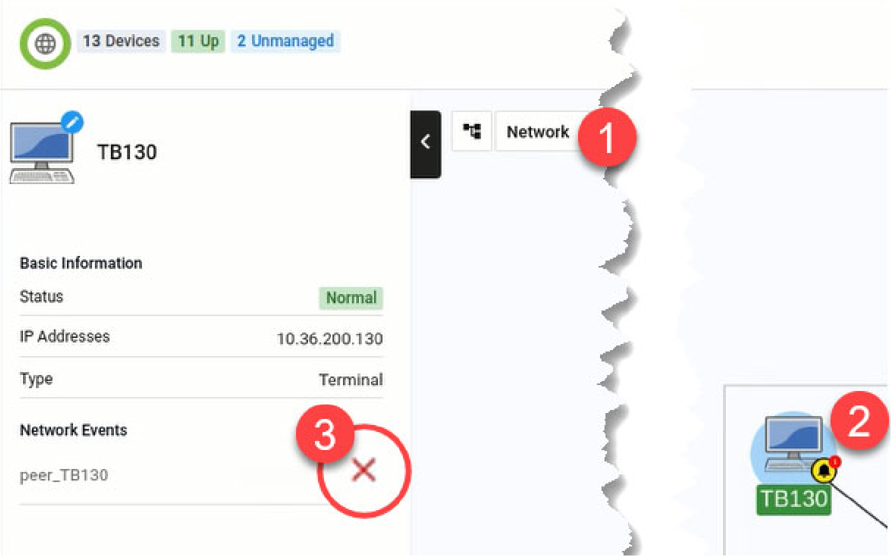
test
area1_read
area2 read

Receive Event and Syslog Rule email notifications:

As a non-admin user, you can change this setting only for yourself. Admin users can enable/disable email notification for all users.

Syslog rule - dismissible alarm

A bell icon will appear on the network map for a device that sends a syslog matching a rule. Click on the bell icon to open up the side panel displaying its syslog details. Here, you may also choose to dismiss the alarm.



Basic Information

Status	Normal
IP Addresses	10.36.200.130
Type	Terminal

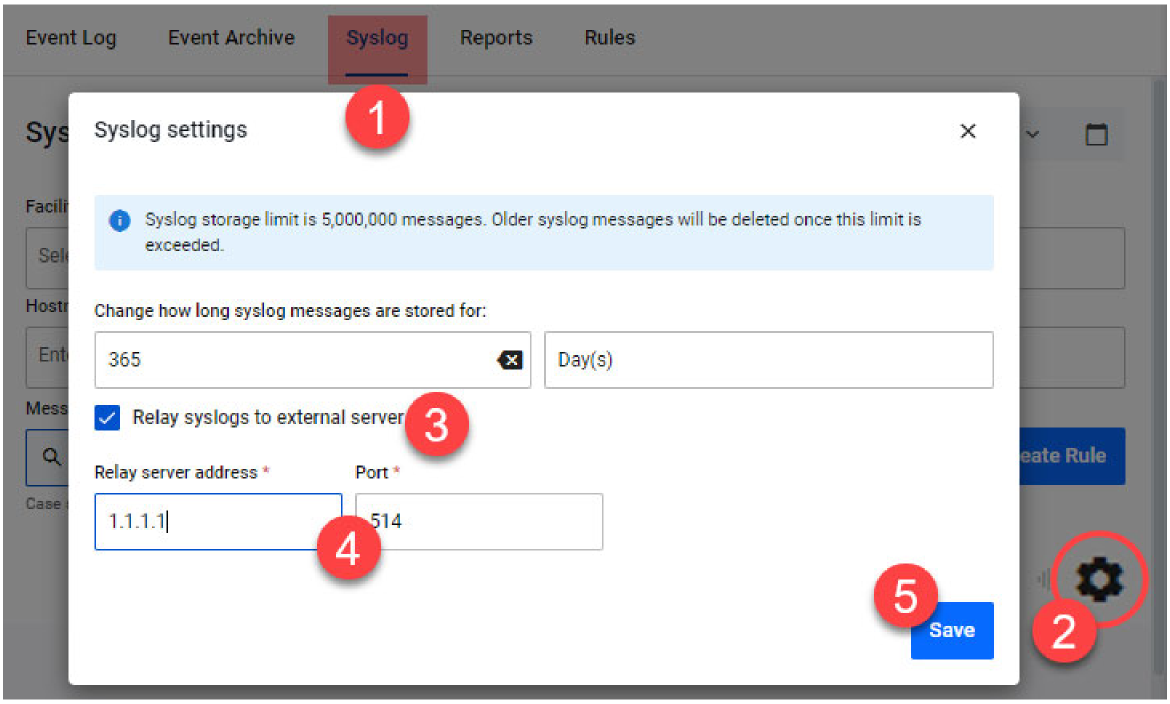
Network Events

peer_TB130

Syslog forwarding

As an admin user, you will have the option to configure syslog forwarding to an external server. This functionality forwards all received syslog messages to a specified syslog server, regardless of any rules configured. Only one external syslog server is supported.

Note: The source address of a syslog cannot be retained to its external server.



Syslog settings

Syslog storage limit is 5,000,000 messages. Older syslog messages will be deleted once this limit is exceeded.

Change how long syslog messages are stored for: 365 Day(s)

☑ Relay syslogs to external server

Relay server address * 1.1.1.1

Port * 514

1. From the Events menu, navigate to the **Syslog** tab page.
2. Click on the Syslog settings gear icon.
3. Check the **Relay syslogs to external server** option.
4. Enter the relay server address and port number.
5. Click **Save**.

AMF Security (AMF-Sec) support

The existing alarm notification supports both AlliedWare Plus devices and wireless devices by leveraging on syslog messages from the AMF-Sec server. Vista Manager EX shows alarms on the integrated map for both blacklist and whitelist security events on AlliedWare Plus devices.

Configure all your AMF-Sec servers to send syslog messages to Vista Manager EX. All syslog messages from the AMF-Sec servers will then appear on the **Event > Syslog** page.

Note: In order to process syslog messages from the AMF-Sec server, Vista Manager EX will have some built-in event rules not visible to users. Because of this, if a user creates a rule with the same name in the event log or syslog table, an error message will display: **"Duplicate rule name used. Note may be a duplicate of a hidden system rule name."**

Alarms on the integrated map

Vista Manager EX will convert only specific actions that match AMF-Sec syslog messages into alarms (high severity event logs) and display them on the map. These specific actions are:

- Blacklist
  - Security Block
  - LinkDown
  - Quarantine VLAN
  - Security Logging (no-action, reporting only)
- Whitelist
  - Auth Failed (deny)

Any other syslog messages from the AMF-Sec server not mentioned above will not be converted. This means the user will not be able to see successful notification events in the Vista Manager event log table, but those events are present in the Syslog tab page.

The alarms will be associated with devices based on IP addresses and hostnames from the AMF-Sec syslog message. If one AMF-Sec syslog message can be associated with multiple devices, all devices will have their own alarm. If an alarm cannot be associated with any device on the map, it will not be visible on the map.

Note: Unmanaged devices are not always visible on the map, such as TQ devices without the AWC plug-in. In this case, alarms will still be associated to the TQ device, but can only be viewed by zooming into the map. Alternatively, add the AWC plug-in to manage the TQ which then makes it visible by default.

The alarms will keep showing on the map until either

- a user dismisses them proactively, or
- a recovery AMF-Sec syslog message dismisses them automatically.

Users with read/write permissions to the associated device can dismiss the alarms in 2 ways:

- **from the event log table**, or
- **from the side panel of the map**.

Alarm recovery

When a user performs an action in the AMF-Sec server, the AMF-Sec server will send syslog messages to Vista Manager EX to indicate a status change on the alarm.

Vista Manager EX automatically dismisses an alarm and removes it from the map, if they are event recovery types such as:

- DISCONNECT
- ACCEPT

A “recovered” event log will then be generated with detailed information.

Feature limitations

There are some feature limitations to take note of:

- As syslog messages are based on UDP protocol, this functionality can be unreliable at times, meaning messages could sometimes go missing.
- In the event that the Vista Manager EX syslog server goes down, syslog messages lost during the downtime will not be recoverable.
- If the AMF-Sec server changes its syslog format, this feature will fail to work as there is no way to detect such failures.
- AMF-Sec alarms that depend on the DISCONNECT action will not be removed when the parent device reboots or leaves the network. This is because the AMF-Sec server does not send a corresponding disconnect message with a device reboot, therefore causing the alarms to remain on the map.
- AMF-Sec will not send syslog messages for the IP-FILTER action. If sourced from a non-AMF device, Vista Manager EX will not be able to detect this action.
- Some changes have been applied to the event messages from the original blacklist feature. Therefore for any event filtering relying on event messages, the existing event filter may appear broken after upgrading to version 3.7.0.

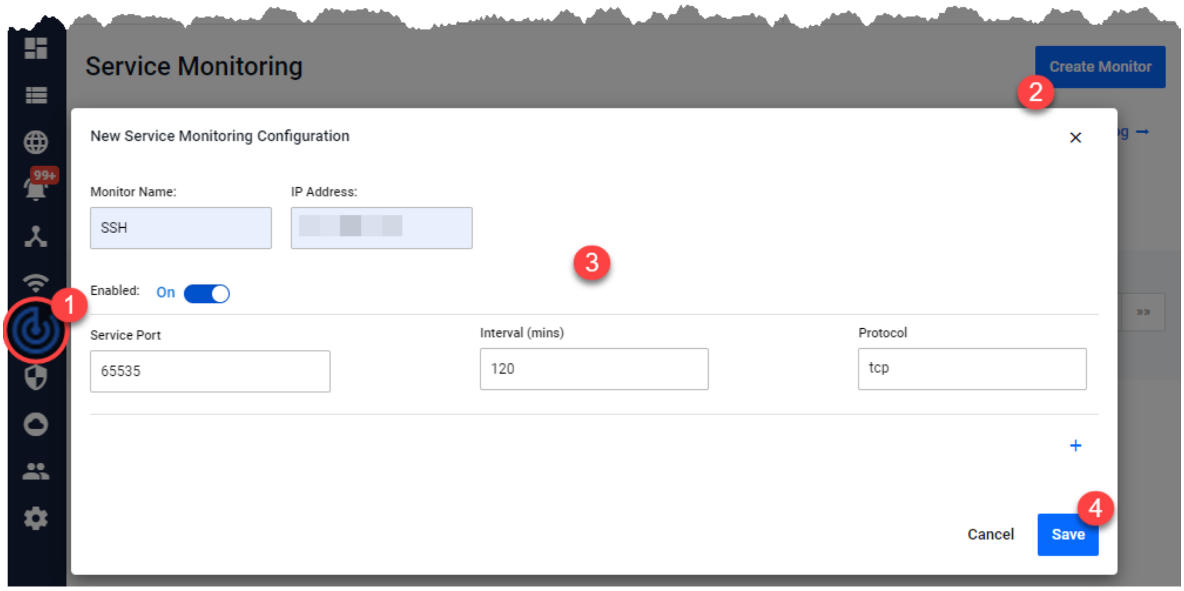
Service monitoring

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:

1. Open **Service Monitoring** in Vista Manager.
2. Click on **Create Monitor.**
3. 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
4. Click **Save**.



Service Monitoring

New Service Monitoring Configuration

Monitor Name: SSH

IP Address:

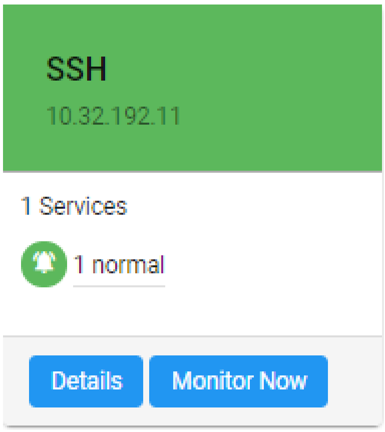
Enabled: On

Service Port: 65535

Interval (mins): 120

Protocol: tcp

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



SSH

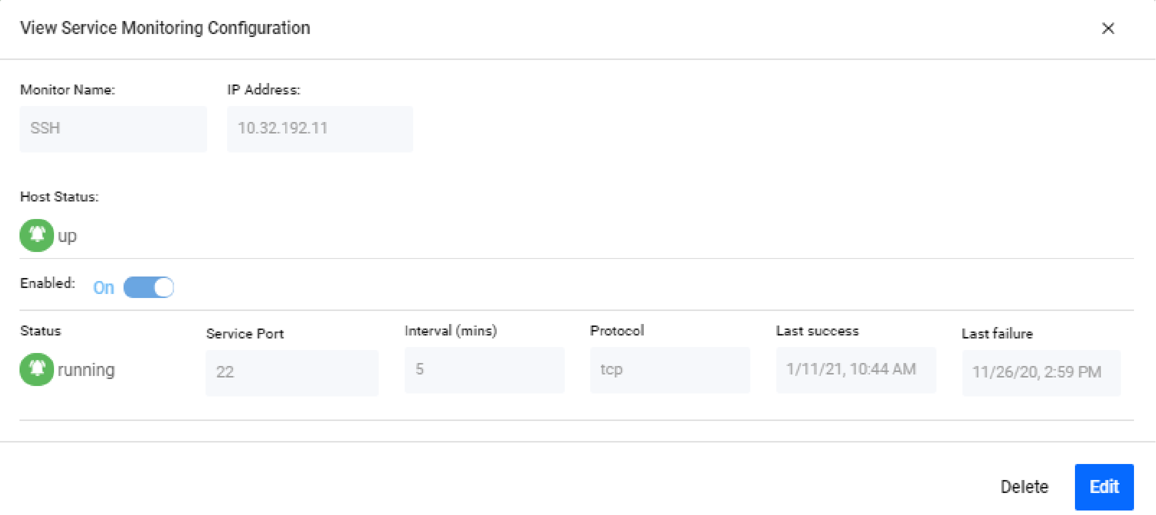
10.32.192.11

1 Services

1 normal

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.



View Service Monitoring Configuration

Monitor Name: SSH

IP Address: 10.32.192.11

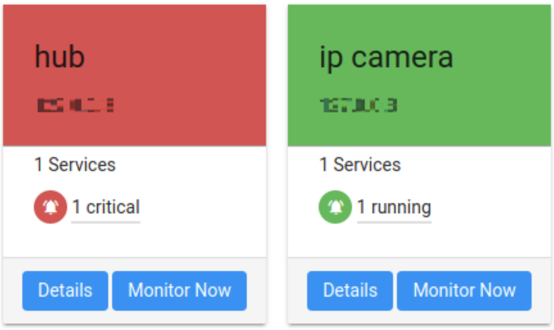
Host Status: up

Enabled: On

Status	Service Port	Interval (mins)	Protocol	Last success	Last failure
running	22	5	tcp	1/11/21, 10:44 AM	11/26/20, 2:59 PM

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.

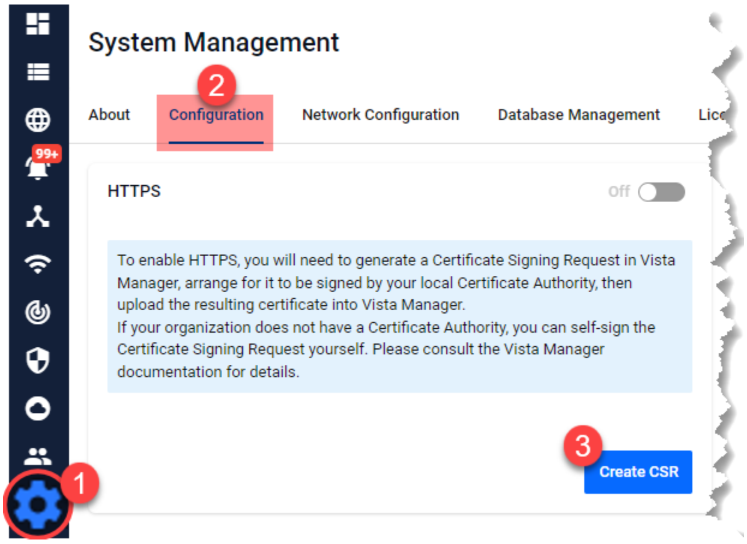
Vista Manager EX can generate a Certificate Signing Request (CSR) which you can then submit to a Certificate Authority (CA). The CA will then give you a signed certificate which you can import back into Vista Manager EX. Note that both the application's and CA's private key are never transmitted; this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

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

Note: Only certificates generated from Vista Manager's CSR can be uploaded into Vista Manager.

To enable HTTPS:

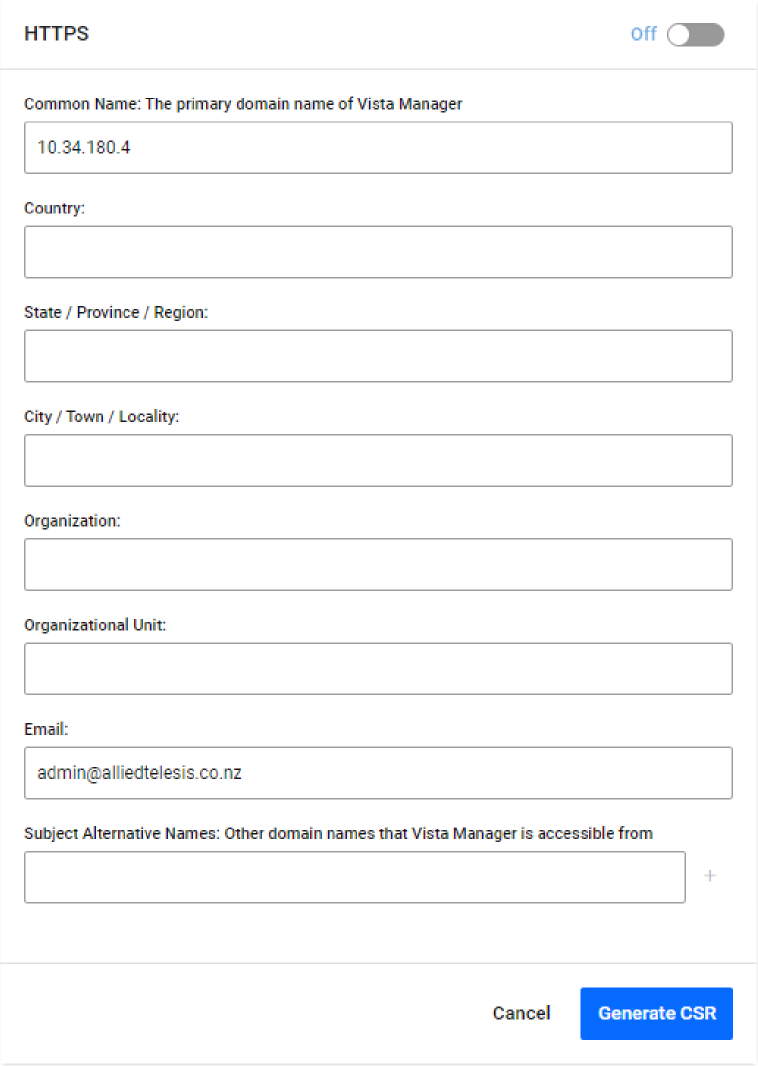
1. In Vista Manager, open the System Management menu item.
2. Then go to the Configuration tab.
3. Click on **Create CSR**.



System Management

To enable HTTPS, you will need to generate a Certificate Signing Request in Vista Manager, arrange for it to be signed by your local Certificate Authority, then upload the resulting certificate into Vista Manager.
If your organization does not have a Certificate Authority, you can self-sign the Certificate Signing Request yourself. Please consult the Vista Manager documentation for details.

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



HTTPS

Common Name: The primary domain name of Vista Manager

10.34.180.4

Country:

State / Province / Region:

City / Town / Locality:

Organization:

Organizational Unit:

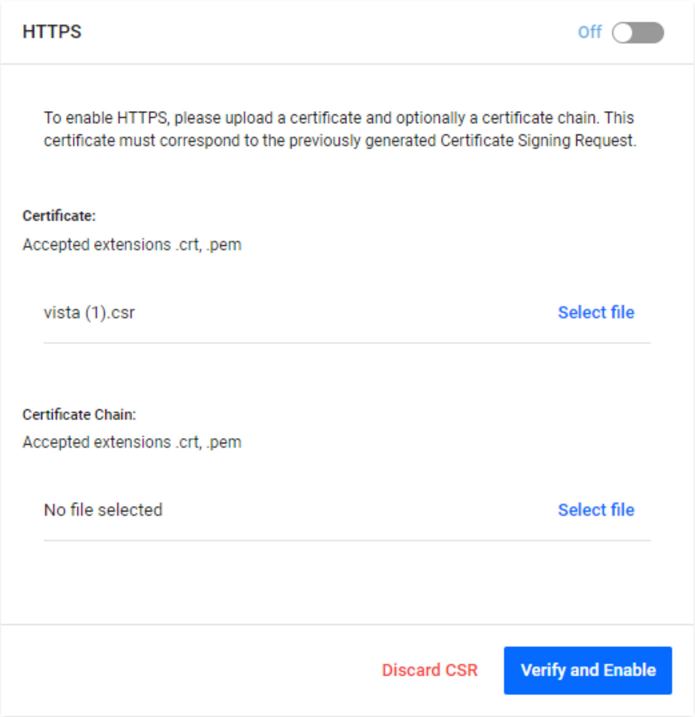
Email:

admin@alliedtelesis.co.nz

Subject Alternative Names: Other domain names that Vista Manager is accessible from

- 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.



To enable HTTPS, please upload a certificate and optionally a certificate chain. This certificate must correspond to the previously generated Certificate Signing Request.

Certificate:

Accepted extensions .crt, .pem

vista (1).csr

Certificate Chain:

Accepted extensions .crt, .pem

No file selected

- 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:

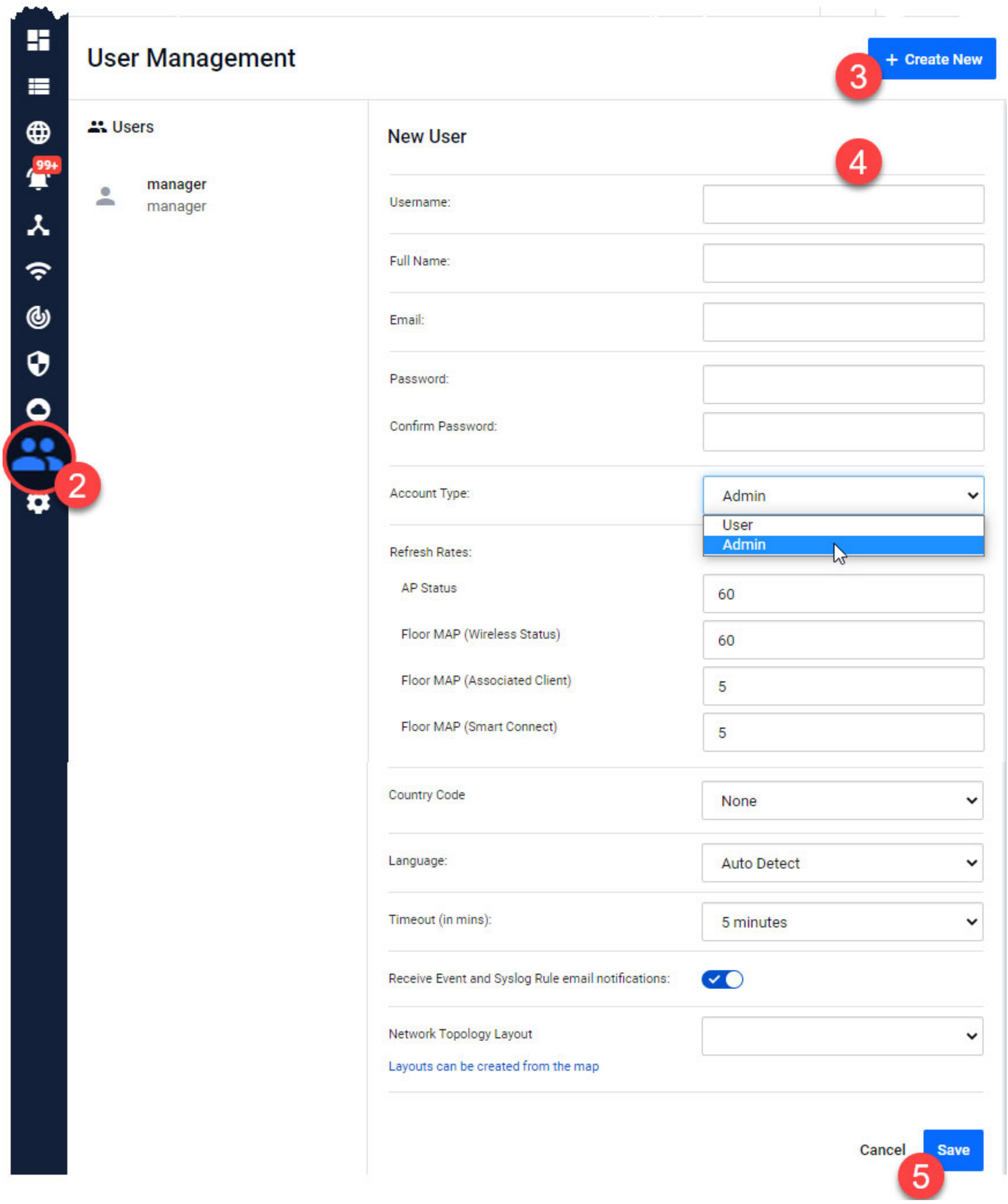
- https://<ip address>
- https://<ip address>:443

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).



User Management

Users

manager
manager

New User

Username:

Full Name:

Email:

Password:

Confirm Password:

Account Type: Admin

Refresh Rates:

AP Status: 60

Floor MAP (Wireless Status): 60

Floor MAP (Associated Client): 5

Floor MAP (Smart Connect): 5

Country Code: None

Language: Auto Detect

Timeout (in mins): 5 minutes

Receive Event and Syslog Rule email notifications: ✓

Network Topology Layout:

Layouts can be created from the map

Create an account

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

Edit an existing account

1. Log in with an Administrator account type.
2. Select **User Management** from the menu item.
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 when complete.

Set the time-out for an account

1. Log in with an Administrator account type.
2. Select **User Management** from the menu item.
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 when complete.

Delete an existing account

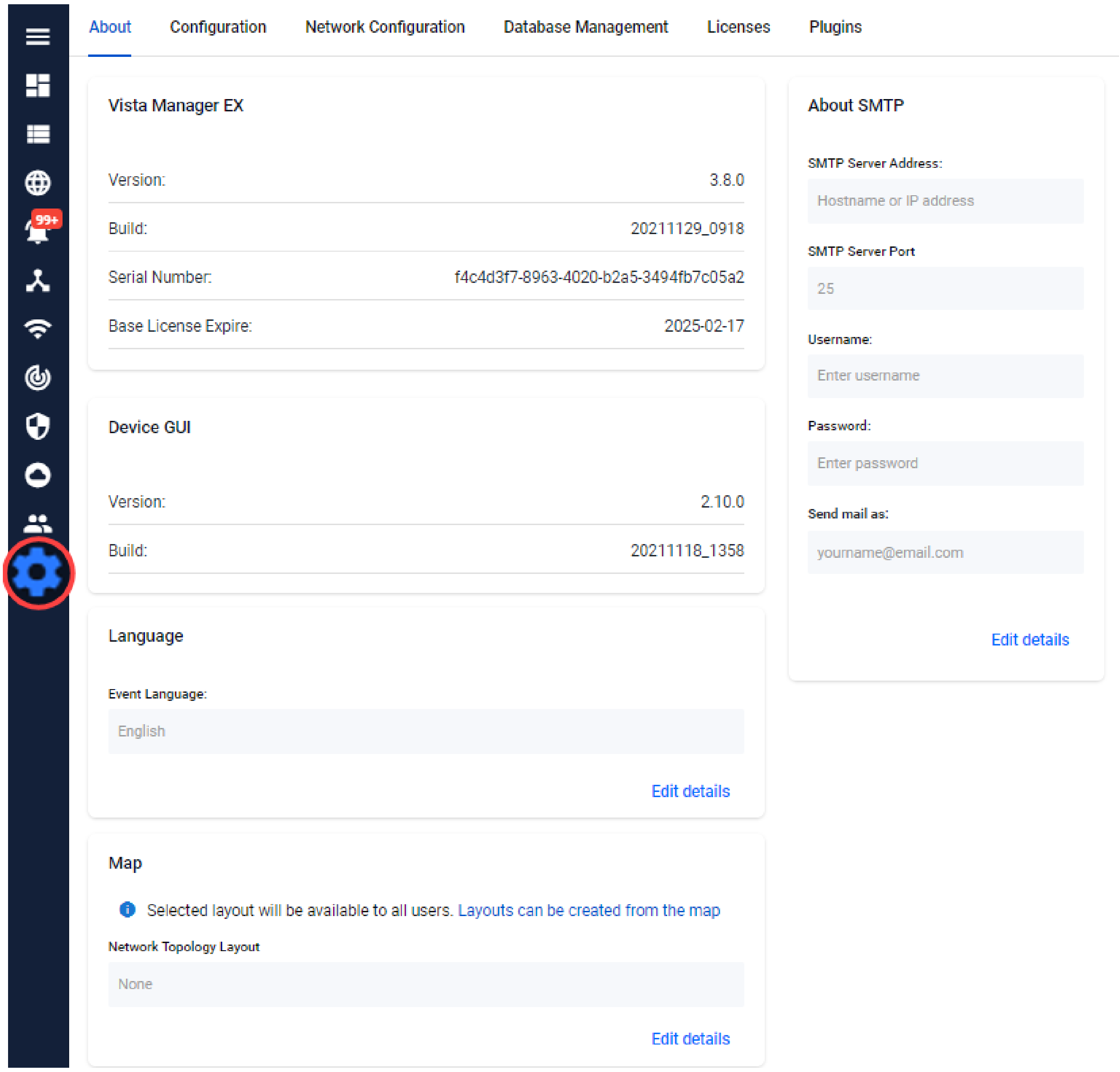
1. Log in with an Administrator account type.
2. Select **User Management** from the menu item.
3. Select the account you want to delete from the account list.
4. Click the **Delete** button.
5. From the Delete User dialog box click the **Delete** button again.

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
- Username and Password can be changed for a network
- The Vista Manager EX database can be backed up, restored, or reset to the factory default
- The event language and network map layout can be changed
- The SMTP Server Username, Password and email address can be changed



Vista Manager EX

Version: 3.8.0

Build: 20211129_0918

Serial Number: f4c4d3f7-8963-4020-b2a5-3494fb7c05a2

Base License Expire: 2025-02-17

Device GUI

Version: 2.10.0

Build: 20211118_1358

Language

Event Language: English

Edit details

Map

Selected layout will be available to all users. Layouts can be created from the map

Network Topology Layout: None

Edit details

About SMTP

SMTP Server Address: Hostname or IP address

SMTP Server Port: 25

Username: Enter username

Password: Enter password

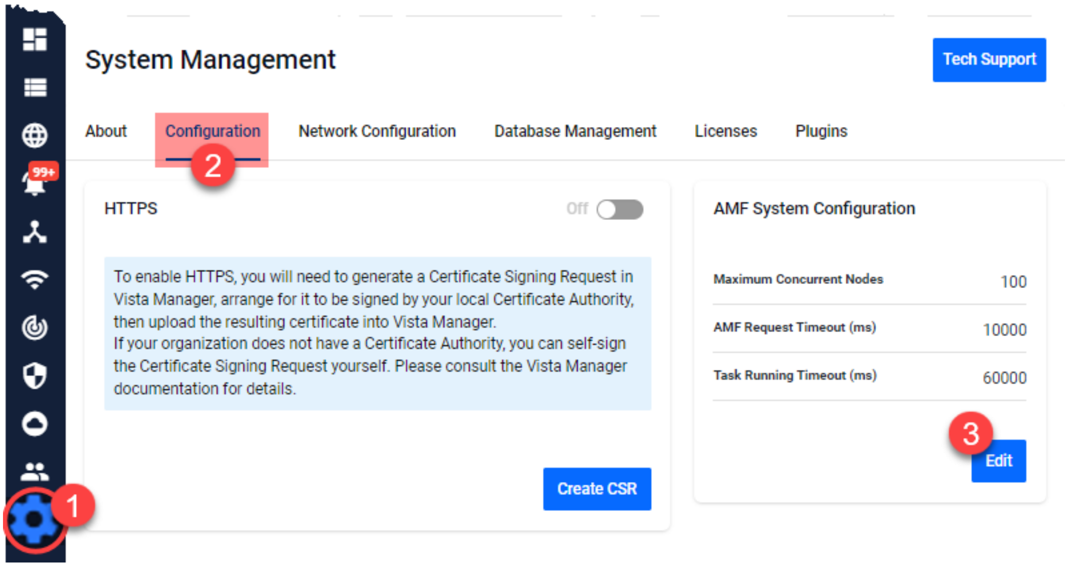
Send mail as: yourname@email.com

Edit details

Changing the AMF system configuration settings

You may need to change the AMF system configuration settings in Vista Manager EX. This was previously done by a support engineer onsite to resolve various network errors that involved changing variables in the configuration file. An event log will be generated after you have applied the new values. To change these settings:

1. Navigate to the **System Management** menu item.
2. Select the **Configuration** tab.
3. Under AMF System Configuration, click on the **Edit** button.
4. Click **Save** when complete.



To enable HTTPS, you will need to generate a Certificate Signing Request in Vista Manager, arrange for it to be signed by your local Certificate Authority, then upload the resulting certificate into Vista Manager.
If your organization does not have a Certificate Authority, you can self-sign the Certificate Signing Request yourself. Please consult the Vista Manager documentation for details.

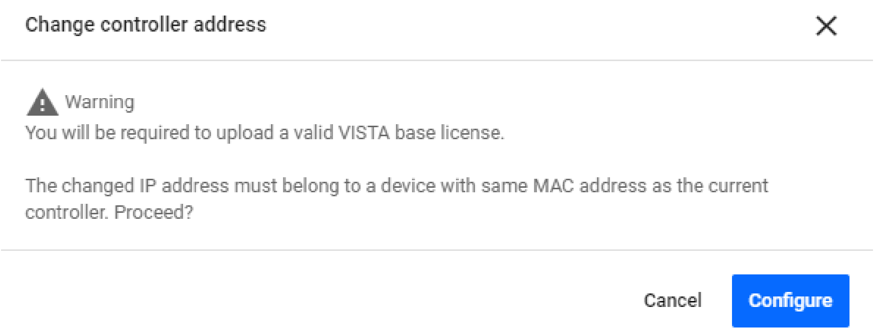
Maximum Concurrent Nodes	100
AMF Request Timeout (ms)	10000
Task Running Timeout (ms)	60000

Note: No restarting is required.

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.



Change controller address

⚠ Warning

You will be required to upload a valid VISTA base license.

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

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.

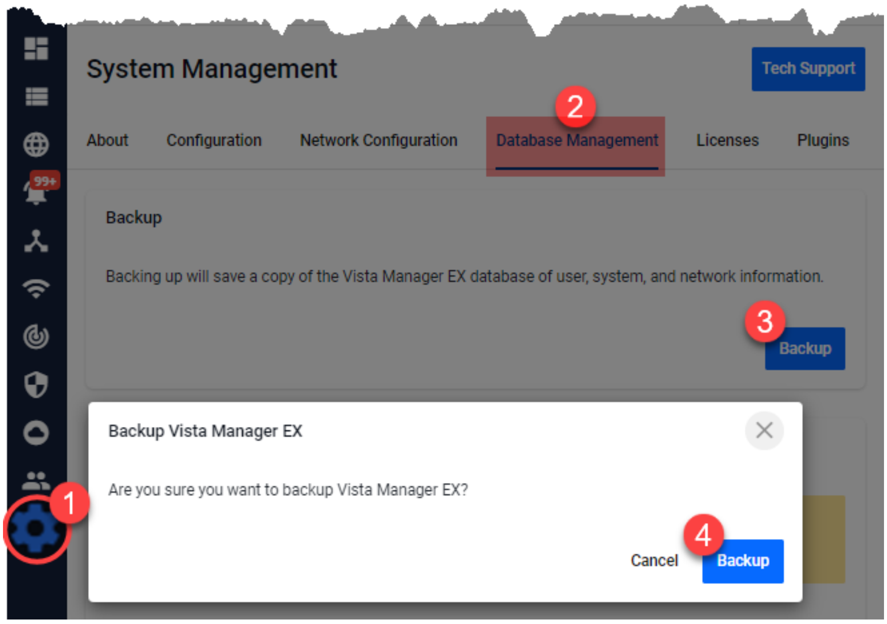
Note: The changed IP address must belong to a device with the same MAC address as the current controller.

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. Navigate to the **System Management** menu item.
2. Then go to the **Database Management** tab.
3. Click on the **Backup** button in the Backup pane.
4. Click **Backup** again to confirm you wish to make a backup.



System Management

Backup

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

Backup Vista Manager EX

Are you sure you want to backup Vista Manager EX?

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

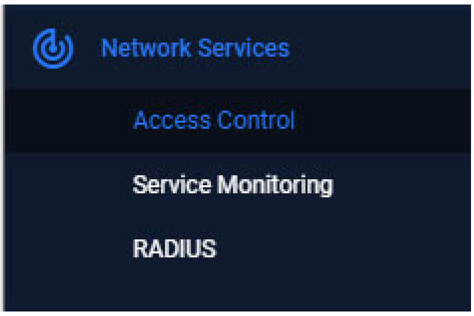
Note: Restoring Vista Manager backups from a newer version into an older version is not supported. It is not possible, for example, to restore a backup made in Vista Manager 3.8.0 into a Vista Manager 3.9.0 installation.

Access Control List matrix

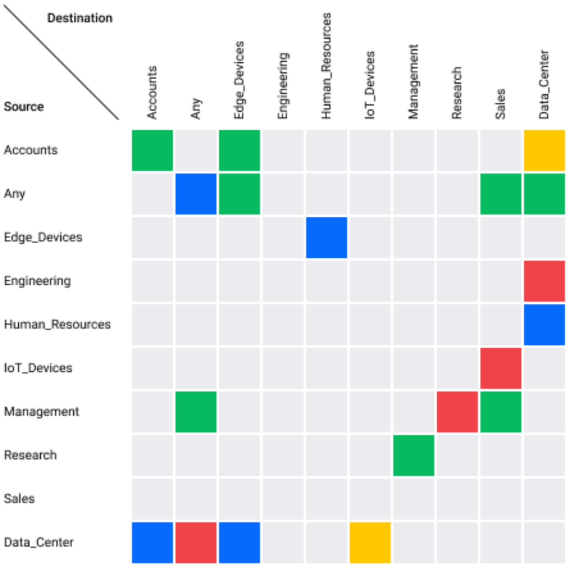
The Access Control List matrix provides a visual representation of the Access Control Lists (ACLs) applied to your network.

Using the Access Control List matrix

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



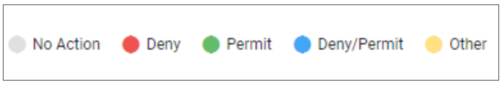
This displays the Access Control List matrix.



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

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

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

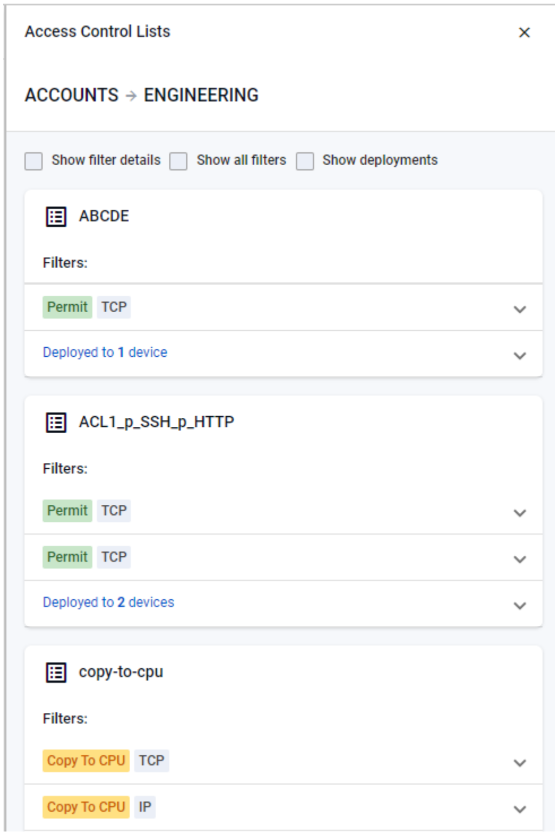


● No Action ● Deny ● Permit ● Deny/Permit ● Other

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

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

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



Access Control Lists ×

ACCOUNTS → ENGINEERING

□ Show filter details □ Show all filters □ Show deployments

ABCDE

Filters:

Permit TCP

Deployed to 1 device

ACL1_p_SSH_p_HTTP

Filters:

Permit TCP

Permit TCP

Deployed to 2 devices

copy-to-cpu

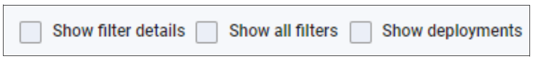
Filters:

Copy To CPU TCP

Copy To CPU IP

There are several check boxes that provide additional information.

Filters and deployments



□ Show filter details □ Show all filters □ Show deployments

Selecting the check box:

- **Show filter details** - displays additional information about the filters
- **Show all filters** - display all filters contained in the ACL
- **Show deployments** - displays which devices the filters are deployed to

By default, only the filters that exactly match the source/destination cells are displayed.

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

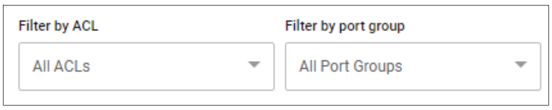
An ACL can contain multiple filter lines. Each line starts with a single action (Permit, Deny, etc), then the filter type, followed by the source and destination matching criteria. Rather than using a host group, you can use 'any' for a wildcard match for source and/or destination.

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

- icmp
- ip
- proto
- tcp
- udp

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

Filter by ACL and port group



Filter by ACL: All ACLs

Filter by port group: All Port Groups

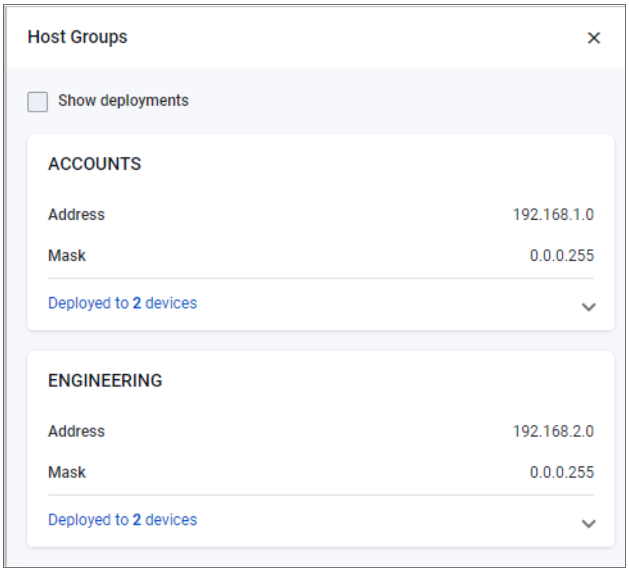
Two selection filters are available above the Access Control List matrix.

- **Filter by ACL** - this allows you to quickly see where a single ACL exists on the matrix.
- **Filter by port group** - this lets you filter out all cells containing an ACL that does not use the specified ACL port group. Named ACL port groups contain port matching rules. For example, a port group called 'HTTP' could contain a rule to match port 80. The name given to host groups and port groups is user-defined, but should describe the group's content.

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

Host and port groups

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



ACCOUNTS

Address	192.168.1.0
Mask	0.0.0.255

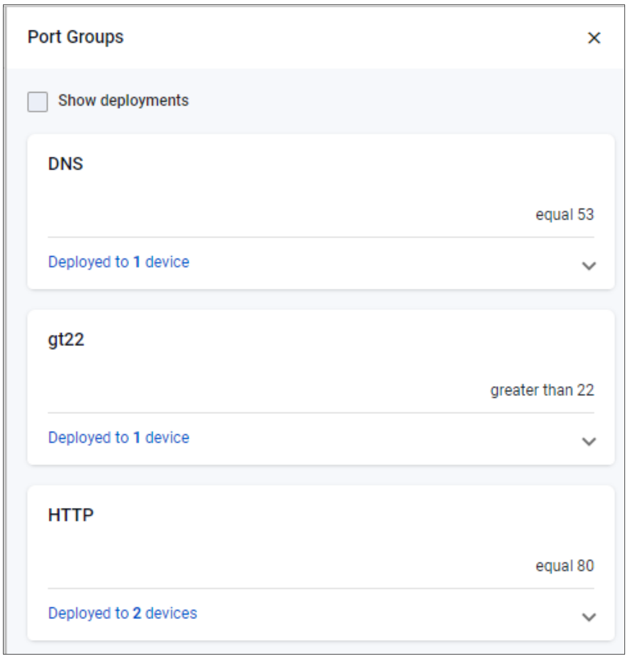
Deployed to 2 devices

ENGINEERING

Address	192.168.2.0
Mask	0.0.0.255

Deployed to 2 devices

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



Port Groups

□ Show deployments

DNS

equal 53

Deployed to 1 device

gt22

greater than 22

Deployed to 1 device

HTTP

equal 80

Deployed to 2 devices

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

Creating new hardware ACLs

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

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

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

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

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

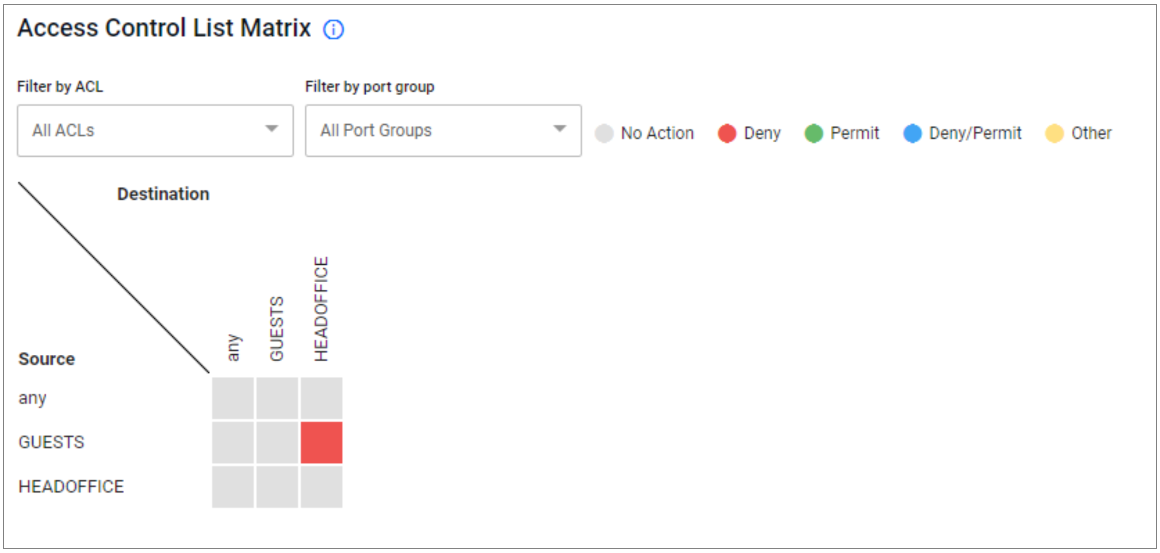
3. Create the hardware ACL to deny TCP packets matching port group SSH from source host group GUESTS to destination host group HEADOFFICE.

```
awplus(config)# access-list hardware Deny_SSH_GUESTS_to_HEADOFFICE

awplus(config-ip-hw-acl)# deny tcp host-group GUESTS
host-group HEADOFFICE port-group SSH

awplus(config-ip-hw-acl)# exit
```

4. Deploy the ACL to a switchport.

```
awplus(config)# interface port1.0.1

awplus(config-if)# access-group Deny_SSH_GUESTS_to_HEADOFFICE
```

This ACL would be shown like this on the ACL Matrix:



Access Control List Matrix ⓘ

Filter by ACL: All ACLs

Filter by port group: All Port Groups

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

Source \ Destination	any	GUESTS	HEADOFFICE
any			
GUESTS			🟥
HEADOFFICE			

Converting existing hardware ACLs

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

```
awplus(config)# access-list hardware 3005_My_ACL

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 10

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 20

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 30

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 40

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 50

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 60

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 70

awplus(config-ip-hw-acl)# deny tcp 1.1.1.1/32 any eq 80

awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 10

awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 20
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 30
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 40
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 50
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 60
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 70
awplus(config-ip-hw-acl)# deny tcp 2.2.2.2/32 any eq 80
```

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

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

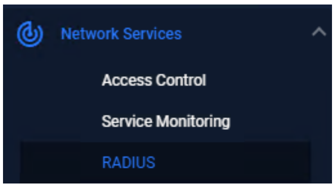
```
awplus(config)# acl-group ip address My_Host_ACL_Group
awplus(config-ip-host-group)# ip 1.1.1.1/32
awplus(config-ip-host-group)# ip 2.2.2.2/32
awplus(config)# acl-group ip port My_Port_ACL_Group
awplus(config-ip-port-group)# eq 10
awplus(config-ip-port-group)# eq 20
awplus(config-ip-port-group)#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

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

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

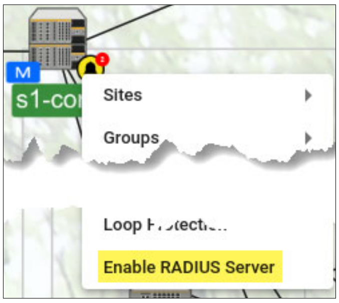
RADIUS server support

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



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

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



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

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

The **Users** tab allows you to:

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

The **Group** tab allows you to:

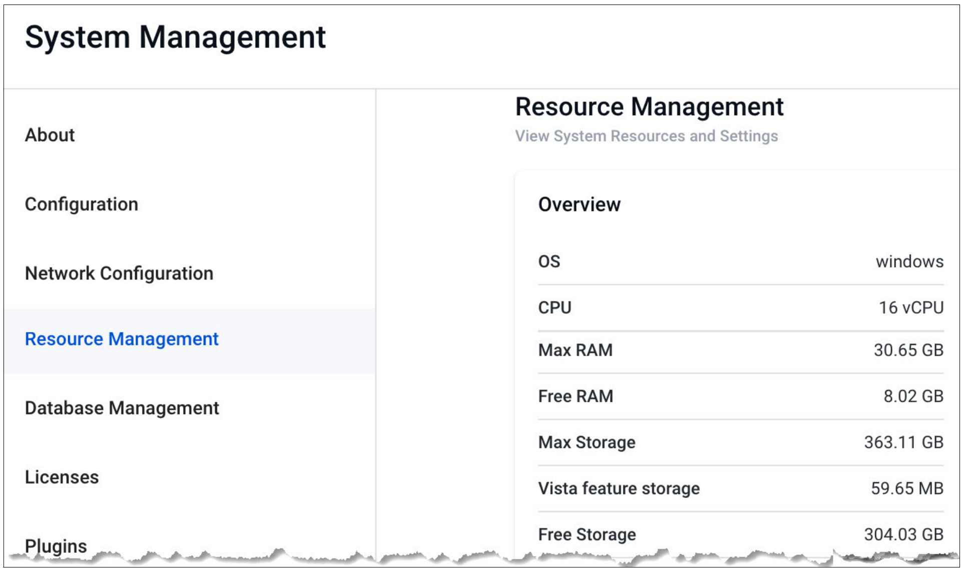
- add/edit/delete groups to the local RADIUS server of a selected device
- optionally specify the Dynamic VLAN of a group
- manage the Dynamic VLAN of a group
- optionally specify the RADIUS attributes of a group
- manage/change the RADIUS attributes of a group
- see an error if attempting to delete a group that has users assigned on the device.
- The RADIUS group attributes allow you to:
  - see all attributes for a group
  - add/delete one or multiple attributes to a group.

The **NAS** tab allows you to:

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

Resource management

In small and large network environments, Vista Manager needs to scale accordingly. To cater to this scenario, use the **Resource Management** page, under the **System Management** menu.



System Management

About

Configuration

Network Configuration

Resource Management

Database Management

Licenses

Plugins

Resource Management

View System Resources and Settings

Overview

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

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

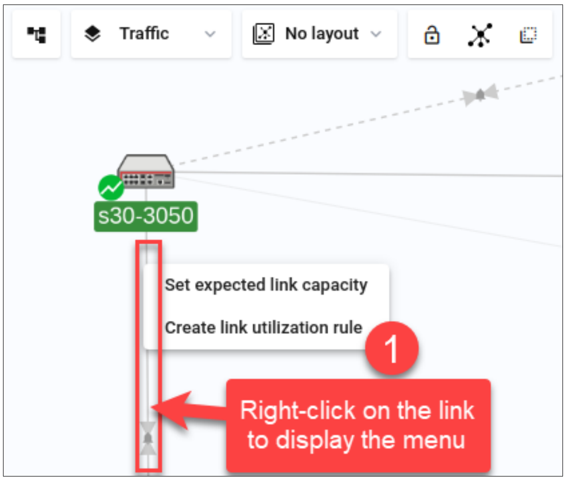
- of Vista Manager on your machine and how much is available
- of Vista Manager inside a container and how much is available
- the resource consumption of each running feature
- how many event logs/syslogs are stored and how much storage they take up (total counts are only available for event logs)

Intelligent networking and data analysis

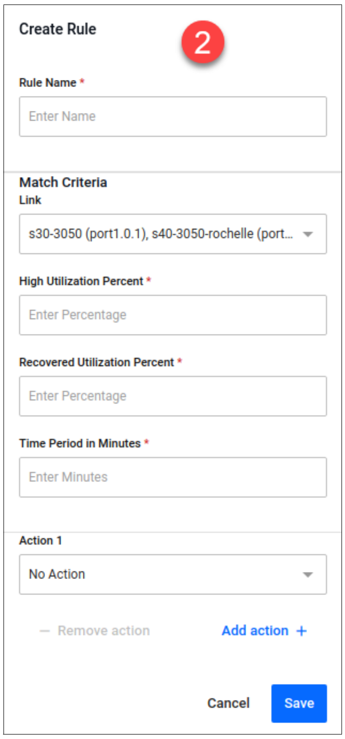
Vista Manager provides an intelligent networking and data analysis functionality that suggests actions to improve your network or solve network issues. As a user, you are:

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

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



Right-click on the link to display the menu



Create Rule

Rule Name *

Enter Name

Match Criteria

Link

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

High Utilization Percent *

Enter Percentage

Recovered Utilization Percent *

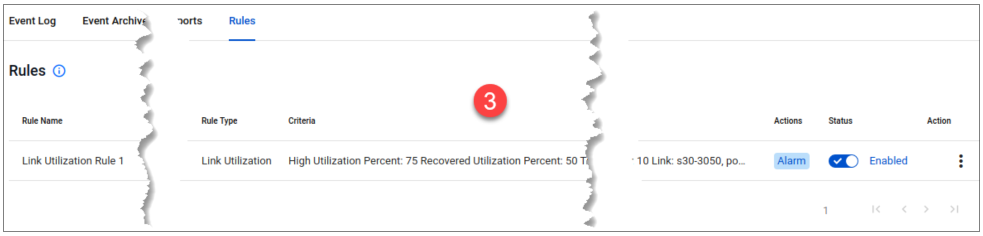
Enter Percentage

Time Period in Minutes *

Enter Minutes

Action 1

No Action



Rules

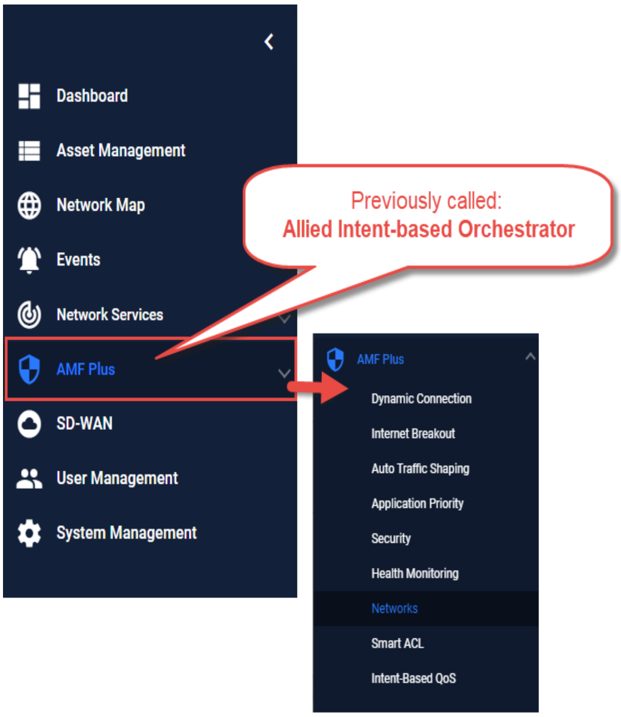
Rule Name	Rule Type	Criteria		Actions	Status	Action
Link Utilization Rule 1	Link Utilization	High Utilization Percent: 75 Recovered Utilization Percent: 50 T	' 10 Link: s30-3050, po...	Alarm	Enabled	⋮

Using AMF Plus

Introduction

Allied Telesis Autonomous Management Framework™ Plus (AMF Plus), is the new name for the Intent-based Orchestrator (AIO) feature, replacing the AIO menu. AMF Plus provides network optimization, automation, management, and visualization. The uniquely designed intent-based configuration, reporting, and map facilities of Vista Manager EX make these powerful tools simple to configure, initiate, and manage. AMF Plus offers automation of branch security and WAN bandwidth management.

The **AMF Plus** feature is located in the left-hand menu.



For this feature to become fully available to you and for all menu items to be activated, install the feature license. The AMF Plus license is not part of the base Vista Manager EX license. But, it is included in the 90-day trial license. If you want to continue using AMF Plus after the 90-day trial license expires, you need to install a feature license for it.
Please contact your authorized Allied Telesis salesperson for assistance.

More about AMF Plus requirements and licensing

The following requirements are needed to run AMF Plus:

- AlliedWare Plus firmware version 5.5.2-2.3 or later running on AMF masters and controllers.
- AMF Plus license for AMF masters and controllers.
- Vista Manager EX version 3.10.1 or later.

How many AMF Plus licenses do I need?

An AMF Plus license manages up to 10 nodes:

- If your network has 75 nodes, then 8 licenses are required.
- A license is available for either a 1or 5 year period.
- The license code name is **AT-SW-APM10**-xYR

See the AMF Plus datasheet for full licensing details.

Can I mix AMF and AMF Plus licenses?

It is possible for an AMF Master/Controller to have a combination of both AMF and AMF Plus node/area licenses.

The Vista Manager AMF Plus functionality requires that **only** AMF Plus licenses are present before the Vista Manager AMF Plus functionality is available. If there are any AMF masters with any AMF node licenses or any AMF controllers with AMF area licenses, then:

- Vista Manager will not display the AMF Plus functionality.
- Both AMF and AMF Plus node/area licenses will count towards the total number of AMF nodes/areas available.

When is the AMF Plus menu visible in Vista Manager EX?

The AMF Plus menu replaces the AIO menu in Vista Manager when all the AMF Masters and AMF Controllers have:

- An AMF Plus Controller/Master license on all Master and Controllers

  AND

- No AMF Controller/Master licenses applied or AMF Controller/Master licenses are disabled with the **atmf amfplus-license-only** command.

Note: You only need to change to AMF Plus licenses if you want to manage more nodes, or want to use the features in the new AMF Plus menu. Existing AMF licenses remain valid.

AMF Plus tools

The AMF Plus feature is made up of several tools to help you manage your network:

- "Dynamic Connection" on page 120
- "Internet Breakout" on page 125
- "Auto Traffic Shaping" on page 128
- "Application Priority" on page 130
- "Security" on page 135
- "Health Monitoring" on page 139
- "Smart ACL" on page 144
- "Intent-based QoS" on page 151

Dynamic Connection

This feature lets you use the simplicity of drag-and-drop on the network map, to create new VPN tunnels between the AR-Series devices (firewalls or routers) at different locations across your WAN.

- Point-to-point tunnels require a source device and destination device.
- Point-to-multipoint tunnels require a source device and multiple destination devices.

Note: The AR1050V does not support Dynamic Connection.

For this feature to be fully functional, apart from installing the AIO license, you must also have either administrator access or write permission on a device.

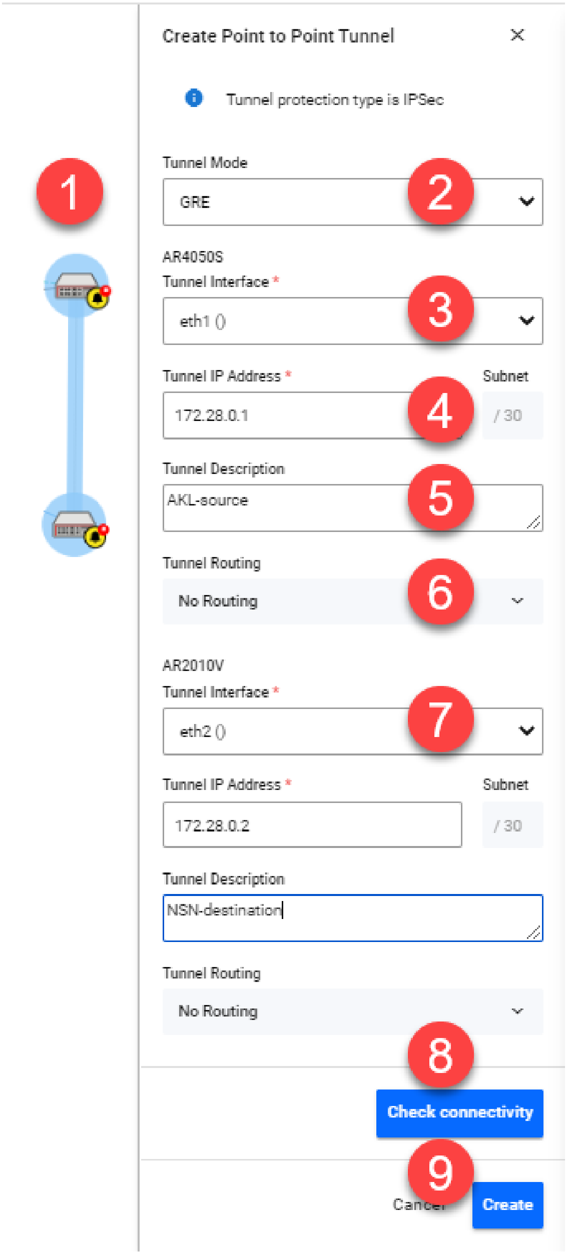
To create a tunnel, both devices must be part of the AMF network, support GRE tunnels and be running firmware version AlliedWare Plus 5.5.0-2.x or later.

You cannot create multiple tunnels with the same source and destination interface pair (e.g. eth1). Split up the interface if you wish to create more than one tunnel, for example, split eth ports into sub-interfaces. You may create another tunnel with the same source interface as long as the destinations are on different devices.

All tunnels are encrypted with IPSec to secure your WAN traffic. Each tunnel will have a different crypto key with a unique name.

Creating tunnels

Option 1: Create a Point-to-Point Tunnel



Create Point to Point Tunnel ×

Tunnel protection type is IPSec

Tunnel Mode: GRE

AR4050S

Tunnel Interface *: eth1 ()

Tunnel IP Address *: 172.28.0.1 Subnet: / 30

Tunnel Description: AKL-source

Tunnel Routing: No Routing

AR2010V

Tunnel Interface *: eth2 ()

Tunnel IP Address *: 172.28.0.2 Subnet: / 30

Tunnel Description: NSN-destination

Tunnel Routing: No Routing

1. Use the pencil icon to draw a line between devices (firewalls/routers) at the two locations you wish to connect with a new VPN tunnel.
2. Next, set up tunnel options. Select tunnel mode.
3. Select an interface for the tunnel to be on.
4. Vista Manager EX generates the tunnel interface IP addresses. The subnet prefix is /30.

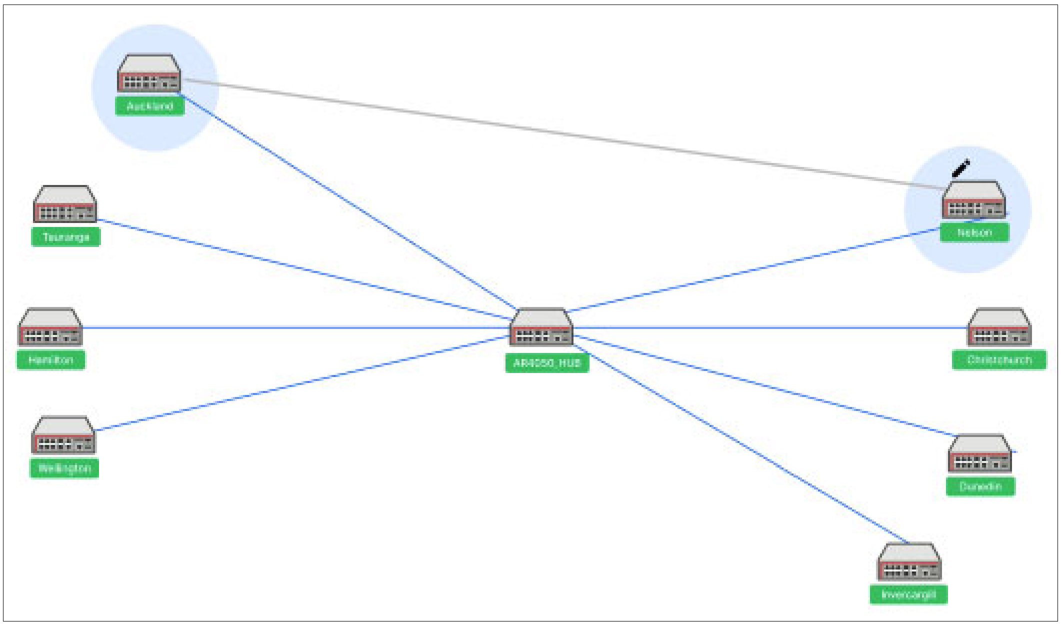
Note: If you choose your own IP address, it must be in the same subnet and must not be used on another interface on those devices.

5. Enter a description name for the tunnel.
6. Configure tunnel routing.

Note: The options here are default or static. You may enter IP addresses for each end of the tunnel by selecting static routing.

7. Repeat steps 3-6 to set up tunnel options for the destination device.
8. Click **Check connectivity**. There should be a ping from source interface to destination interface if there is a connection.
9. Click **Create** when complete.

Option 2: Create a Point-to-Multipoint Tunnel



1. Click on the pencil icon and select point-to-multipoint tunnel.
2. Use the pencil icon to first select a tunnel hub. This is usually a head office router.
3. Next, select spokes one by one. These should be your branch offices.
4. Perform Option 1 steps 2-6 to set up tunnel options.

Note: In version 3.5.0, adding a static route to the hub of a multipoint tunnel is not supported.

5. Repeat for all your spokes (branch offices).
6. Click **Check connectivity**.
7. Click **Create** when complete.

Note: For multipoint tunnels, a hub of multipoint tunnel cannot share the same interface (with the same IP address) as a GRE point-to-point tunnel.

Note: Connectivity is not needed for the new tunnel configuration to be created, although the tunnel will not be fully formed until there is a connection.

Distributed tunnel routing

When you create a tunnel, you can choose to distribute routes to additional devices in order to create a return routing path.

You will see a list of subnets to choose from, with these subnets being accessible from the device. However, not all networks and devices at the tunnel destination are used to form new primary routes. The list of destinations are pre-filtered.

The following types of networks and hosts are allowed:

- connected by static routes
- directly connected to the end router (direct routes)
- routed through a dynamic routing protocol

Example: When a tunnel is created from (A) to (B), (A) will distribute networks and hosts (X) to (B). However, that does not necessarily mean (X) can reach (B), so networks on (B) are allowed to be distributed to add as routes on (X).

If a tunnel is deleted, all static routes associated with the nexthops of that tunnel will also be deleted. However, manual routes can still be added from the pull-down menus.

Administrative distances are added to static routes; static routes with the same default administrative distance (zero) to the same destination is not supported. When a route is shared, Vista Manager adds a 1 to its distance. Therefore, a direct connection route with a default distance of 0 will have a distance of 1 when added to a destination device’s route table.

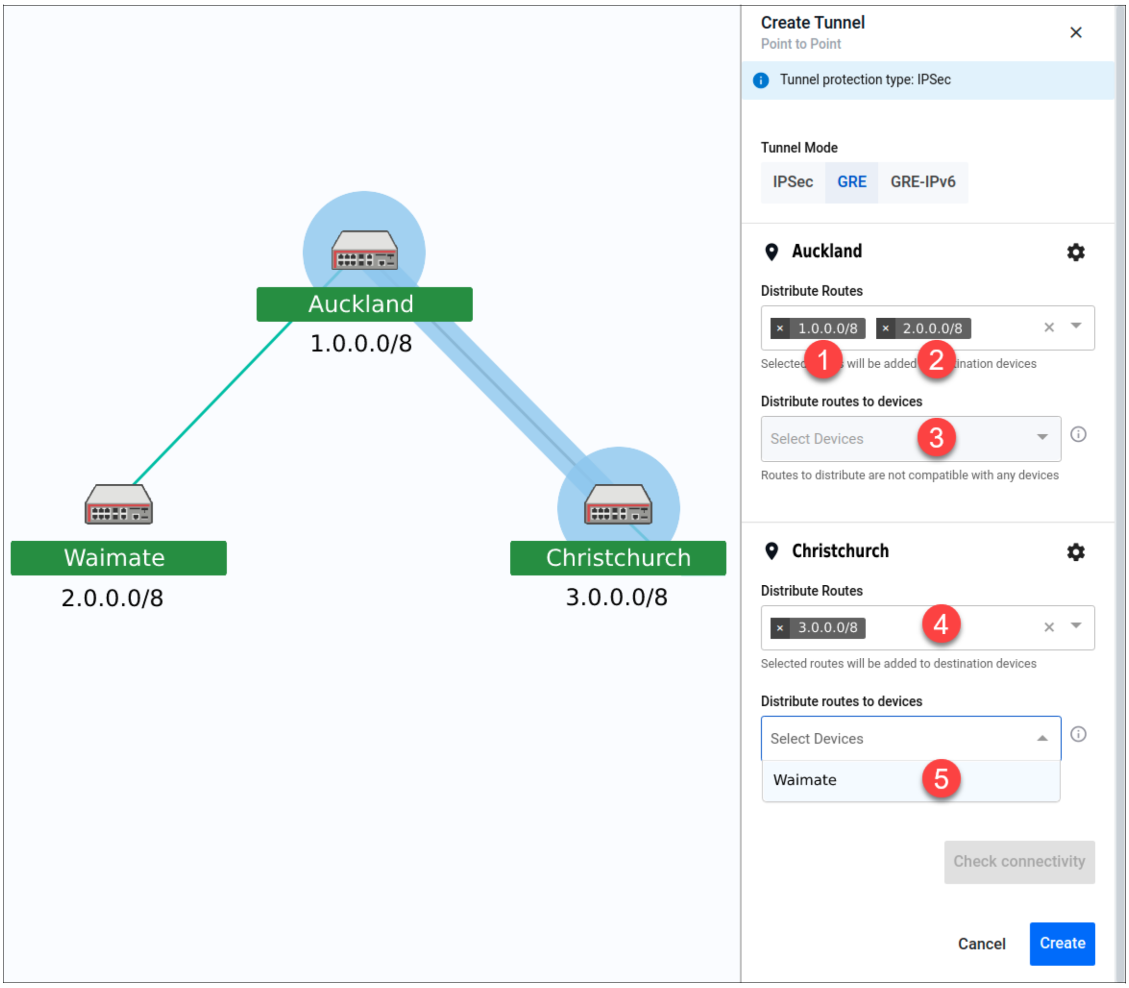
For this feature to be fully supported, AlliedWare Plus version 5.5.1-2.1 or later is required.

Settings for the source end of tunnel (Auckland)

1. The route to **Auckland (1.0.0.0/8)** is selected in the “Distribute Routes” input. This route is added to the route table of the Christchurch device, allowing traffic to go from Auckland to Christchurch.
2. A tunnel between Auckland and Waimate already exists, so the route to **Waimate (2.0.0.0/8)**, is an option in the “Distribute Routes” input. This route is added to the route table of the Christchurch device, allowing traffic to go from Waimate to Christchurch.
3. Nothing is needed in the “Distribute routes to devices” input because the selected routes are automatically distributed to the destination end of the tunnel (Christchurch).

Settings for the destination end of tunnel (Christchurch)

4. The route to **Christchurch (3.0.0.0/8)** is selected in the “Distribute Routes” input. This route is added to the route table of the Auckland device, allowing traffic to go from Christchurch to Auckland.
5. Because the route to Waimate is added to the route table of the Christchurch device, there is now an option to distribute a route to Christchurch on the Waimate device. This route is added to Waimate, allowing traffic to go from Christchurch to Waimate.



Create Tunnel
Point to Point

Tunnel protection type: IPSec

Tunnel Mode
IPSec GRE GRE-IPv6

Auckland

Distribute Routes
× 1.0.0.0/8 × 2.0.0.0/8
Selected 1 will be added 2 ination devices

Distribute routes to devices
Select Devices 3
Routes to distribute are not compatible with any devices

Christchurch

Distribute Routes
× 3.0.0.0/8 4
Selected routes will be added to destination devices

Distribute routes to devices
Select Devices
Waimate 5

Note: It is mandatory to choose a route. Vista Manager is unable to prevent loops from being created as all forwarding paths in the network are not known. Some WAN-facing interfaces will not be included in the list of routing destinations, as this could form routing loops caused by networks beyond the immediate control of the user.

Feature limitations

There are some feature limitations to take note of:

- Because this is adding static routing, there may be potential for routing loops. The risk of causing such loops cannot be eliminated.
- Entity subnets will not be filtered out if they overlap or are duplicated with other subnets. It is up to the user to create valid entities.
- Changes made to subnets and entities after the tunnel has been created will not be automatically deleted; routes on the devices will not be updated. Users will have to make these changes on the tunnels and devices if they make changes to subnet and entities.
- IPv6 routes are supported as static routes, but are not supported as distributed subnets. The IP version of static routes must match the IP version of the tunnel IP address.
- mGRE tunnels use GRE-based protocols and are therefore stateless. Static routes on mGRE will not be re-routed automatically if a hub-to-spoke tunnel link goes down.

Internet Breakout

Internet Breakout lets specific applications being used at branch office locations, access the Internet directly, rather than going via the head office. This improves the performance of cloud-based applications (e.g. Office 365) and reduces traffic volumes on VPN connections between branch offices and the head office.

- This feature requires AR-series devices to run AlliedWare Plus 5.5.0-2.1 or later.
- Internet Breakout requires Device DPI Per Entity and DPI Learning to be enabled.
- Before configuring, start by identifying the types of applications you may want to allow direct Internet access.
- Enabling this feature reduces router throughput.
- Any traffic that bypasses security processing may reduce security and threat protection at the local branch office. Carefully consider the potential consequences of giving direct Internet access to a type of traffic, and whether additional local or cloud-based security needs to be implemented to protect Internet Breakout traffic and the branch office.
- Internet Breakout needs to classify applications for sending direct to the Internet. It does this most effectively when it can read both incoming and outgoing traffic on the interface that was/is sending those applications to the head office. For IPSec protected tunnels, this requires a feature called tunnel security reprocessing. Vista Manager does not enable tunnel security reprocessing because it reduces router performance.
    - To enable tunnel security reprocessing, enter the following commands on the router's CLI:

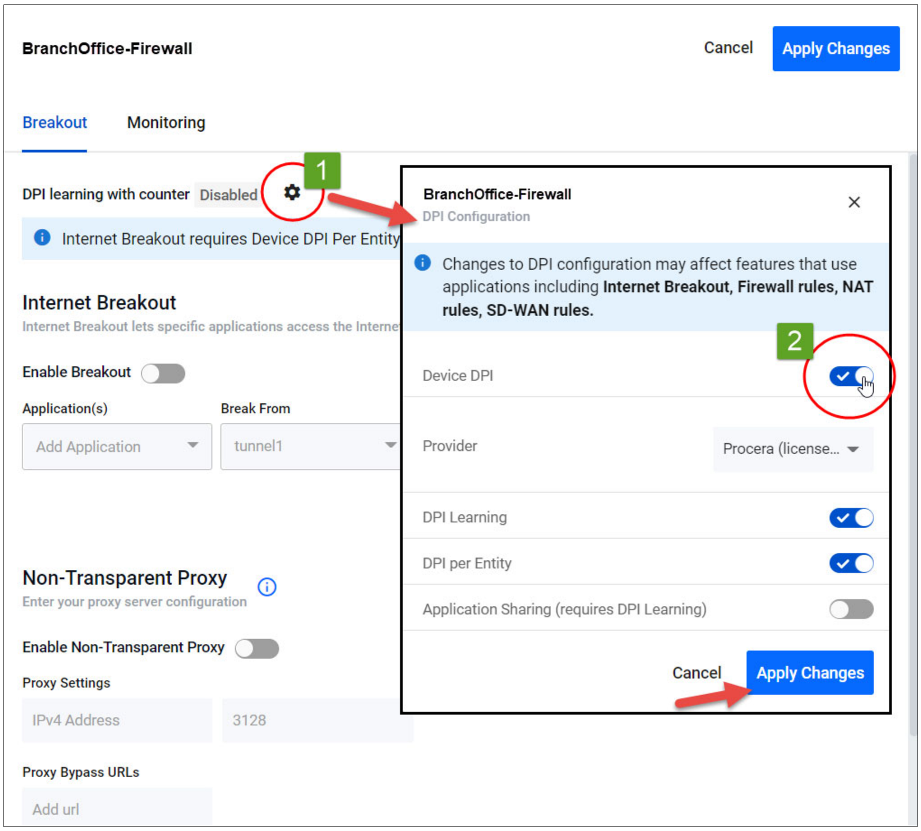
```
enable
conf t
tunnel security-reprocessing
```

Step 1. **Enable Internet Breakout and specify the traffic path for applications**

By default, Internet Breakout inputs are disabled until **Breakout** or **Non-Transparent Proxy** is enabled. If invalid options are selected followed by disabling Internet Breakout, these options will be removed. This prevents saving a disabled but invalid configuration.

Use the **Internet Breakout** > **Breakout** tab and select a device:

1. Click the **Settings** icon
2. Enable **Device DPI**



DPI learning with counter Disabled

Internet Breakout requires Device DPI Per Entity

Internet Breakout

Internet Breakout lets specific applications access the Interne

Enable Breakout

Application(s)

Break From

Non-Transparent Proxy

Enter your proxy server configuration

Enable Non-Transparent Proxy

Proxy Settings

Proxy Bypass URLs

BranchOffice-Firewall

DPI Configuration

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.**

Device DPI ✓

Provider: Procera (license...

DPI Learning ✓

DPI per Entity ✓

Application Sharing (requires DPI Learning)

3. Select **Enable Breakout**

4. Add **Applications** to the Breakout List, for example, Office365, Google, Youtube, etc.

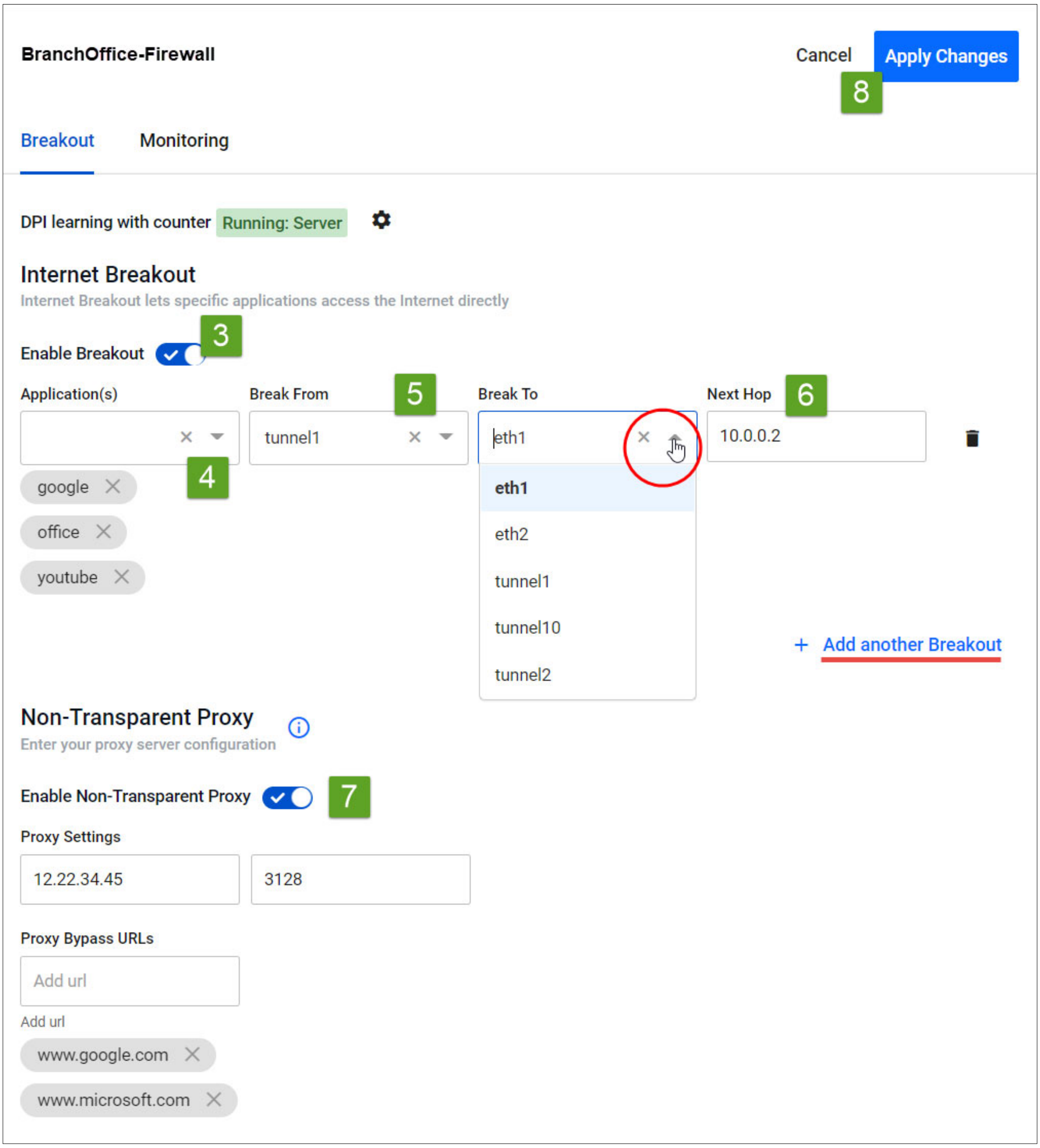
5. Select the interfaces to **Break from** and **Break to**.

   - To add another break from or break to interface, click **+ Add another Breakout** and repeat steps 4, 5, and 6.

6. Enter the **Next Hop** address (optional). If ‘tunnel’ is selected as ‘break from’, then next hop is disabled.

7. Enable and configure the **Non-Transparent Proxy** settings (optional).

8. Click **Apply Changes**.



DPI learning with counter Running: Server

Internet Breakout

Internet Breakout lets specific applications access the Internet directly

Enable Breakout ✓

Application(s)	Break From	Break To	Next Hop
google office youtube	tunnel1	eth1	10.0.0.2

Non-Transparent Proxy

Enter your proxy server configuration

Enable Non-Transparent Proxy ✓

Proxy Settings

12.22.34.45

3128

Proxy Bypass URLs

Add url

Add url

www.google.com

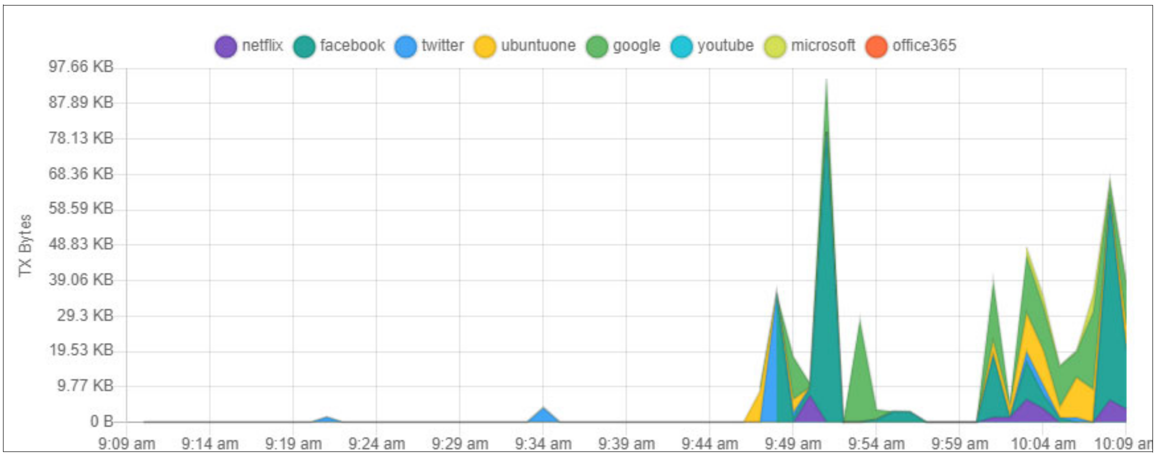
www.microsoft.com

Step 2. **Monitor the breakout**

Use the Internet Breakout > Monitoring tab

Two charts are available here:

- The pie chart shows the top 5 breakout applications. Clicking applications on the vertical legend adds/removes them to/from the chart.
- The line graph shows breakout traffic over a set period of time. Clicking applications on the horizontal legend or using the drop-down list adds/removes them to/from the graph.



Auto Traffic Shaping

This feature dynamically adjusts the maximum transit capacity of remote locations (spoke tunnels) to not exceed the receive capacity of the central site (hub). This is termed the **maximum Rx bandwidth** of the hub.

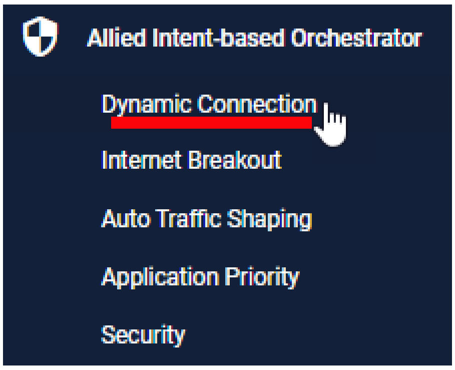
To allocate this bandwidth optimally, we recommend you also deploy Application Priority profiles on each spoke tunnel.

To manage traffic, an algorithm uses current spoke tunnel traffic rates, and any configured application priority settings, across all spoke tunnels to fairly allocate bandwidth. Spoke tunnels have a guaranteed transmit bandwidth. This equals the sum of the CIRs (committed information rate) plus system bandwidth defaulted to 5%.

Prerequisite Step: Configure tunnels between spokes and hubs.

Use the Allied Intent-based Orchestrator (or AMF Plus) > Dynamic Connection feature

This step requires you to navigate away from Auto Traffic Shaping.



Allied Intent-based Orchestrator

Dynamic Connection

Internet Breakout

Auto Traffic Shaping

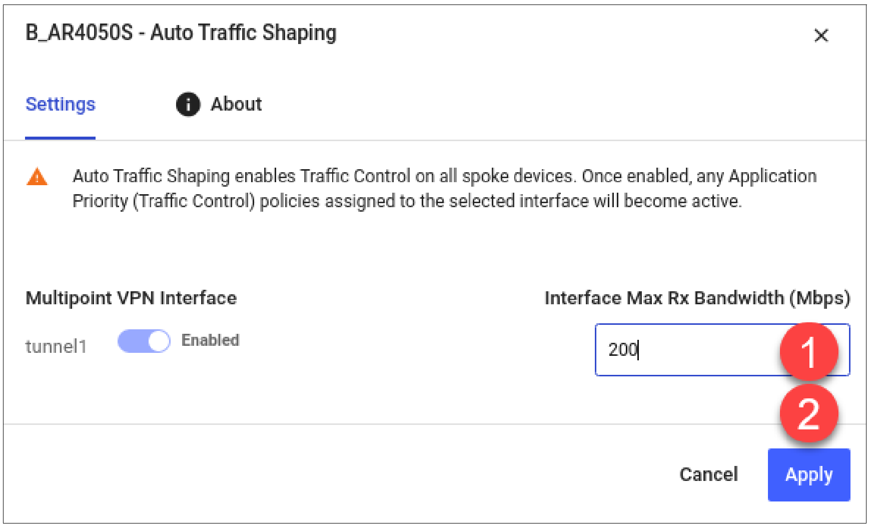
Application Priority

Security

Step 1: Configure the Interface Max Rx Bandwidth value.

Use the Auto Traffic Shaping > Settings tab or button

1. Enter the maximum bandwidth a hub can handle. The algorithm calculates and applies optimal traffic shaping based on this number.
2. Click **Apply**.



B_AR4050S - Auto Traffic Shaping

Settings | About

Auto Traffic Shaping enables Traffic Control on all spoke devices. Once enabled, any Application Priority (Traffic Control) policies assigned to the selected interface will become active.

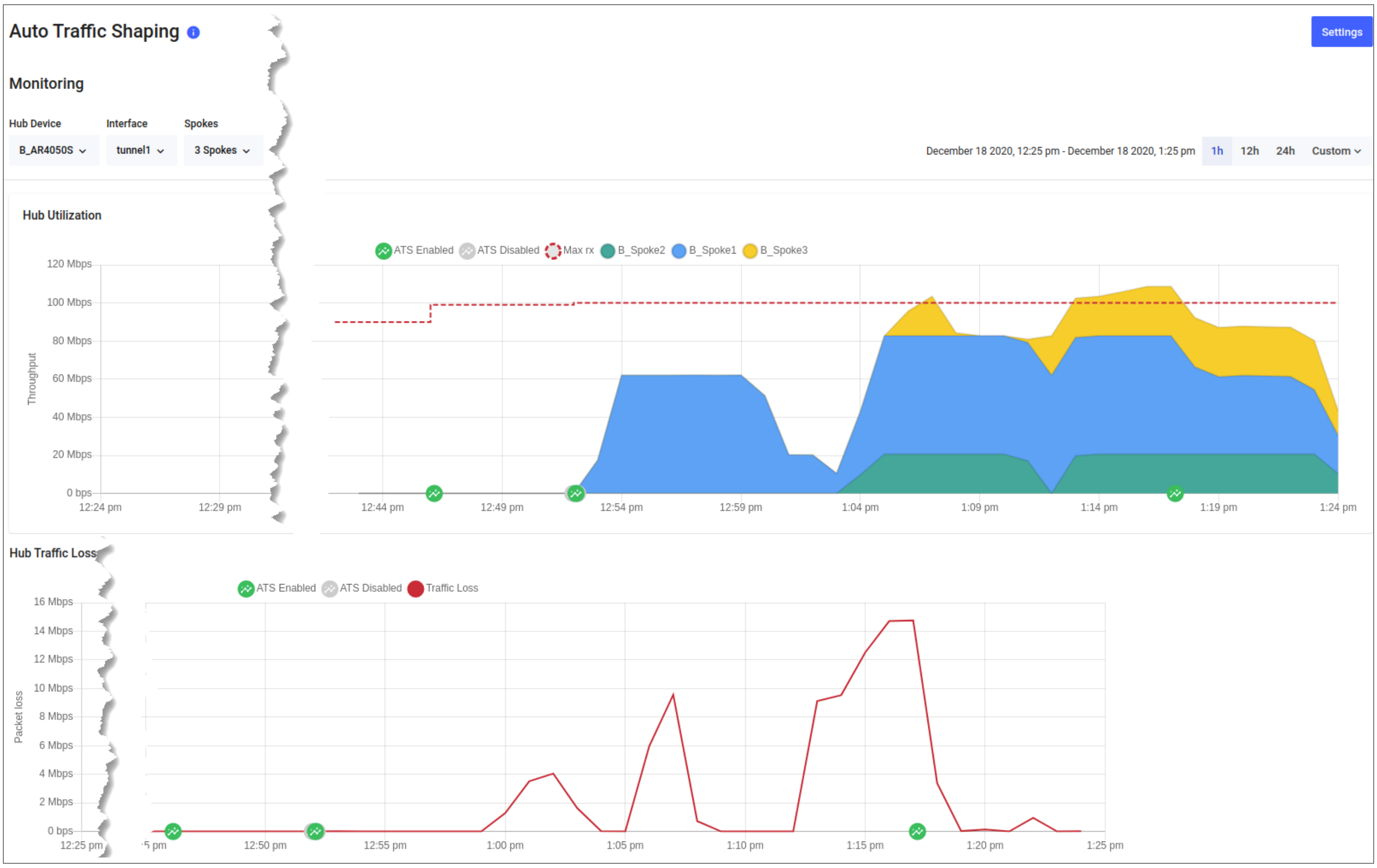
Multipoint VPN Interface: tunnel1 Enabled

Interface Max Rx Bandwidth (Mbps): 200

Step 2: Monitor hub utilization and traffic loss.

Use the Auto Traffic Shaping > Monitoring tab

View charts in the Monitoring page, where you can use filters to specify what traffic is shown.



Auto Traffic Shaping

Monitoring

Hub Device: B_AR4050S
Interface: tunnel1
Spokes: 3 Spokes

December 18 2020, 12:25 pm - December 18 2020, 1:25 pm

Hub Utilization

Hub Traffic Loss

Application Priority

You can use Application Priority to choose specific applications and prioritize or deprioritize them. This ensures your most important business traffic is prioritized for transmission between locations across your WAN. Vista Manager EX provides 3 priority classes:

1. **Critical Services**
2. **Daily Operations**
3. **Non-Essential**

You can assign different applications to each priority class, save the assignment in a policy, and deploy the policy on the AR-Series device (firewall or router) at each location in your WAN.

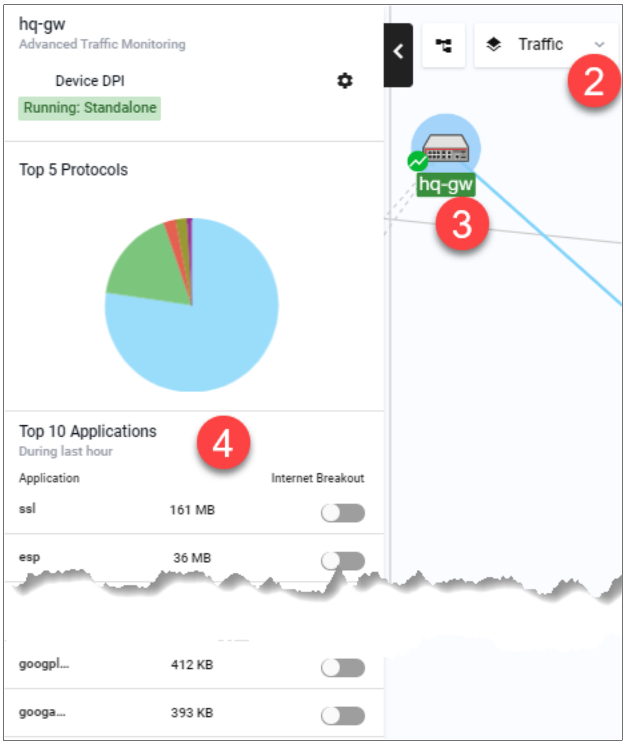
A policy is the overall title for a set of rules and priorities. It also defines the type of algorithm for how it calculates the priority of traffic. Traffic for any unassigned applications set in the rules will fall into the **Default** policy class. The default class is not directly visible when creating a policy, but the traffic matching the default class (either in throughput or packet loss) can be seen in the Monitoring graphs.

This feature lets you view any existing Application Priority policies, and shows throughput and packet loss graphs for devices that have a policy deployed on them. You can also see how much guaranteed bandwidth each class has and how much shared bandwidth remains. When the network is congested, use the slider or advanced option to set bandwidth requirements to ensure smooth application traffic.

Vista Manager EX application usage data lets you better prioritize applications. When creating or deploying policies, you can analyze current traffic present on a device, which helps you assign applications into the most appropriate priority classes for a policy.

Step 1: Check application usage on a device.

1. Navigate to the Network Map.
2. Select **Traffic** mode from the drop-down list.
3. Select the device you want to check. A blue circle appears around it.
4. Examine the traffic usage data, which appears in the left-hand panel.



hq-gw
Advanced Traffic Monitoring

Device DPI
Running: Standalone

Top 5 Protocols

Top 10 Applications
During last hour

Application		Internet Breakout
ssl	161 MB	
esp	36 MB	
googpl...	412 KB	
googa...	393 KB	

Step 2: Create an Application Priority policy.

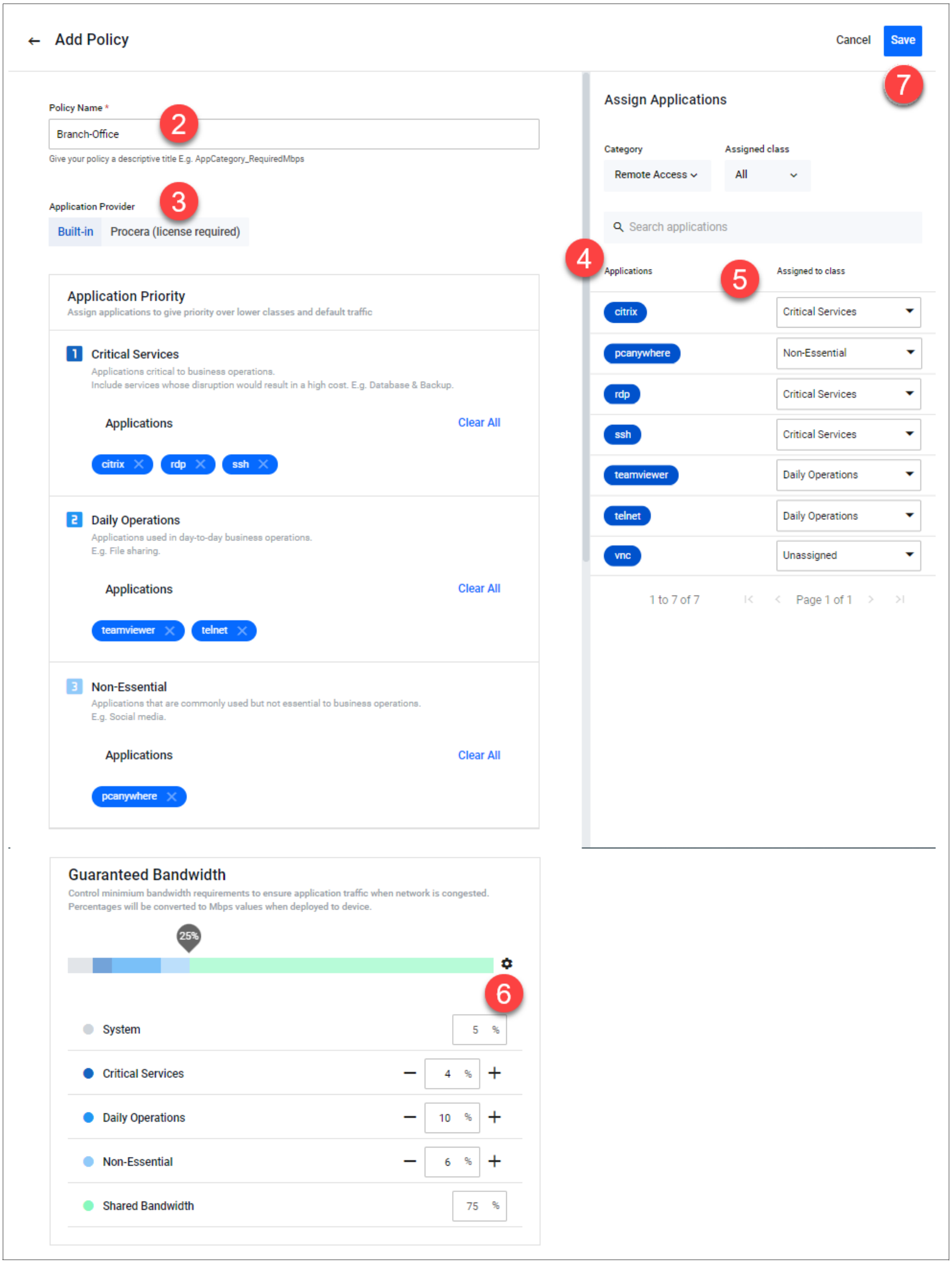
1. To create a policy, you may:
   - Right-click on the device in Traffic mode of the Network Map and select: **Application Priority** > **Add Policy**, or
   - Navigate to the Application Priority menu item and click **+Add Policy**, or
   - Navigate to the Application Priority menu item, and **clone** an existing policy by clicking the 3 dots for that policy, in the Action column.

All of the above approaches open the Add Policy page.

2. Next, type in a policy name. For example, **Branch-Office**.
3. Select an Application Provider. By default, Built-in is selected. If you have bought an Advanced Firewall licence for your AR-Series UTM firewall, select Procera instead, which enables a much larger application list to work with.
4. On the right-hand panel, choose a Category of applications. For example, **Remote Access**. A list of applications will appear.
5. Assign appropriate classes to the relevant applications. You can use the Assigned Class filter at any point to see what applications you have assigned to a class. When you assign a class, it appears accordingly on the policy classes on the left.
6. Here, you may adjust the bandwidth for each class. To do this, either **move the slider** or **enable advanced bandwidth adjustment** to type in the percentage. Percentages will be converted to Mbps values when deployed to device. If the advanced option is used after the slider, any manually-set values are automatically replaced by the slider pre-sets.

Note: The reserved percentage of guaranteed bandwidth for system traffic is displayed here. The 5% value is based on the default value that traffic control sets on a device. The actual value may vary depending on what device(s) the user deploys the policy on to. Vista Manager will just show **5% as the system bandwidth.**

7. If you have accessed the page via the Network Map, click **Save and Deploy**.
   Otherwise, click **Save**.



Policy Name *

Branch-Office

Give your policy a descriptive title E.g. AppCategory_RequiredMbps

Application Provider

Built-in | Procera (license required)

Application Priority

Assign applications to give priority over lower classes and default traffic

1 **Critical Services**

Applications critical to business operations.
Include services whose disruption would result in a high cost. E.g. Database & Backup.

Applications — Clear All

citrix ✕ rdp ✕ ssh ✕

2 **Daily Operations**

Applications used in day-to-day business operations.
E.g. File sharing.

Applications — Clear All

teamviewer ✕ telnet ✕

3 **Non-Essential**

Applications that are commonly used but not essential to business operations.
E.g. Social media.

Applications — Clear All

pcanywhere ✕

Assign Applications

Category: Remote Access
Assigned class: All

Search applications

Applications	Assigned to class
citrix	Critical Services
pcanywhere	Non-Essential
rdp	Critical Services
ssh	Critical Services
teamviewer	Daily Operations
telnet	Daily Operations
vnc	Unassigned

1 to 7 of 7 — Page 1 of 1

Guaranteed Bandwidth

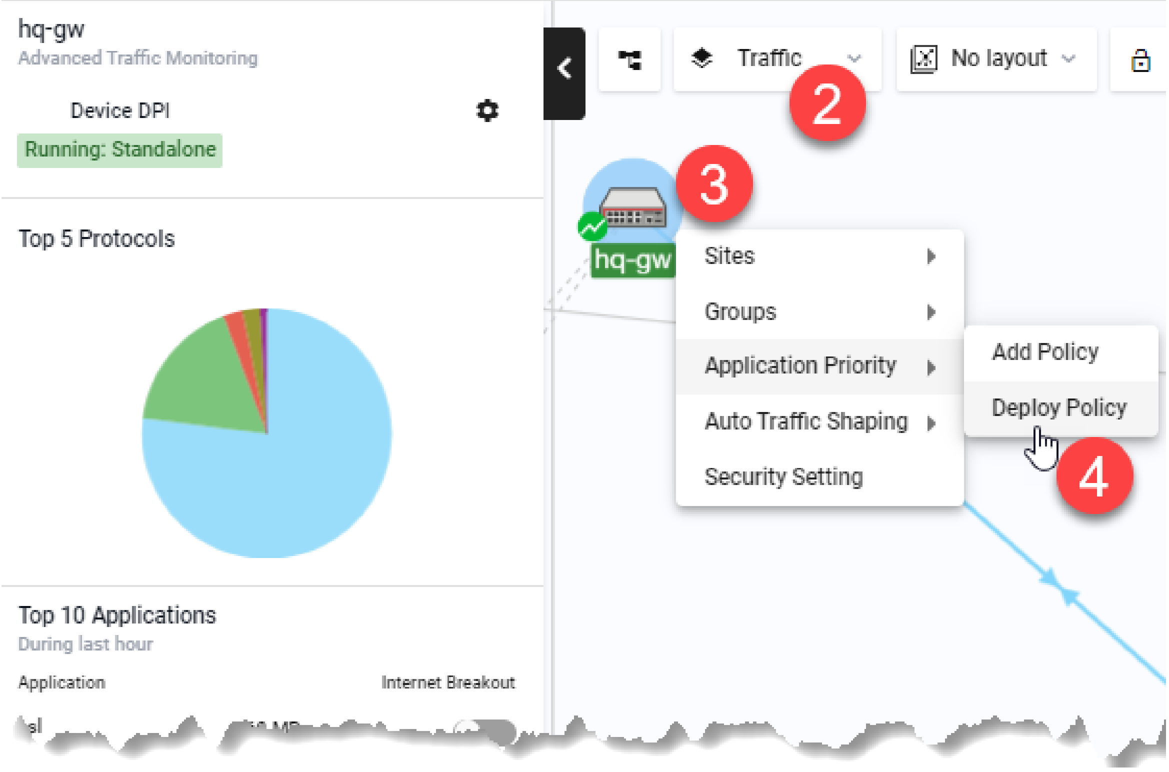
Control minimium bandwidth requirements to ensure application traffic when network is congested.
Percentages will be converted to Mbps values when deployed to device.

25%

System	5 %
Critical Services	4 %
Daily Operations	10 %
Non-Essential	6 %
Shared Bandwidth	75 %

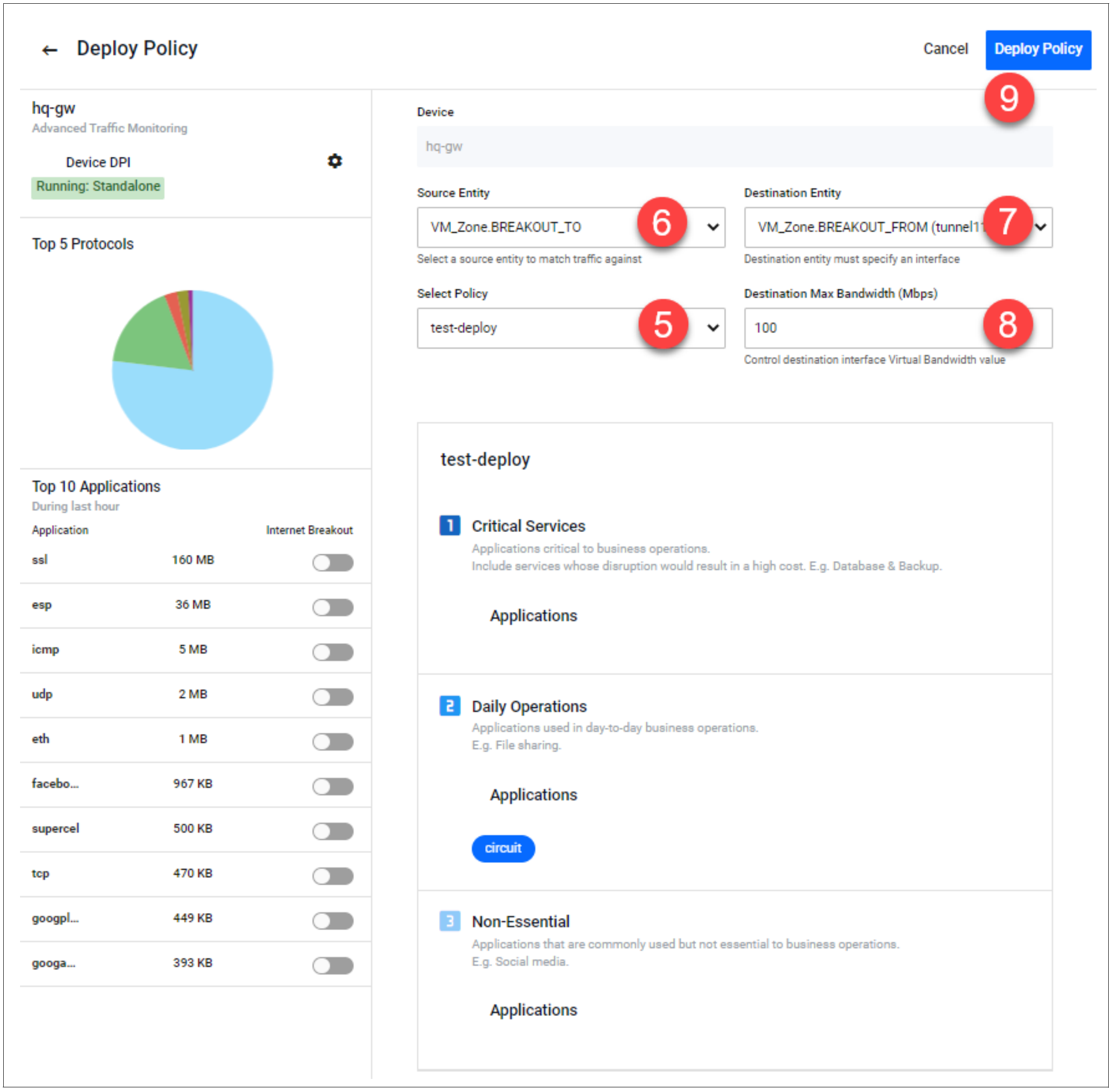
Step 3: Deploy a policy.

1. Navigate to the Network Map.
2. Select **Traffic** mode from the drop-down list.
3. Select the device you want to deploy a policy to. A blue circle appears around it.
4. Right-click on the device, select Application Priority > **Deploy Policy**.



5. Select a policy to deploy.
6. Specify a **Source Entity** to match traffic against.
7. Specify an interface for **Destination Entity**.
8. Define a **maximum bandwidth**. This places a cap on the virtual bandwidth.

9. Click **Deploy Policy** when complete.



Deploy Policy

hq-gw
Advanced Traffic Monitoring

Device DPI
Running: Standalone

Top 5 Protocols

Top 10 Applications
During last hour

Application		Internet Breakout
ssl	160 MB	○
esp	36 MB	○
icmp	5 MB	○
udp	2 MB	○
eth	1 MB	○
facebo...	967 KB	○
supercel	500 KB	○
tcp	470 KB	○
googpl...	449 KB	○
googa...	393 KB	○

Device: hq-gw

Source Entity: VM_Zone.BREAKOUT_TO
Select a source entity to match traffic against

Destination Entity: VM_Zone.BREAKOUT_FROM (tunnel1
Destination entity must specify an interface

Select Policy: test-deploy

Destination Max Bandwidth (Mbps): 100
Control destination interface Virtual Bandwidth value

test-deploy

1 Critical Services
Applications critical to business operations.
Include services whose disruption would result in a high cost. E.g. Database & Backup.

Applications

2 Daily Operations
Applications used in day-to-day business operations.
E.g. File sharing.

Applications

circuit

3 Non-Essential
Applications that are commonly used but not essential to business operations.
E.g. Social media.

Applications

Security

The security feature lets you configure the web control and IP reputation features on the UTM firewalls at a number of locations simultaneously, for centralized and simplified management.

- **Web control** offers an easy way to monitor and control the types of websites viewed by employees.
- **IP reputation** blocks employee access to websites that are known source of spam, viruses and other malicious activity, to protect your network against security threats.

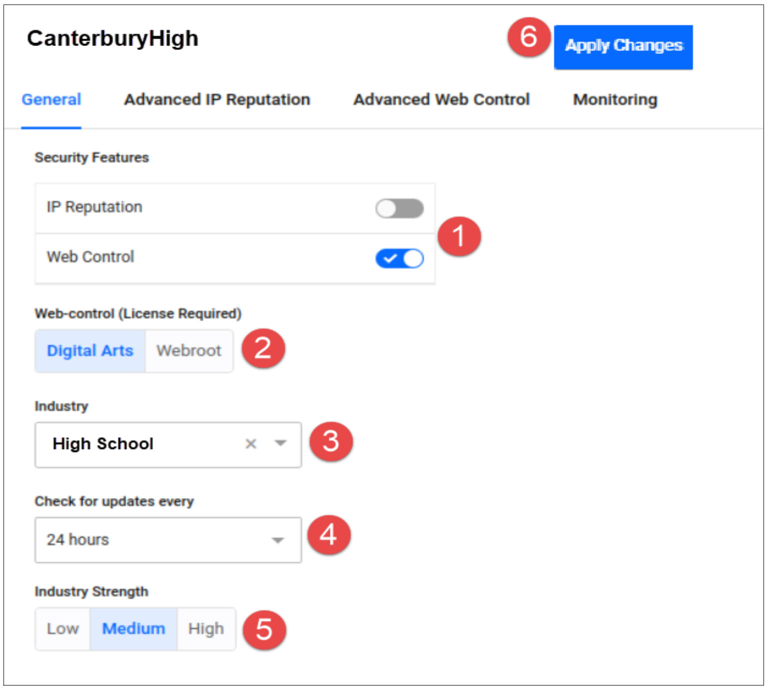
The overall security feature allows you to enable recommended security settings for a group of UTM firewall devices based on an industry type and security strength. This simplifies the process as there is no need to manually choose website or reputation categories for each device.

Note: For this feature to be fully functional, you may need to do additional configuration in the device GUI. Internet access and domain name lookup are required. Enable the ATL Live update server in order to download and check for IP reputation or web control updates.

Step 1: Enable security features and select industry settings.

Use the Security > General tab

1. Enable **IP Reputation** and **Web Control** for the desired device group(s).
2. Select a Security provider (e.g. Digital Arts).
3. Select the industry type (e.g. High School).
4. Set a time to check for updates.
5. Select the desired security strength for the industry (e.g. Medium).
6. Click **Apply Changes**.



CanterburyHigh

Security Features

IP Reputation: off

Web Control: on

Web-control (License Required): Digital Arts (selected), Webroot

Industry: High School

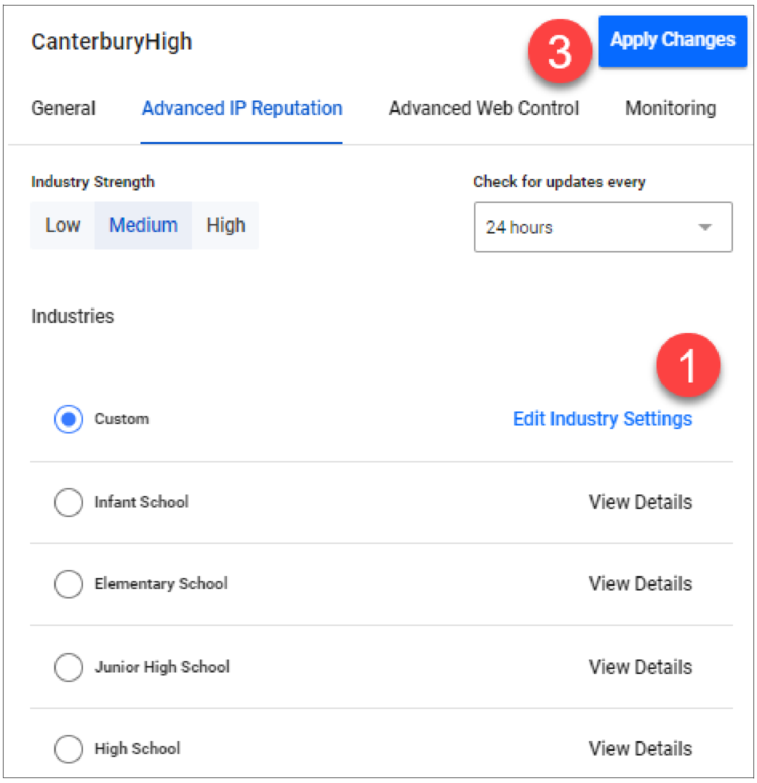
Check for updates every: 24 hours

Industry Strength: Low, Medium (selected), High

Step 2: Edit advanced IP reputation settings if required.

Use the Security > Advanced IP Reputation tab

1. Click **Edit Industry Settings**.



CanterburyHigh

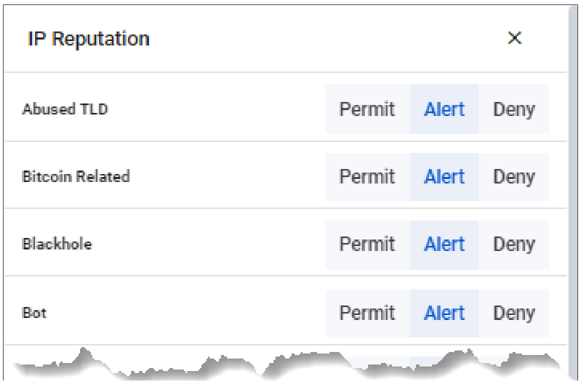
Industry Strength: Low [✓ Medium] High

Check for updates every: 24 hours

Industries

● Custom	Edit Industry Settings
○ Infant School	View Details
○ Elementary School	View Details
○ Junior High School	View Details
○ High School	View Details

2. **Permit**, **alert**, or **deny** a reputation category action as needed.
   A warning appears if one or more devices in the group have had different IP reputation or Web Control settings already applied via another group.



IP Reputation ×

Abused TLD	Permit [✓ Alert] Deny
Bitcoin Related	Permit [✓ Alert] Deny
Blackhole	Permit [✓ Alert] Deny
Bot	Permit [✓ Alert] Deny

3. Click **Apply Changes**. This changes the industry type to Custom.

Step 3: Edit advanced Web Control settings if required.

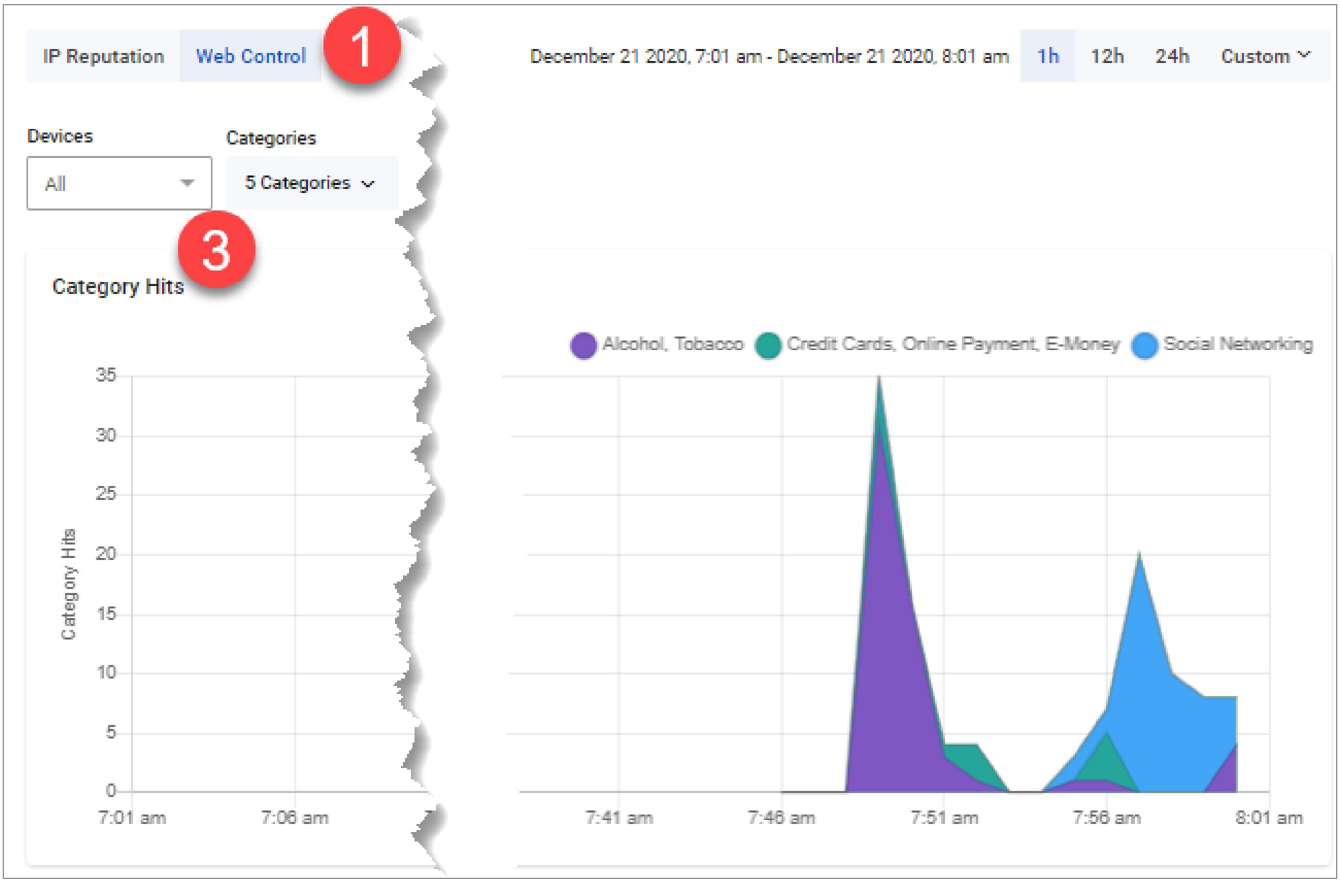
Use the Security > Advanced Web Control tab

1. Click **Edit Industry Settings**.
2. **Permit** or **deny** website categories as needed.
   A warning appears if one or more devices in the group have had different IP reputation or Web Control settings already applied via another group.
3. Click **Apply Changes**. This changes the industry type to Custom.

Step 4: Monitor Web Control and IP Reputation performance.

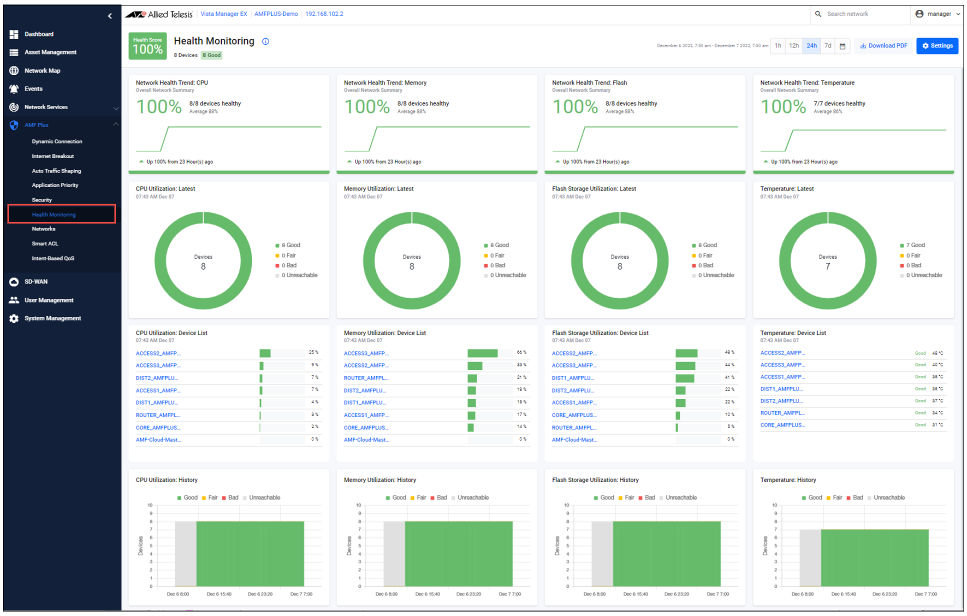
Use the Security > Monitoring tab

1. Click on the IP Reputation and Web Control buttons to view respective graphs.
2. For IP Reputation, click the drop-down list to select the UTM firewall device from a specific location to view.
3. For Web Control, click the drop-down list to select the UTM firewall device from a specific location to view. Clicking Categories on the legend or drop-down list lets you add/remove categories to view on the graph.



Health Monitoring

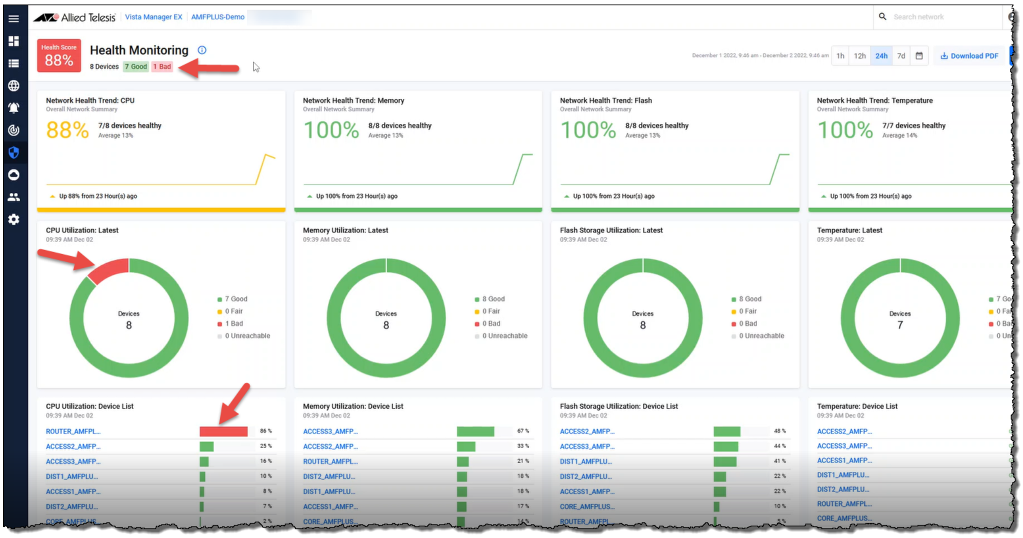
Use the Health Monitoring feature to view a summary of the state of your network's health as part of AMF Plus. Understanding network health indicators enables you to investigate, analyze, and improve the overall health of your network quickly. Such indicators include CPU utilization, storage, temperature, and memory usage.



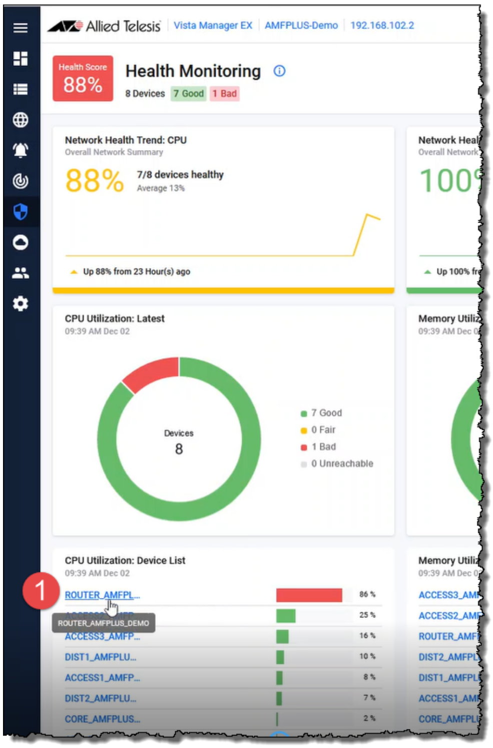
The **Health Score** is a percentage based on how many devices are healthy in the network. The state of each device is selected based on the worst state of any of the gathered statistics. Result charts are color coded for easy understanding of device status: Green = Good, Yellow=Fair, Red=Bad, and Grey=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

Here's how it works

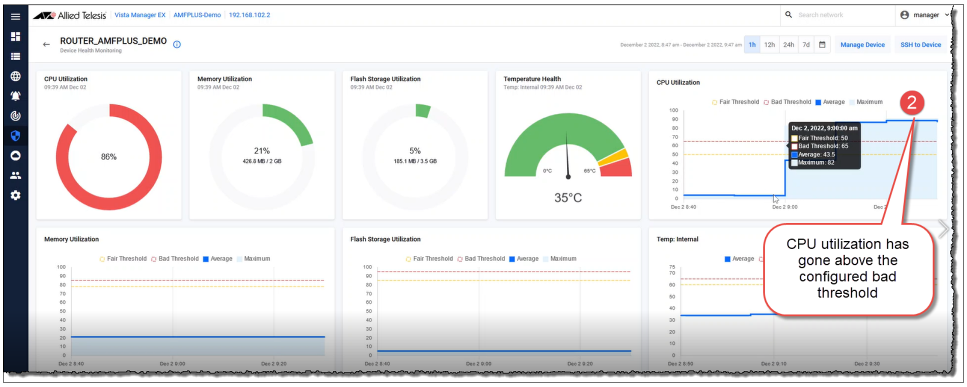
In the example below, you can see a Health Score of 88%. There are 8 devices in this network, but there's a CPU issue with one of them. The bad device is highlighted in red.



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

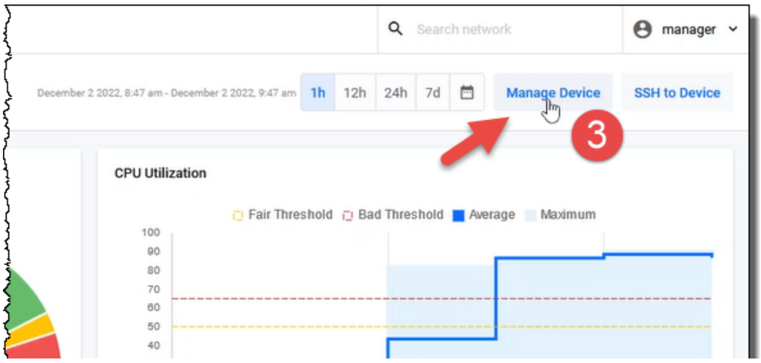


2. Drilling down confirms that around 9am CPU utilization rose above the configured band threshold.

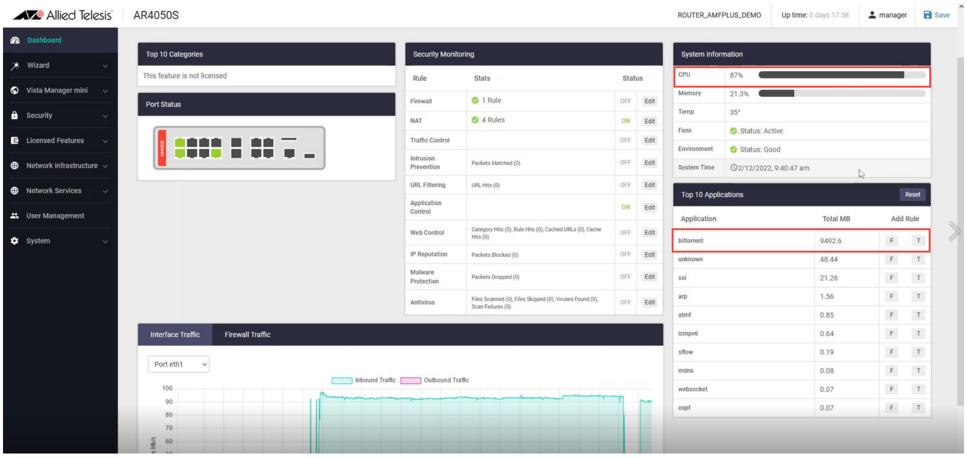


CPU utilization has gone above the configured bad threshold

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



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



Security Monitoring

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

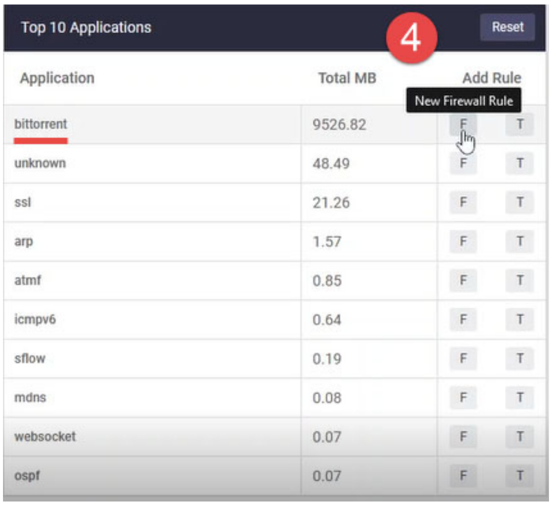
System Information

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

Top 10 Applications — Reset

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

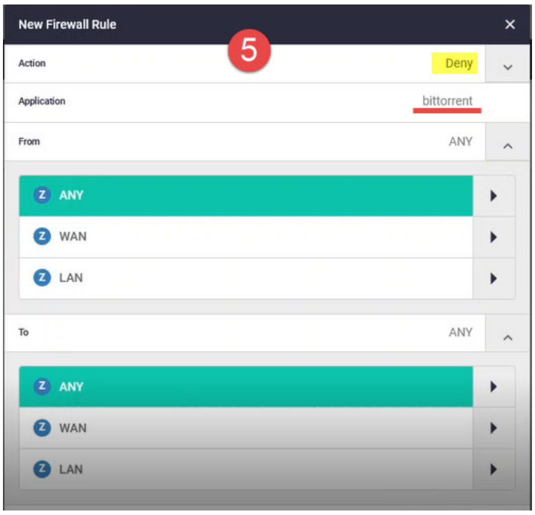
4. At this point you may decide to disallow the bittorrent traffic by adding a firewall rule.



Top 10 Applications — Reset

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

5. Configure the firewall rules.



Action: Deny

Application: bittorrent

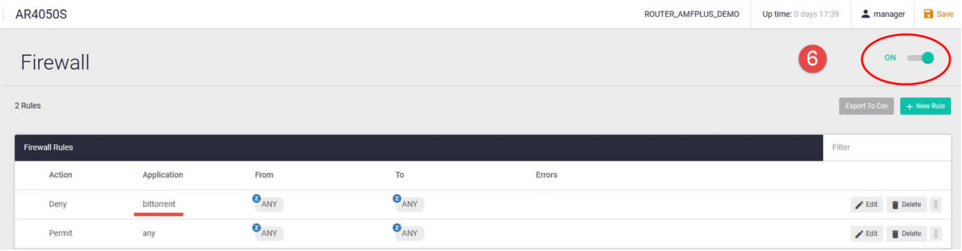
From: ANY

- Z ANY
- Z WAN
- Z LAN

To: ANY

- Z ANY
- Z WAN
- Z LAN

6. Turn on the firewall.



AR4050S

ROUTER_AMFPLUS_DEMO | Up time: 0 days 17:39 | manager | Save

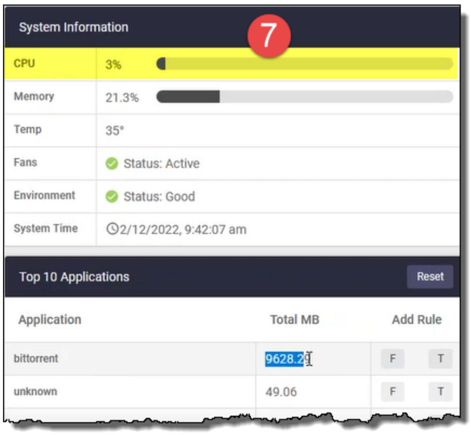
Firewall

2 Rules

Firewall Rules

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

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



System Information

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

Top 10 Applications

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

FAQs

1. What devices are monitored, and can you select the devices that will be monitored?

   - All AlliedWare Plus devices are automatically added to Health Monitoring. Devices cannot be added or deleted manually.

2. How often is a device polled?

   - Polling occurs every 5 minutes.

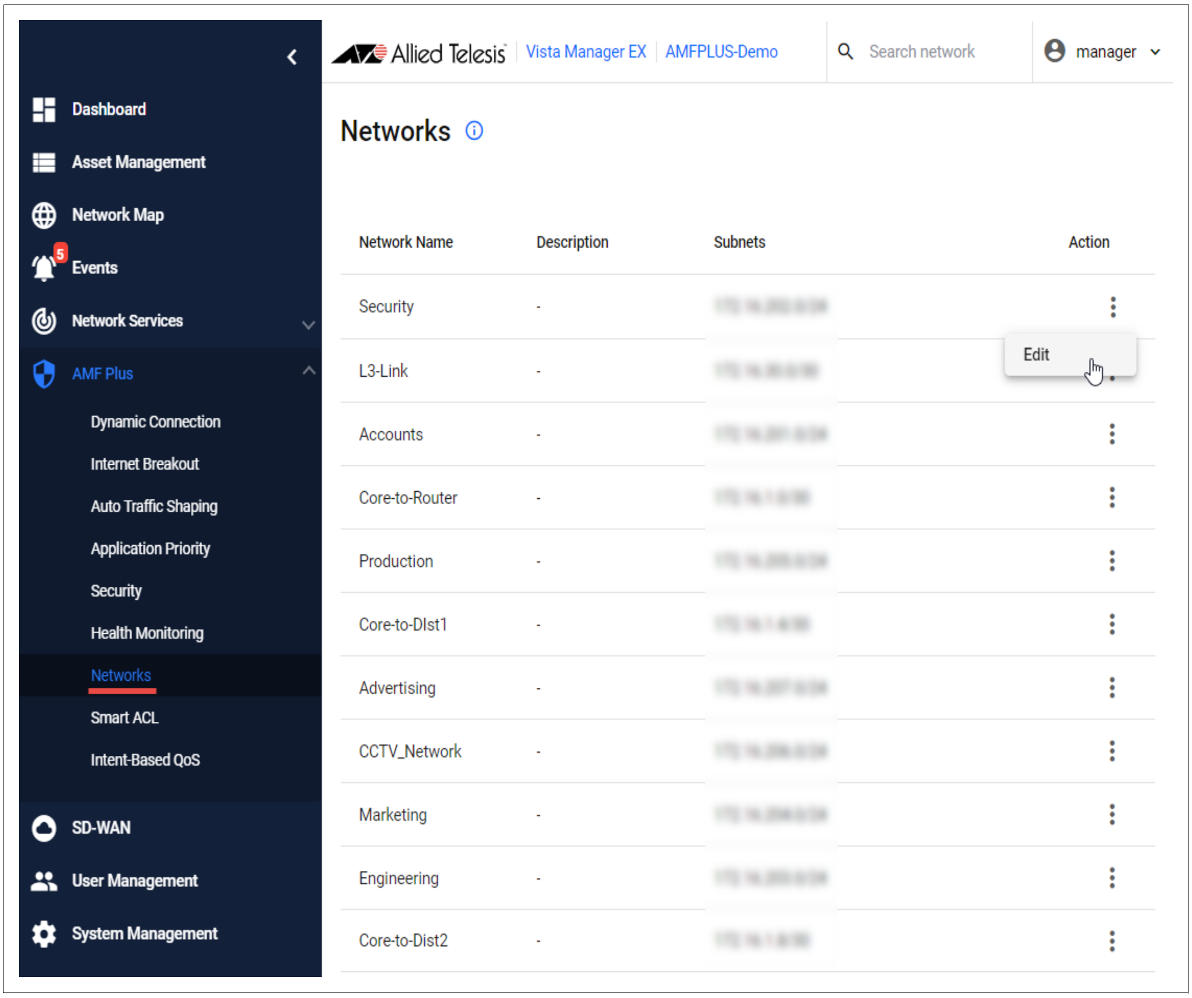
3. How much historical data is stored?

   - 7 days.

Networks

Vista Manager EX defines a Network as an IP subnet attached to a VLAN. For example, subnet 192.168.1.0/24 is associated with VLAN1. As part of the Smart ACL feature, network entries are automatically imported and maintained by Vista Manager EX via the attached network devices.

Each network is given a default **Network Name** and **Description** which you can **Edit** to suit your needs.



Networks

Network Name	Description	Subnets	Action
Security	-	[redacted]	⋮
L3-Link	-	[redacted]	⋮
Accounts	-	[redacted]	⋮
Core-to-Router	-	[redacted]	⋮
Production	-	[redacted]	⋮
Core-to-DIst1	-	[redacted]	⋮
Advertising	-	[redacted]	⋮
CCTV_Network	-	[redacted]	⋮
Marketing	-	[redacted]	⋮
Engineering	-	[redacted]	⋮
Core-to-Dist2	-	[redacted]	⋮

NETWORKS - FIELD	DESCRIPTION
Network Name	These are auto-generated in sequence Network-1, Network-2...Network-n, but you can rename them via the Edit Action.
Description	The network description, for example: VLAN100. Use the Edit Action to add or change a description.
Subnets	The subnet IP address, these are auto-generated and derived from the attached networks. But, networks can only be added via the CLI, i.e. configuring a VLAN with subnet(s).
Action	Use the Action menu to edit the network name and description.

Smart ACL

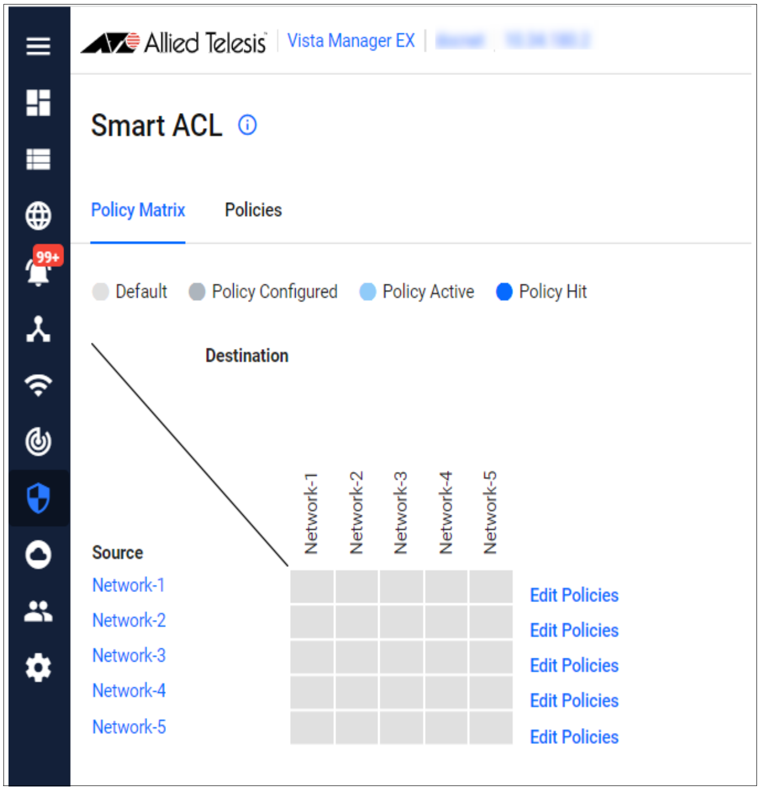
The Smart ACL tool allows you to manage ACLs across devices in the network. ACLs provide traffic flow control and decide which types of traffic are forwarded or blocked.

You can (could) use Smart ACL to control the resources that clients access in the network. For example, you might want to stop marketing clients from being able to see a security client's CCTV video stream and also stop the security clients from accessing marketing videos.

There are three parts to the Smart ACL tool:

1. **Networks**: VLANs configured with an IP subnet.
2. **Policies**: Access List filters (rules) used to control network traffic.
3. **Policy Matrix**: A display of:
   - currently configured source and destination networks
   - policy status - configured, active, and hits on the ACL policy

The objective of Smart ACL is to allow you to apply policies between networks - to control traffic from a source network going to a destination network.



Smart ACL ⓘ

Policy Matrix | Policies

○ Default ● Policy Configured ● Policy Active ● Policy Hit

Source \ Destination	Network-1	Network-2	Network-3	Network-4	Network-5	
Network-1						Edit Policies
Network-2						Edit Policies
Network-3						Edit Policies
Network-4						Edit Policies
Network-5						Edit Policies

Getting started with Smart ACLs

You need to do some initial configuration before you can use the Smart ACL tool. The initial configuration ensures that the Policy Matrix shows the current active policies.

In brief, you first configure a network and optionally assign it a meaningful name, then create an ACL policy and apply it to the network. Let’s look at each step in more detail:

1. Configure a network.

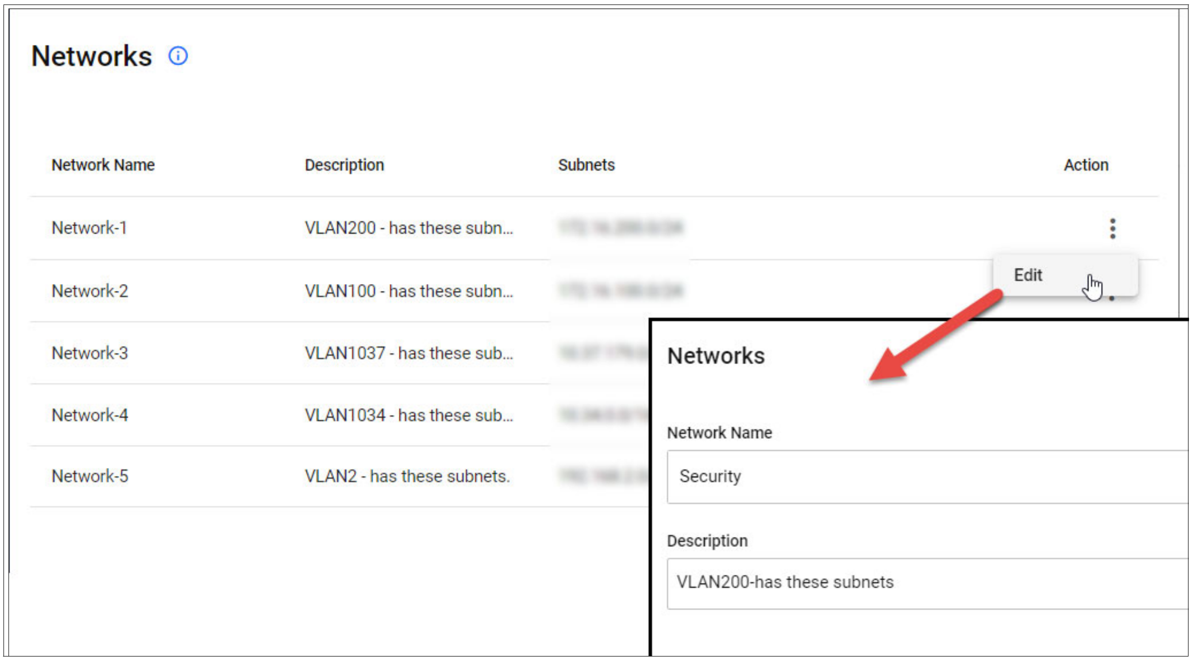
   - Use the **CLI** to configure a network on your AlliedWare Plus device.

   For example:

```
vlan database
 vlan 100

 interface port1.0.5
  switchport mode trunk
  switchport trunk allowed vlan add 100

  interface vlan100
   ip address 172.16.2.1/24
```

2. Assign a meaningful name to the network (optional).

   - Go to **AMF Plus** > **Networks**
   - By default, networks are auto-generated in sequence Network-1, Network-2...Network-n, but you can change the default name to a more meaningful one by using the **Edit** action. You can also add a useful **Description** to the **Network Name**.



Networks ⓘ

Network Name	Description	Subnets	Action
Network-1	VLAN200 - has these subn...	[redacted]	⋮
Network-2	VLAN100 - has these subn...	[redacted]	
Network-3	VLAN1037 - has these sub...	[redacted]	
Network-4	VLAN1034 - has these sub...	[redacted]	
Network-5	VLAN2 - has these subnets.	[redacted]	

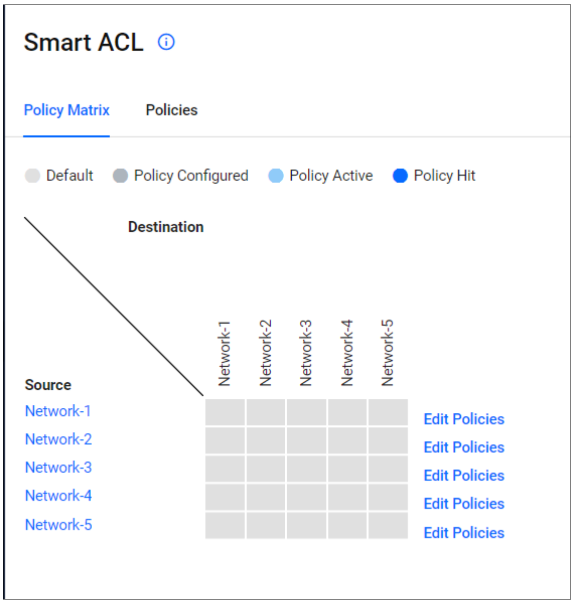
Networks

Network Name: Security

Description: VLAN200-has these subnets

3. Create an ACL Policy

   - Go to **AMF Plus** > **Smart ACL**
   - The **Policy Matrix** displays all currently configured networks. In the example below, there are 5 networks configured with default names.



Source	Network-1	Network-2	Network-3	Network-4	Network-5	
Network-1						Edit Policies
Network-2						Edit Policies
Network-3						Edit Policies
Network-4						Edit Policies
Network-5						Edit Policies

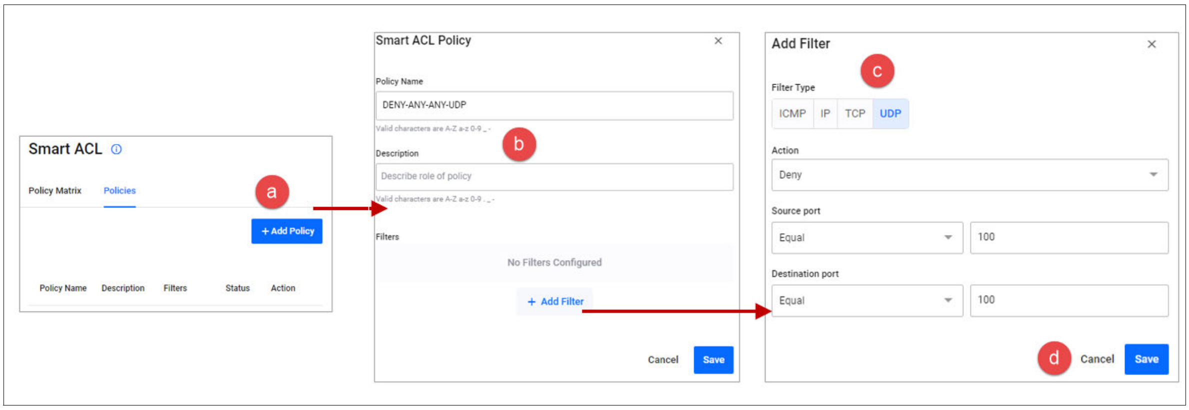
4. Select the **Policies** tab, then:

   a. Click **+Add Policy**

   b. Enter a **Policy Name** and **Description**

   c. Click **+ Add Filter** - set the **Action** and **Filter Type**

   d. Click **Save**.



Policy Name: DENY-ANY-ANY-UDP

Description:

Filters

Filter Type: UDP

Action: Deny

Source port: Equal 100

Destination port: Equal 100

In the example above, an ACL policy called DENY-ANY-ANY-UDP has an action of DENY if the packet matches UDP source port =100and destination port =100.

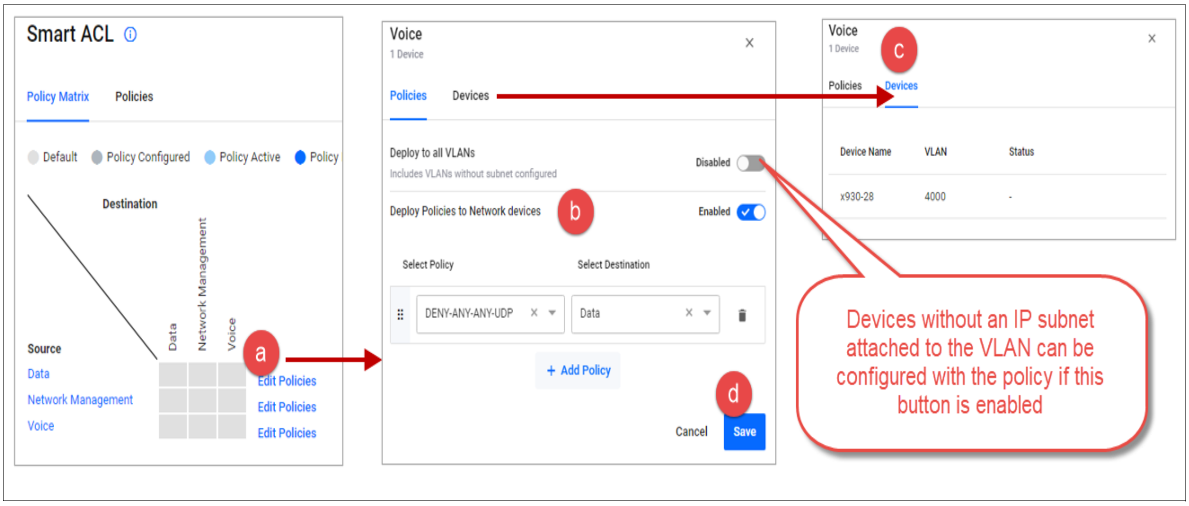
5. Back in the **Policy Matrix** tab, apply a policy to a network.

   a. Select **Edit Policies**

   b. Configure as required - i.e. select a policy and destination

   c. Check the policy is applied to the correct device(s)

   d. Click **Save**



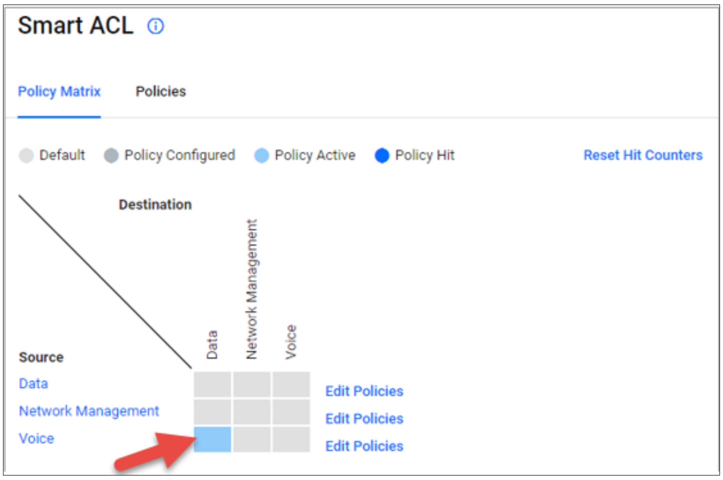
Device Name	VLAN	Status
x930-28	4000	-

Devices without an IP subnet attached to the VLAN can be configured with the policy if this button is enabled

In the example above:

- The ACL policy DENY-ANY-ANY-UDP is applied to packets from the Voice network going to the Data network.
- The Devices tab shows all the devices that the policy will be applied to. In this case, only the device x930-28 will be configured with the ACL policy.

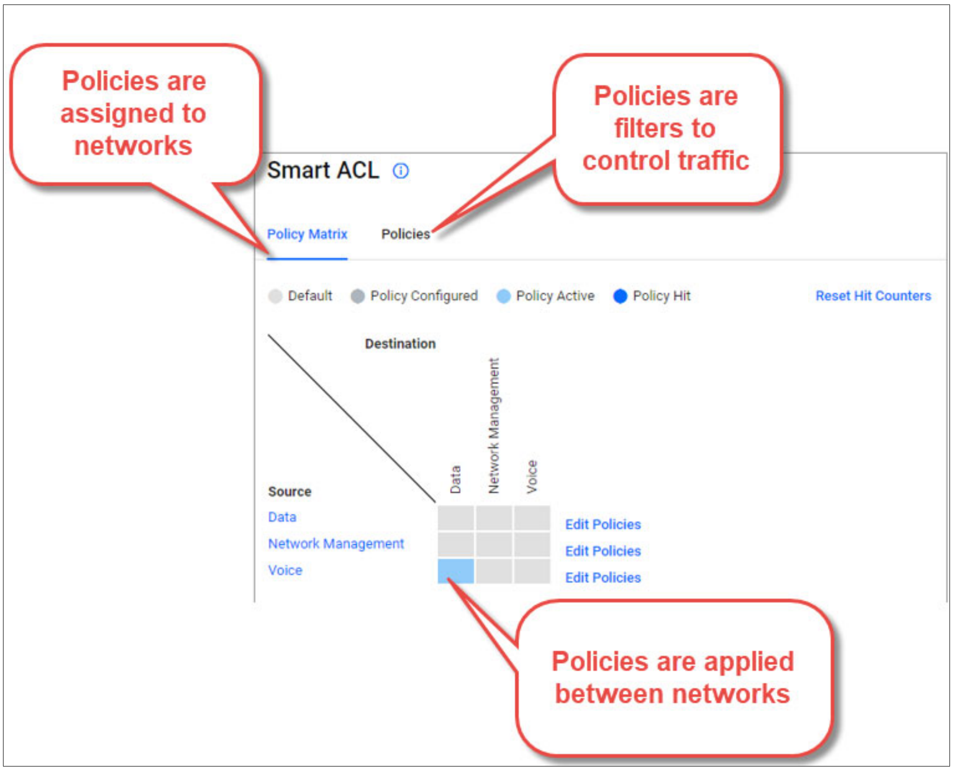
Now you can see the policy is active from source network **Voice** to destination network **Data**.



This completes the initial configuration.

Understanding the Smart ACL Policy Matrix and its operation

Once the initial configuration is complete, the Policy Matrix is set up with the configured networks. In the example below, you can see an active policy from source network **Voice** to destination network **Data**.

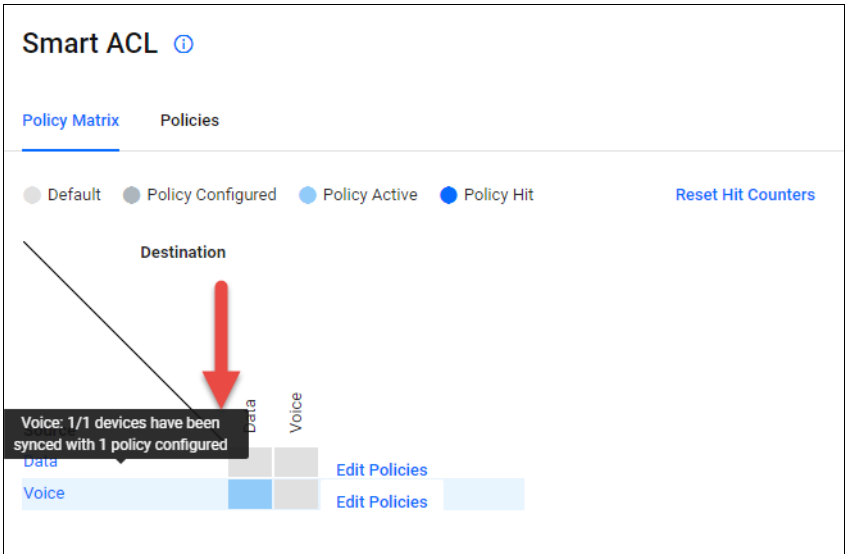


Policies are assigned to networks

Policies are filters to control traffic

Policies are applied between networks

You can hover your mouse over a network name to see how many of the devices in that network have been synced with the ACL configuration for the policy.



Voice: 1/1 devices have been synced with 1 policy configured

The benefit of this is every time a new device is added as part of the network and this subnet, the values will increase and the new device will automatically receive the policy.

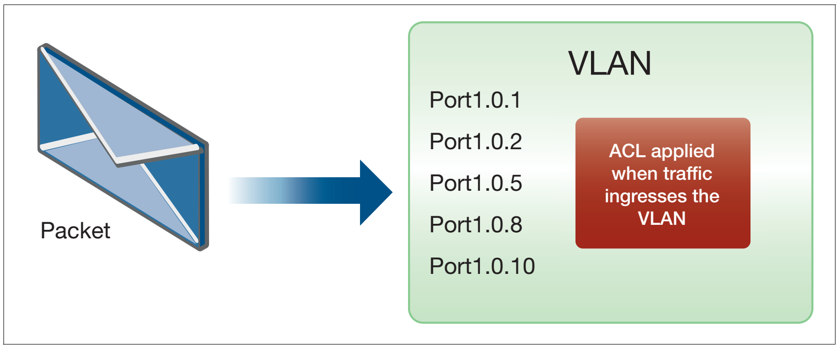
Smart ACL operation

The Smart ACL tool makes configuring complex ACLs on networks easier. It allows you to create, edit, view, and delete ACL policies. ACL policy changes are sync-ed and applied by Vista Manager EX automatically to VLANs using **per-VLAN ACLs**.

What are per-VLAN ACLs?

Per-VLAN ACLs filter traffic as it **ingresses** a VLAN.

Per-VLAN ACL rules are applied to **all** ports on which the VLAN is active. This means they are applied to all ports that are access ports in the VLAN, all trunk ports that allow packets tagged for the VLAN, and all trunk ports whose native VLAN is this VLAN.



Can Smart ACL configure other types of ACLs, for example an interface ACL?

Smart ACL only supports per-VLAN ACLs, and only applies when traffic is going from one subnet to another subnet.

What actual configuration is applied to the device?

Take the example used in "Getting started with Smart ACLs" on page 145:

- An ACL policy called DENY-ANY-ANY-UDP has an action of DENY if the packet matches UDP source port =100 and destination port=100.
- This policy is applied to traffic from the Voice network (V4000, 172.16.0.0/16) going to the Data network (V1, 10.37.62/27).

```
! acl-group matching the Data subnet 10.37.62.64/27
acl-group ip address VISTA_V4_1
 ip 10.37.62.64/27

! Deny traffic matching source IP = any, UDP source port = 100, and
destination IP = Data subnet, UDP destination = 100.
access-list hardware VISTA_V4_source2_destination1_policy1
 deny udp any eq 100 host-group VISTA_V4_1 eq 100

! Apply access-list to access-map
vlan access-map VISTA_ACCESS_MAP_source2
 match access-group VISTA_V4_source2_destination1_policy1

! Attach access-map to VLAN 4000
vlan filter VISTA_ACCESS_MAP_source2 vlan-list 4000 input
```

What commands can I use to view the Smart ACL configuration?

Use the following commands to view the Smart ACL configuration:

```
show acl ip address

show access-list

show vlan access-map

show vlan filter
```

To view the hit counters, use the command:

```
show access-list counters
```

Intent-based QoS

Introduction

Quality of Service (QoS) is a way to prioritize network traffic to ensure that the most important traffic gets through the network with minimal delay or interference.

QoS is a complicated feature with many configuration options and different ways to configure the feature. To configure QoS on a network, you will typically follow these steps:

- Identify the types of traffic that are important and need to be prioritized, such as voice or video traffic.
- Assign each type of traffic a priority level based on its importance. This is typically done using a QoS tagging system.
- Configure your network devices (routers, switches, etc.) to recognize the QoS tags and prioritize traffic accordingly.
- Set bandwidth limits or rate limits on non-priority traffic to prevent it from interfering with the prioritized traffic.

By configuring QoS on your network, you can ensure that critical applications like voice and video are given priority over less important traffic, leading to better network performance and user experience.

From Vista Manager EX version 3.10.1 onwards, you can use **Intent-based QoS** to easily manage and troubleshoot a basic QoS configuration on your network as part of **AMF Plus**.

The benefits of Intent-based QoS

In a congested network where packets are being dropped, it is quite difficult to determine where the drops are occurring. A network could consist of numerous devices, each with a number of ports with egress queues. Detecting drops on one of the queues, on one of those ports, on one of those devices is challenging. Intent-based QoS helps you troubleshoot and visualize the performance of egress queues and manage their settings.

You can:

- Visualise egress queues across the entire network and for individual devices:
  - Drops
  - Throughput
- Modify egress queue settings:
  - Strict priority – queue egress limits
  - Weighted Round Robin – queue weightings

Getting started

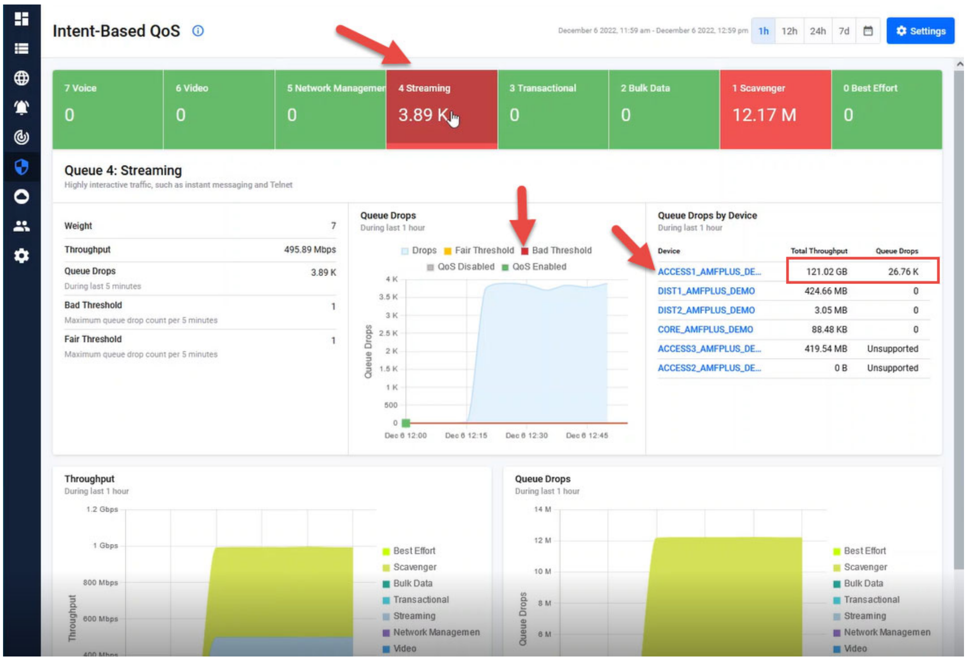
First you need to **manually** apply a default QoS configuration VISTA_DEFAULT_POLICY to all switches in your network. Please see "Default configuration for Intent-based QoS" on page 163 for guidelines and some complete configuration examples.

This default configuration sets up 2 priority queues and 6 weighted round robin (WRR) queues. The strict priority queues have an egress rate limit applied, and the WRR queues each have a weighting applied. The configuration also defines a mapping of DSCP fields to QoS queue based on industry standards. This mapping cannot be changed via Vista Manager EX.

New ports configured with the default QoS policy are added to the list of polled ports. Likewise, removed ports with the default QoS policy are deleted from the list of polled ports.

Once the default configuration has been applied on the network, the **Intent-Based QoS** dashboard shows the state of the network in regards to the QoS queues.

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



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

Queue 4: Streaming

Highly interactive traffic, such as instant messaging and Telnet

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

Queue Drops by Device

During last 1 hour

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

You can see in the diagram above that the **Streaming** queue is experiencing queue drops. Using the dashboard, you can investigate further to see when and on which device drops are occurring.

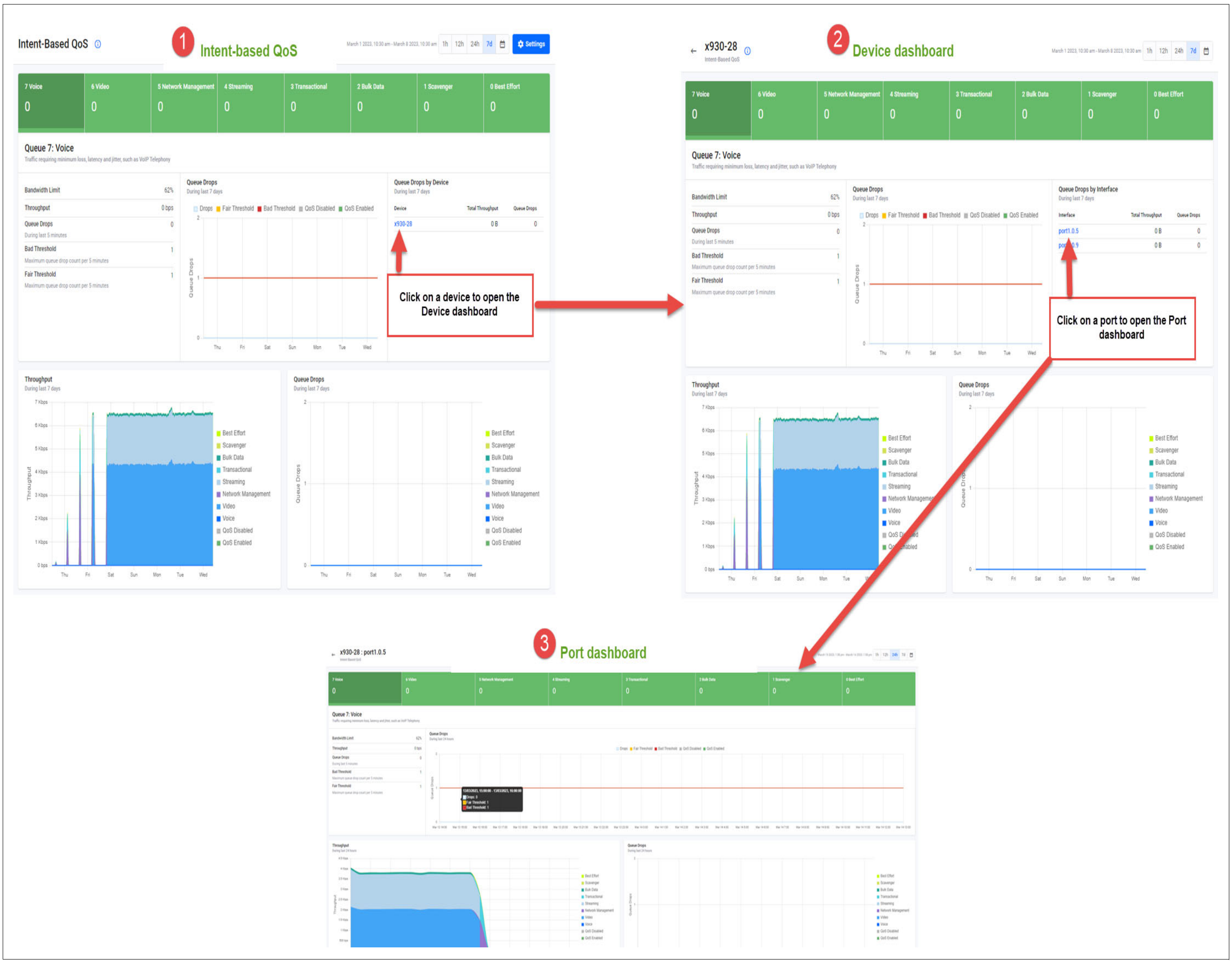
Using the Dashboards

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

In fact, there are three interlinked dashboards:

1. **Intent-based QoS** - displays egress queue details across the network. Data is aggregated from all ports on all devices in the network.
   - Click on a device name to open the device dashboard.
2. **Device** - displays egress queue details from a single device. Data is aggregated from all ports on the device.
   - Click on a port name to open the port dashboard.
3. **Port** - displays queue drops and throughput from a port.

The three dashboards allow you manage QoS configurations on your network. You can use them to drill-down from a wide-angle view of the network traffic, select a device, and then select a port on that device.



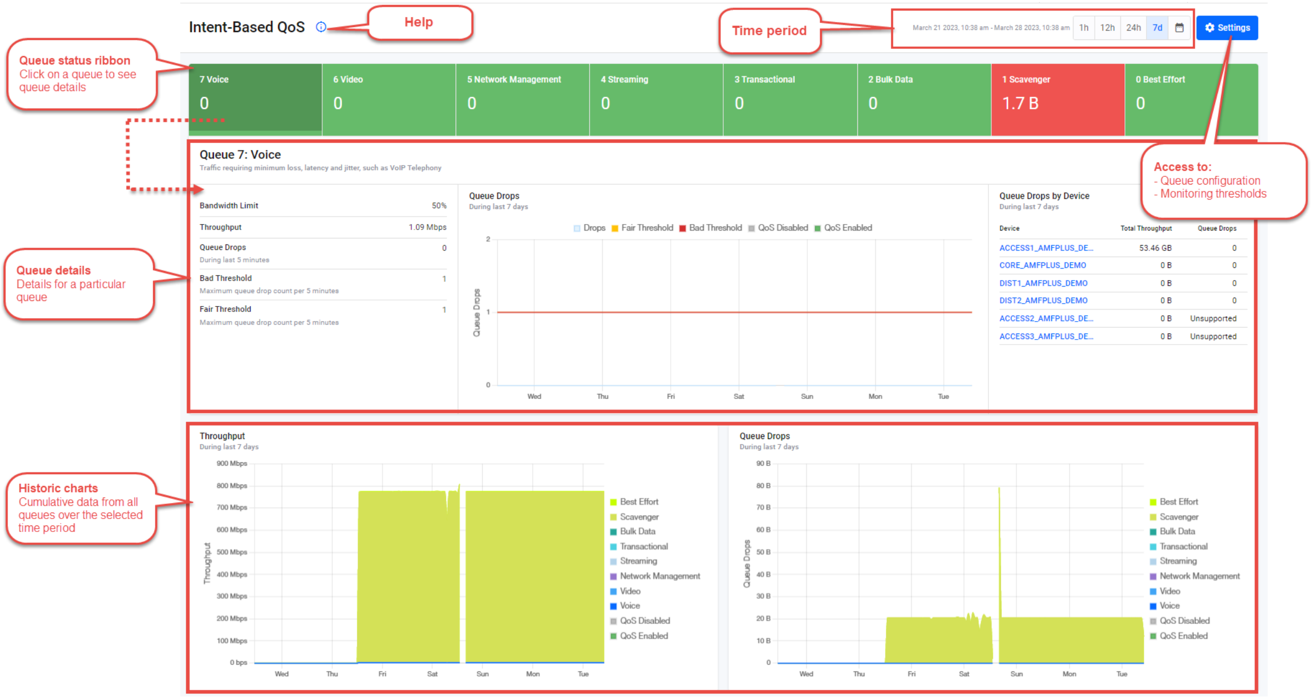
Click on a device to open the Device dashboard

Click on a port to open the Port dashboard

Navigating the dashboards

The Intent-Based QoS dashboard shows queue details for the entire network. Data is aggregated from all ports configured with the VISTA_DEFAULT_POLICY. Vista Manager EX scans the network for any ports configured with the default Vista QoS policy. Every five minutes Vista will poll these ports for queue drops and queue throughput (transmitted bytes). Intent-Based QoS presents the data in dashboards:

The layout is similar for all three dashboards. The Queue status ribbon run along the top, with specific queue details and historic charts below.



Intent-Based QoS

Help

Time period

March 21 2023, 10:38 am - March 28 2023, 10:38 am | 1h | 12h | 24h | 7d

Settings

Queue status ribbon
Click on a queue to see queue details

7 Voice	6 Video	5 Network Management	4 Streaming	3 Transactional	2 Bulk Data	1 Scavenger	0 Best Effort
0	0	0	0	0	0	1.7 B	0

Access to:
- Queue configuration
- Monitoring thresholds

Queue 7: Voice
Traffic requiring minimum loss, latency and jitter, such as VoIP Telephony

Queue details
Details for a particular queue

Bandwidth Limit	50%
Throughput	1.09 Mbps
Queue Drops During last 5 minutes	0
Bad Threshold Maximum queue drop count per 5 minutes	1
Fair Threshold Maximum queue drop count per 5 minutes	1

Queue Drops
During last 7 days

Queue Drops by Device
During last 7 days

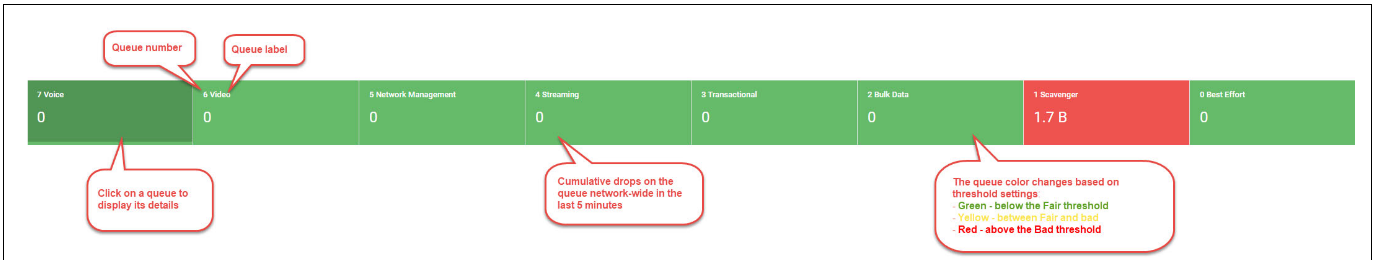
Device	Total Throughput	Queue Drops
ACCESS1_AMFPLUS_DE...	53.46 GB	0
CORE_AMFPLUS_DEMO	0 B	0
DIST1_AMFPLUS_DEMO	0 B	0
DIST2_AMFPLUS_DEMO	0 B	0
ACCESS2_AMFPLUS_DE...	0 B	Unsupported
ACCESS3_AMFPLUS_DE...	0 B	Unsupported

Historic charts
Cumulative data from all queues over the selected time period

Throughput
During last 7 days

Queue Drops
During last 7 days

The Queue status ribbon displays the drops and the status of each queue.



Queue number

Queue label

7 Voice	6 Video	5 Network Management	4 Streaming	3 Transactional	2 Bulk Data	1 Scavenger	0 Best Effort
0	0	0	0	0	0	1.7 B	0

Click on a queue to display its details

Cumulative drops on the queue network-wide in the last 5 minutes

The queue color changes based on threshold settings:
- Green - below the Fair threshold
- Yellow - between Fair and bad
- Red - above the Bad threshold

Drops should be investigated, especially on higher numbered queues, as it could be an indication that congestion is occurring in the network, and potentially impacting on user experience.

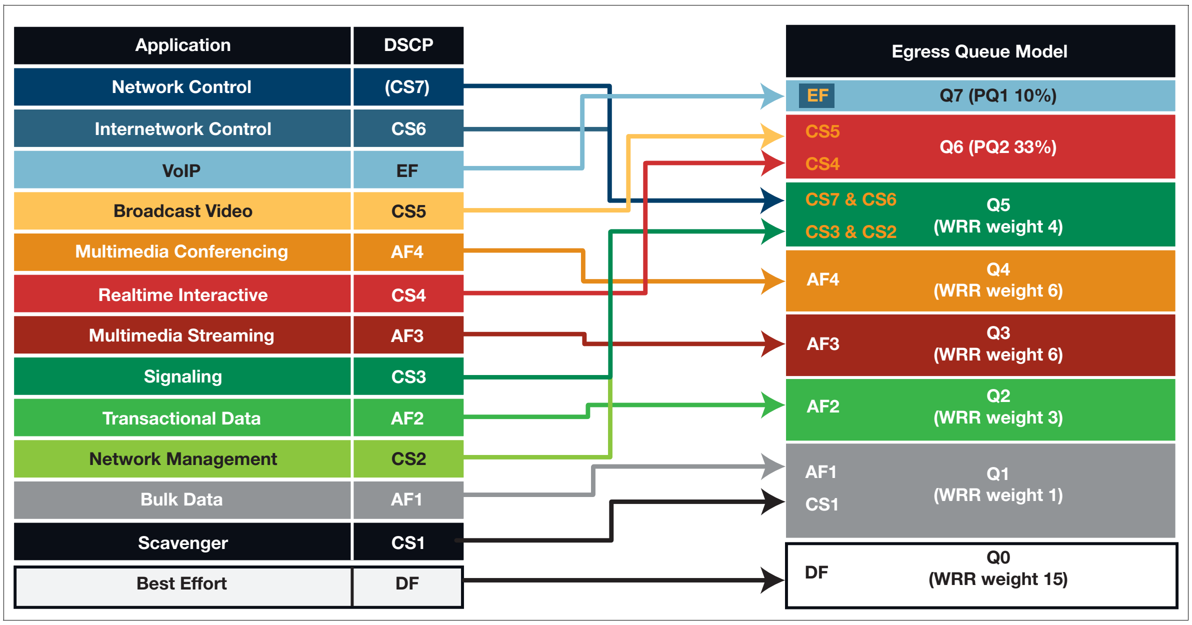
Where do the dashboard queue names come from?

Each of the eight queues has a label describing what sort of traffic is expected on the queue.

QUEUE	LABEL	DESCRIPTION
7	Voice	Traffic requiring minimum loss, latency, and jitter, such as VoIP telephony.
6	Video	Traffic requiring low loss, latency, and jitter, such as video-conferencing.
5	Network Management	Traffic protected with a minimum bandwidth guarantee such as SNMP, NTP, and Syslog.
4	Streaming	Highly interactive traffic, such as instant messaging and Telnet
3	Transactional	Low response time traffic where users wait for transactions to finish, such as SAP and Oracle.
2	Bulk Data	Low interaction, not drop sensitive traffic, such as FTP, E-Mail and Backup Operations.
1	Scavenger	Business-irrelevant traffic, such as Gaming and Peer-to-Peer Media Sharing.
0	Best Effort	Traffic not requiring differentiated treatment.

We recommended traffic is place into the correct queues, but there is no strict requirement. For example, there is nothing stopping you from putting Voice traffic into the Streaming queue. However, the labels in Intent-Based QoS cannot be changed.

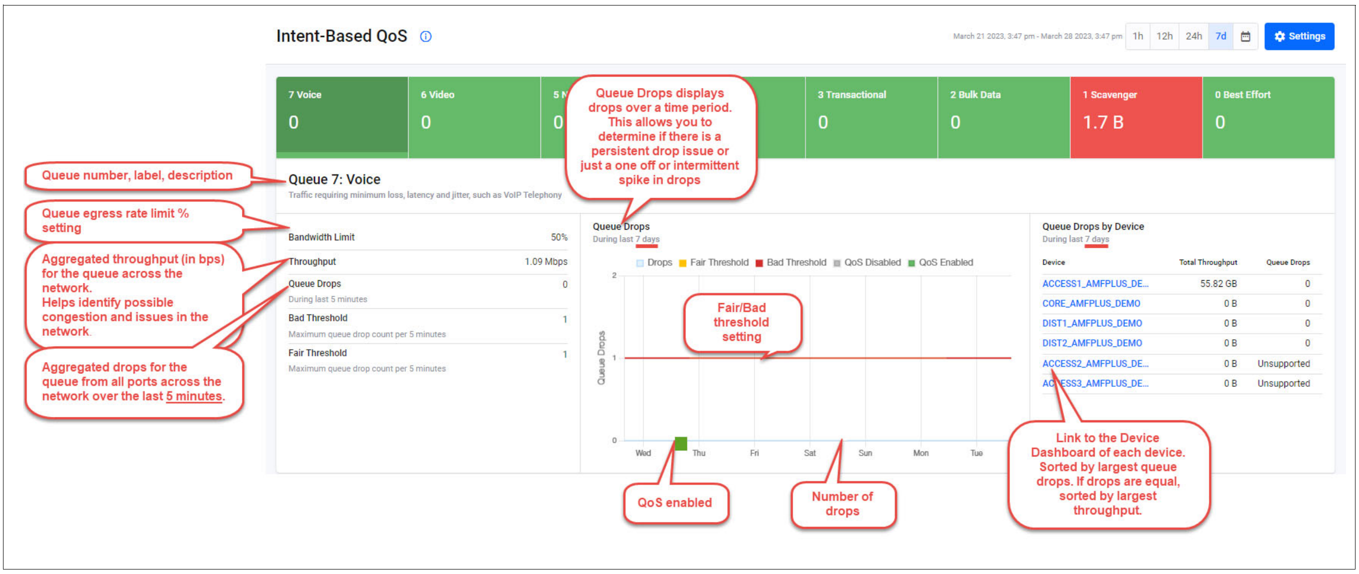
It is ultimately up to you how you want to bind RFC4594 traffic classes to egress queues, however the bindings denoted in the following diagram are recommended.



Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

Queue details

Click on a queue in the Queue Status ribbon to see its details. In the example below, queue 7 Voice is selected and its details displayed underneath.



Queue 7: Voice

Traffic requiring minimum loss, latency and jitter, such as VoIP Telephony

Bandwidth Limit	50%
Throughput	1.09 Mbps
Queue Drops During last 5 minutes	0
Bad Threshold Maximum queue drop count per 5 minutes	1
Fair Threshold Maximum queue drop count per 5 minutes	1

Queue Drops by Device

During last 7 days

Device	Total Throughput	Queue Drops
ACCESS1_AMFPLUS_DE...	55.82 GB	0
CORE_AMFPLUS_DEMO	0 B	0
DIST1_AMFPLUS_DEMO	0 B	0
DIST2_AMFPLUS_DEMO	0 B	0
ACCESS2_AMFPLUS_DE...	0 B	Unsupported
ACCESS3_AMFPLUS_DE...	0 B	Unsupported

Queue number, label, description

Queue egress rate limit % setting

Aggregated throughput (in bps) for the queue across the network.
Helps identify possible congestion and issues in the network.

Aggregated drops for the queue from all ports across the network over the last 5 minutes.

Queue Drops displays drops over a time period. This allows you to determine if there is a persistent drop issue or just a one off or intermittent spike in drops

Fair/Bad threshold setting

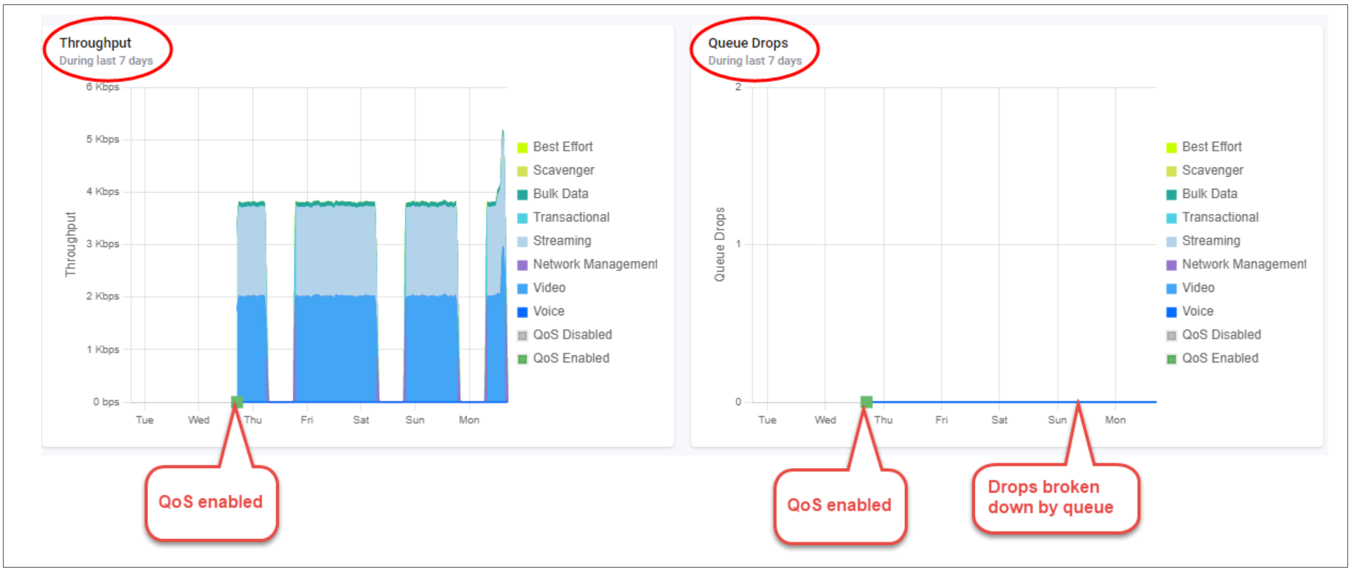
QoS enabled

Number of drops

Link to the Device Dashboard of each device. Sorted by largest queue drops. If drops are equal, sorted by largest throughput.

Historic charts

The historic charts display past details for all queues across all devices on the network. In the left chart below you can see the throughput per queue aggregated from ports over the selected time period, in this case the last 7 days. In the right chart, you can see drops per queue aggregated from ports over the same time period.



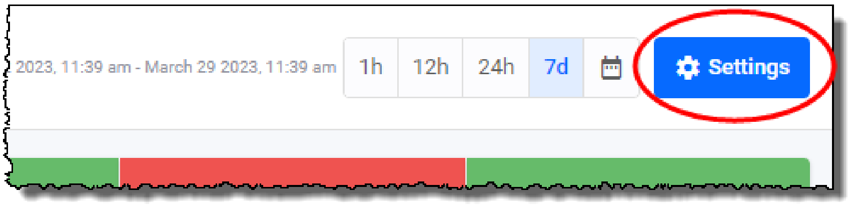
QoS enabled

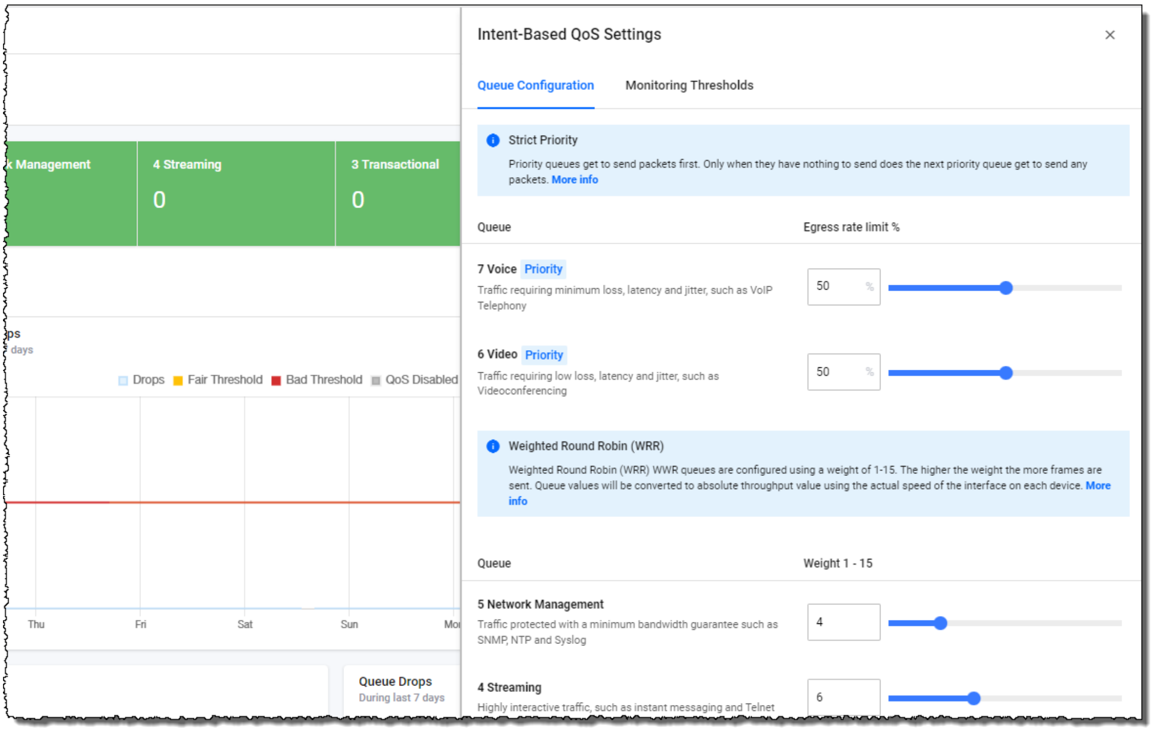
QoS enabled

Drops broken down by queue

Configuring the queue settings

You access the queue settings from the Intent-based QoS dashboard.





Intent-Based QoS Settings

Queue Configuration | Monitoring Thresholds

Strict Priority

Priority queues get to send packets first. Only when they have nothing to send does the next priority queue get to send any packets. More info

Queue	Egress rate limit %
7 Voice Priority Traffic requiring minimum loss, latency and jitter, such as VoIP Telephony	50 %
6 Video Priority Traffic requiring low loss, latency and jitter, such as Videoconferencing	50 %

Weighted Round Robin (WRR)

Weighted Round Robin (WRR) WWR queues are configured using a weight of 1-15. The higher the weight the more frames are sent. Queue values will be converted to absolute throughput value using the actual speed of the interface on each device. More info

Queue	Weight 1 - 15
5 Network Management Traffic protected with a minimum bandwidth guarantee such as SNMP, NTP and Syslog	4
4 Streaming Highly interactive traffic, such as instant messaging and Telnet	6

This is where you set or change queue parameters for Strict Priority egress limits and WRR queue weightings. Any changes you make are pushed out to all devices configured with the QoS policy named: VISTA_DEFAULT_POLICY.

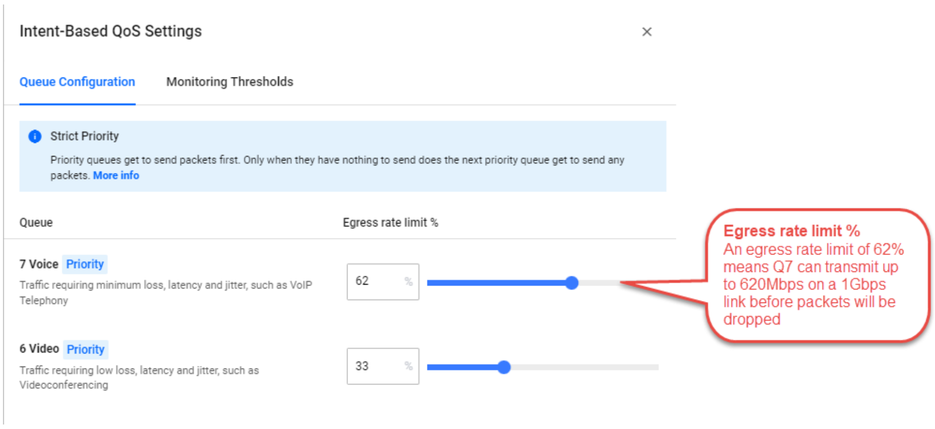
The Intent-based QoS Settings page contains two tabs: **Queue Configuration** and **Monitoring Thresholds**.

Queue Configuration tab

The **Queue Configuration** tab lets you set queue parameters for: Strict Priority (egress rate limiting) and WRR - weighting.

Strict Priority queue settings

Use the Strict Priority queues for traffic requiring minimum loss, latency, and jitter, such as VoIP and video conferencing.



Intent-Based QoS Settings

Strict Priority

Priority queues get to send packets first. Only when they have nothing to send does the next priority queue get to send any packets. More info

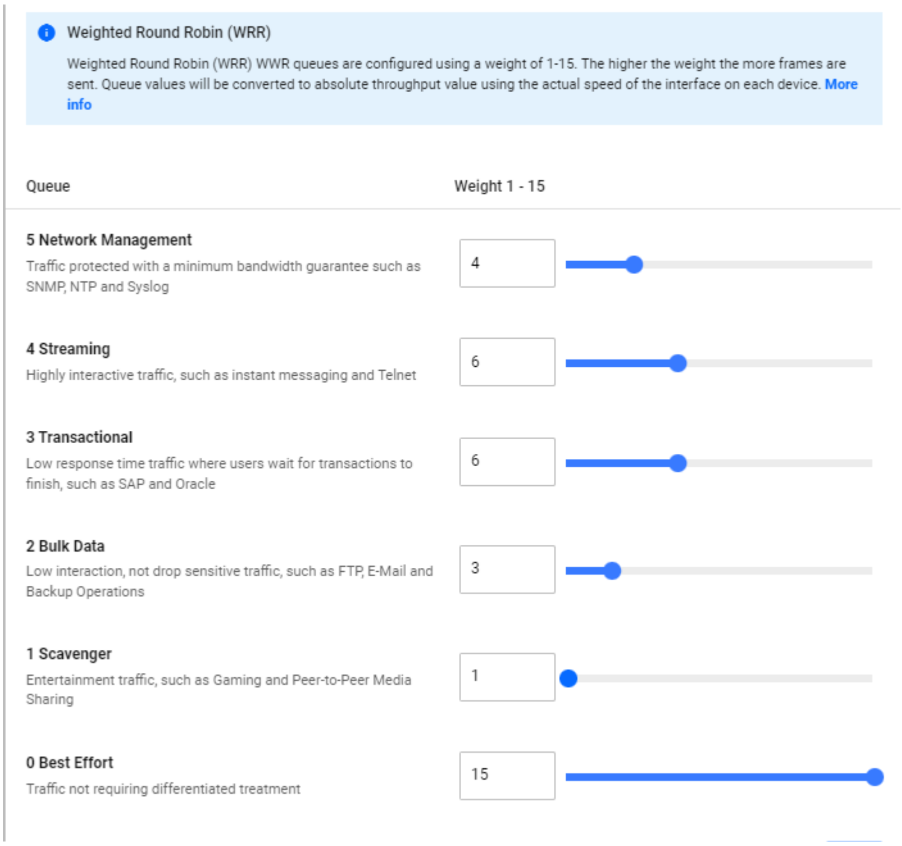
Queue	Egress rate limit %
7 Voice Priority Traffic requiring minimum loss, latency and jitter, such as VoIP Telephony	62 %
6 Video Priority Traffic requiring low loss, latency and jitter, such as Videoconferencing	33 %

Egress rate limit %
An egress rate limit of 62% means Q7 can transmit up to 620Mbps on a 1Gbps link before packets will be dropped

WRR queue settings

Use the WRR queues for:

- Network Management, Streaming, Transactional, Bulk Data, Scavenger, and Best Effort.



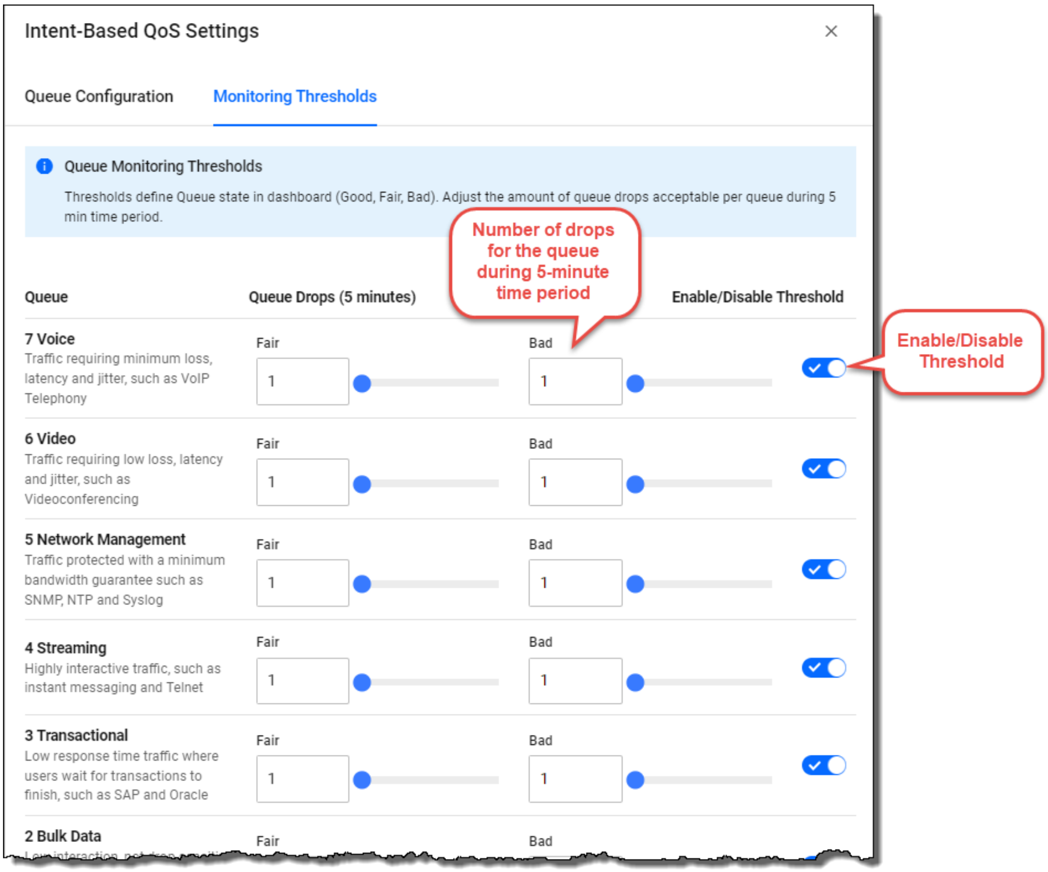
Weighted Round Robin (WRR)

Weighted Round Robin (WRR) WWR queues are configured using a weight of 1-15. The higher the weight the more frames are sent. Queue values will be converted to absolute throughput value using the actual speed of the interface on each device. More info

Queue	Weight 1 - 15
5 Network Management Traffic protected with a minimum bandwidth guarantee such as SNMP, NTP and Syslog	4
4 Streaming Highly interactive traffic, such as instant messaging and Telnet	6
3 Transactional Low response time traffic where users wait for transactions to finish, such as SAP and Oracle	6
2 Bulk Data Low interaction, not drop sensitive traffic, such as FTP, E-Mail and Backup Operations	3
1 Scavenger Entertainment traffic, such as Gaming and Peer-to-Peer Media Sharing	1
0 Best Effort Traffic not requiring differentiated treatment	15

Monitoring Thresholds tab

The **Monitoring Thresholds** tab lets you change the drop threshold for queues. By default, the Fair and Red thresholds are set to 1 drop. This means that if there are >=1 drops, the queue display will show as red.



Intent-Based QoS Settings

Queue Monitoring Thresholds

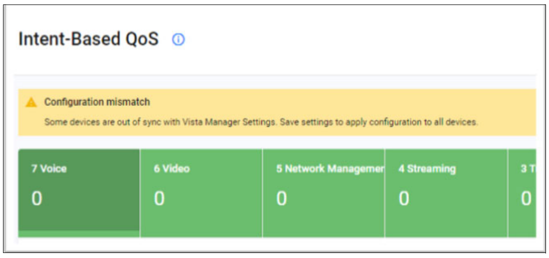
Thresholds define Queue state in dashboard (Good, Fair, Bad). Adjust the amount of queue drops acceptable per queue during 5 min time period.

Queue	Queue Drops (5 minutes)		Enable/Disable Threshold
7 Voice Traffic requiring minimum loss, latency and jitter, such as VoIP Telephony	Fair 1	Bad 1	✓
6 Video Traffic requiring low loss, latency and jitter, such as Videoconferencing	Fair 1	Bad 1	✓
5 Network Management Traffic protected with a minimum bandwidth guarantee such as SNMP, NTP and Syslog	Fair 1	Bad 1	✓
4 Streaming Highly interactive traffic, such as instant messaging and Telnet	Fair 1	Bad 1	✓
3 Transactional Low response time traffic where users wait for transactions to finish, such as SAP and Oracle	Fair 1	Bad 1	✓
2 Bulk Data	Fair	Bad	

Number of drops for the queue during 5-minute time period

Enable/Disable Threshold

Thresholds are applied network-wide and cannot be set on a single device or port. If the QoS configuration is different between device ports, a warning message is displayed in the Intent-Based QoS dashboard.



Intent-Based QoS

Configuration mismatch

Some devices are out of sync with Vista Manager Settings. Save settings to apply configuration to all devices.

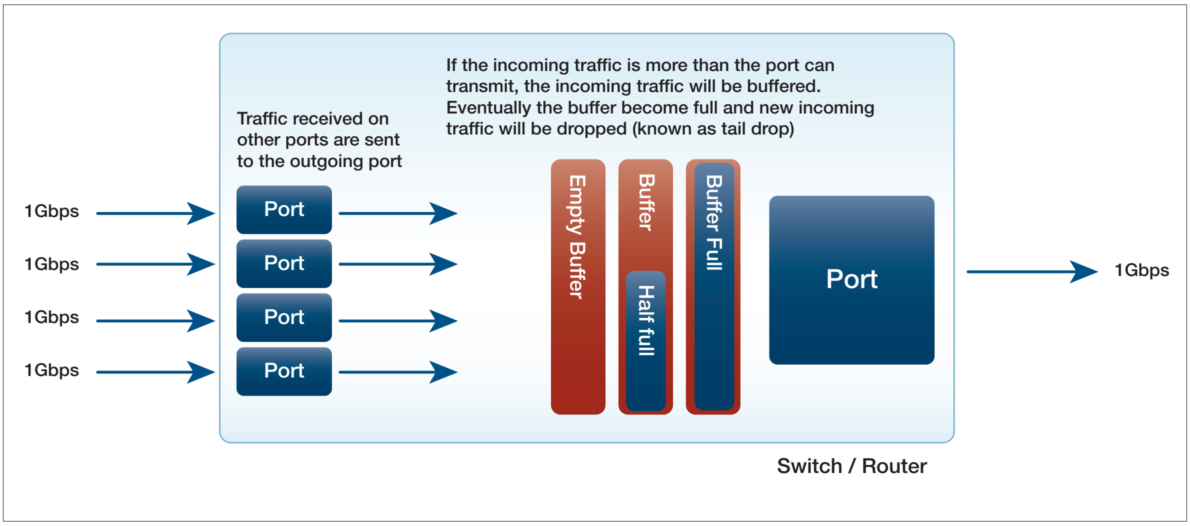
7 Voice	6 Video	5 Network Managemer	4 Streaming	3 T
0	0	0	0	0

Port congestion

When a port receives more traffic than it can transmit, it buffers the traffic until the traffic can be sent. If the buffer becomes full and cannot buffer any more packets, any new incoming packets will be dropped, this is known as tail drop. This can cause two issues:

- **packet delay** - the packet in the buffer is delayed until the port is ready to send it.
- **packet drops** - the packet is dropped and lost forever.

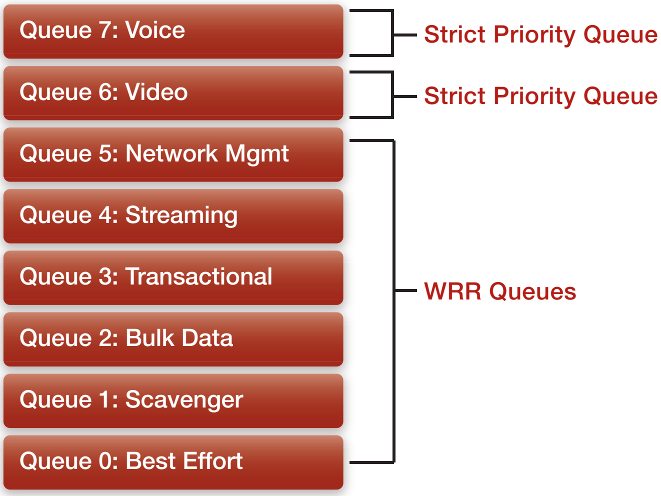
  The transmitting device may choose to resend the lost packet, but this could take some time, because it has to detect the packet has been lost.


If the incoming traffic is more than the port can transmit, the incoming traffic will be buffered. Eventually the buffer become full and new incoming traffic will be dropped (known as tail drop)
Traffic received on other ports are sent to the outgoing port
1Gbps
1Gbps
1Gbps
1Gbps
Port
Port
Port
Port
Empty Buffer
Buffer
Half full
Buffer Full
Port
1Gbps
Switch / Router

Delays and drops result in network degradation, and for some applications can cause serious problems. For example, voice traffic is sensitive to packet loss, so excessive loss will cause a deterioration of voice quality.

Egress queue modelling

Vista Manager's Intent-based QoS uses two strict priority and six WRR queues. The QoS queue types, Strict priority and WRR are described in more detail next.

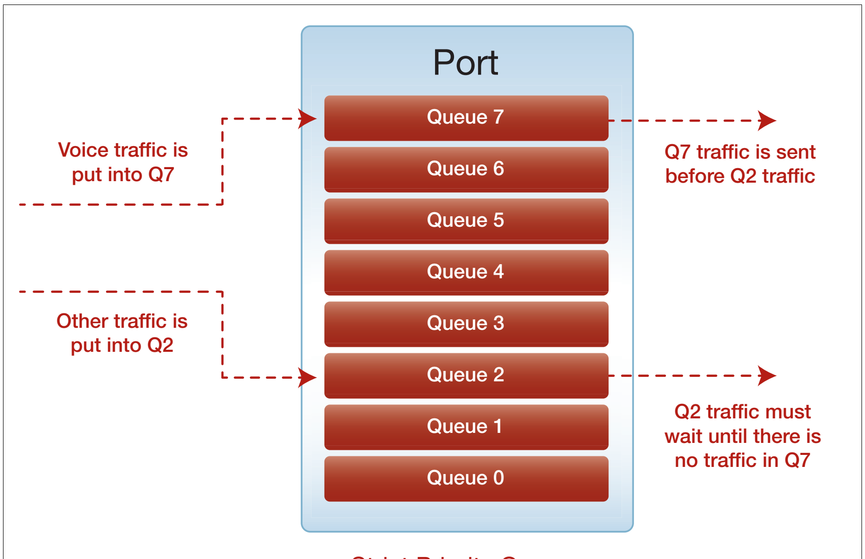


QoS egress queue types

Egress queues help with application performance by allocating a preference to outgoing traffic. For example, voice traffic could be given a high priority so it will be sent before other types of traffic.

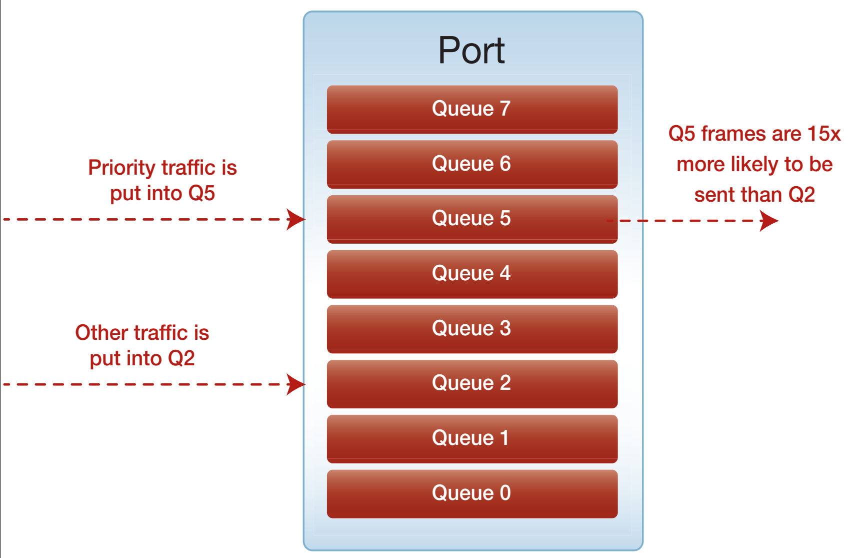
There are two types of egress queues available, strict priority and weighted round robin:

- **Strict priority** - traffic in a higher queue is sent before traffic in a lower queue. The lowest queue is queue 0 and the highest is queue 7.


Port
Queue 7
Queue 6
Queue 5
Queue 4
Queue 3
Queue 2
Queue 1
Queue 0
Voice traffic is put into Q7
Other traffic is put into Q2
Q7 traffic is sent before Q2 traffic
Q2 traffic must wait until there is no traffic in Q7

Strict Priority Queues

- **Weighted round robin** - queues are given a weighting. When the egress interface is congested, the specified weightings act as relative ratios to each other. For example:
  - If Q2 weight = 1 and Q5 weight = 15, then Q5 will send 15 times as much traffic as Q2.
  - If Q2 weight = 15 and Q5 weight = 15, then Q2 and Q5 will send the same amount of traffic.


Port
Queue 7
Queue 6
Queue 5
Queue 4
Queue 3
Queue 2
Queue 1
Queue 0
Priority traffic is put into Q5
Other traffic is put into Q2
Q5 frames are 15x more likely to be sent than Q2

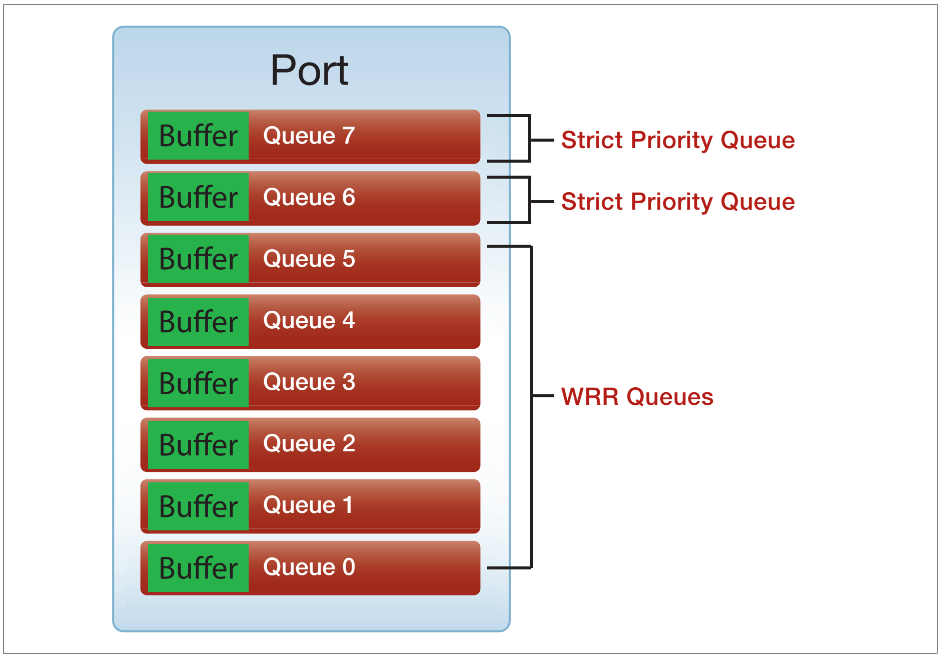
Weight Round Robin Queues

What are the main advantages and disadvantages of WRR and Strict Priority queue types?

The main advantage of strict priority queues is that they ensure that drop sensitive traffic can be forwarded without loss. The difficulty with strict priority queues is that they can lead to starvation of traffic on lower priority queues.

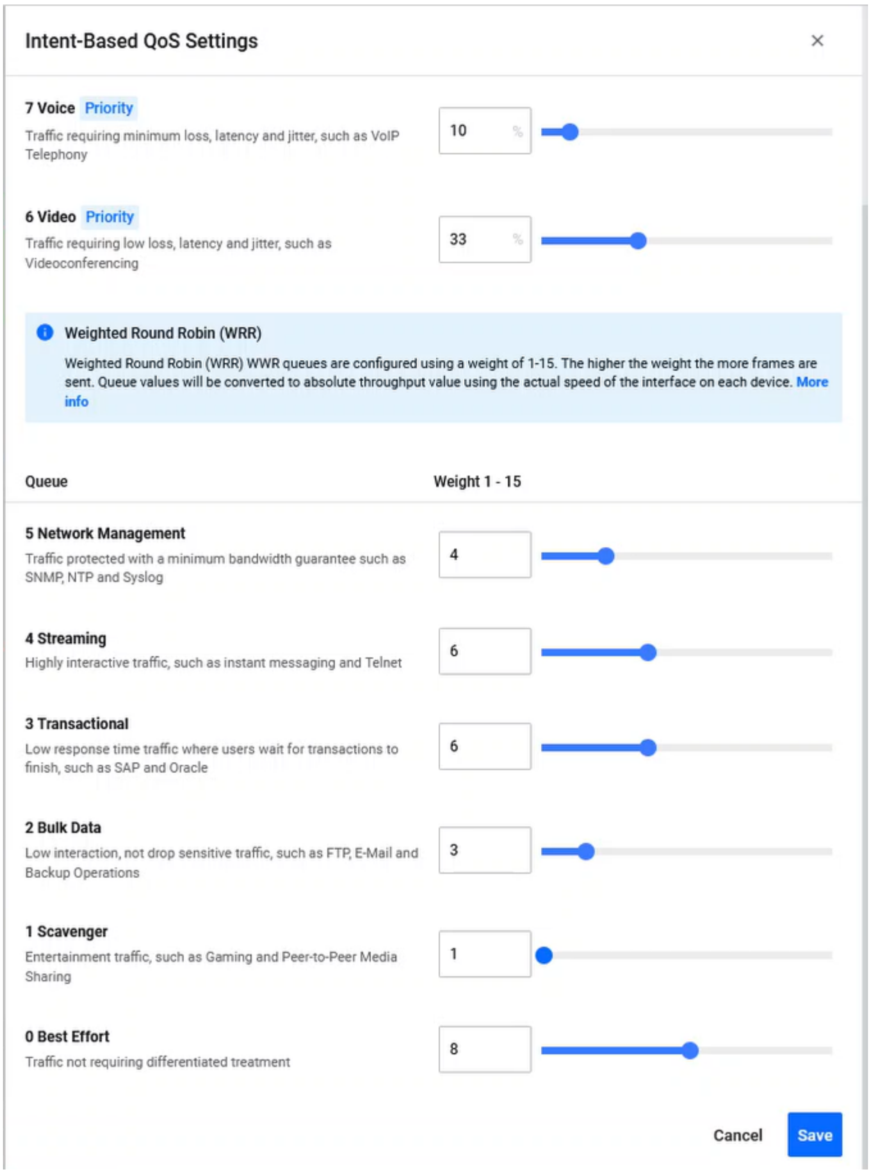
The main advantage of WRR queues is that they ensure that at least some traffic on all queues in a WRR group is sent when congestion occurs, making full starvation of lower priority queues impossible. The difficulty with WRR queues is that some degree of packet-loss occurs on all queues when under congestion, which is problematic for applications sensitive to packet-loss.

Vista Manager EX uses two strict priority queues with egress-rate-limiting and six WRR queues. This ensures forwarding of drop sensitive traffic, while also ensuring that starvation doesn't occur on the lower priority queues.



Default configuration for Intent-based QoS

When you first open the Intent-based QoS Settings page in Vista Manager EX, you will see settings similar to the following:



Intent-Based QoS Settings

7 Voice Priority
Traffic requiring minimum loss, latency and jitter, such as VoIP Telephony
10 %

6 Video Priority
Traffic requiring low loss, latency and jitter, such as Videoconferencing
33 %

Weighted Round Robin (WRR)

Weighted Round Robin (WRR) WWR queues are configured using a weight of 1-15. The higher the weight the more frames are sent. Queue values will be converted to absolute throughput value using the actual speed of the interface on each device. More info

Queue	Weight 1 - 15
5 Network Management Traffic protected with a minimum bandwidth guarantee such as SNMP, NTP and Syslog	4
4 Streaming Highly interactive traffic, such as instant messaging and Telnet	6
3 Transactional Low response time traffic where users wait for transactions to finish, such as SAP and Oracle	6
2 Bulk Data Low interaction, not drop sensitive traffic, such as FTP, E-Mail and Backup Operations	3
1 Scavenger Entertainment traffic, such as Gaming and Peer-to-Peer Media Sharing	1
0 Best Effort Traffic not requiring differentiated treatment	8

The initial default configuration ensures that:

- Packets are marked and put into an appropriate queue.
- Queues types are set and configured with the appropriate weight and bandwidth settings:
  - Strict Priority queues for the high priority traffic (queues 7 Voice and 6 Video).
  - Weighted Round Robin (WRR) queues for the lower priority queues (all other queues).
- Interfaces are configured for QoS.

The next section describes the initial QoS queue and interface configuration steps.

Configuring the Vista default policy

The initial manual configuration includes: enabling QoS on devices, creating a default policy 'VISTA_DEFAULT_POLICY', and applying the default policy to interfaces.

For **all** platforms:

1. Enable QoS on all devices to be managed by Intent-based QoS:

```
mls qos enable
```

2. Create a QoS policy VISTA_DEFAULT_POLICY and apply it to all ports that you want Intent-based QoS to monitor and manage:

```
policy-map VISTA_DEFAULT_POLICY
 trust dscp
 class default
```

3. Set default policy queue weights:

For platforms: x8100, x220 & GS980M, x530 & GS980MX, x320 and GS980EM:

On these platforms the weights can be configured to any multiple of 17 that you choose (between 17 and 255). The reason for this is that AlliedWare Plus platforms, aside from the ones listed above, only support weightings between 1 and 15.

For Vista Manager EX to support both platform weightings - i.e. some between 1 and 15 and some between 17 and 255 in a single network, the number of possible weightings on platforms which support 17 and 255 has to be reduced to 15 possible combinations. 255/17=15, hence why these platforms must be configured as with a weighting which is a multiple of 17.

If the weight is not a multiple of 17, then when the configuration is updated by Vista Manager, it will be updated to a multiple of 17.

- Set the scheduler to configure the WRR queue weights.

```
mls qos scheduler-set 1 wrr-queue group 1 weight 255 queue 0
mls qos scheduler-set 1 wrr-queue group 1 weight 11 queue 1
mls qos scheduler-set 1 wrr-queue group 1 weight 40 queue 2
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queue 3
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queue 4
mls qos scheduler-set 1 wrr-queue group 1 weight 70 queue 5
```

- The QoS policy must then be applied to each interface that will use QoS.

In addition to this the queue weights and egress rate **limits** must be set on each queue. The egress-rate limit can be set to whatever values you choose. Here they are set to 333m and 100m on a 1Gig link, this is equivalent to 33% and 10% of the total bandwidth of this interface.

```
interface port1.0.1
 service-policy input VISTA_DEFAULT_POLICY
 strict-priority-queue egress-rate-limit 333m queues 6
 strict-priority-queue egress-rate-limit 100m queues 7
 mls qos scheduler-set 1
```

- **For other platforms:**

  For other platforms, the configuration is slightly different. Instead of having a scheduler-set the weights, they are applied individually to each interface. The egress-rate limit can be set to whatever values you choose. Here they are set to 333m and 100m on a 1Gig link, this is equivalent to 33% and 10% of the total bandwidth of this interface. The percentage values must be consistent across the entire network. If queue 7 is set to the equivalent of 10% on one interface, then it must be the same percentage for all other interfaces.

```
interface port1.0.1
 service-policy input VISTA_DEFAULT_POLICY
 wrr-queue weight 15 queues 0
 wrr-queue weight 1 queues 1
 wrr-queue weight 3 queues 2
 wrr-queue weight 6 queues 3
 wrr-queue weight 6 queues 4
 wrr-queue weight 4 queues 5
 strict-priority-queue egress-rate-limit 333m queues 6
 strict-priority-queue egress-rate-limit 100m queues 7
```

QoS mapping traffic to the right queue

For platforms: x8100, x220 & GS980M, x530 & GS980MX, x320 and GS980E:

Additionally, you will need to ensure the right traffic ends up on the right queues. Here are two possible ways of doing this, but it's entirely up to you how this is done.

1: Mapping from DSCP values to queues

One way to achieve this is with the following configuration that uses the existing DSCP value on each packet to map the packet into the specified queue.

```
mls qos map premark-dscp 8 to new-queue 1
mls qos map premark-dscp 10 to new-queue 2
mls qos map premark-dscp 12 to new-queue 2
mls qos map premark-dscp 14 to new-queue 2
mls qos map premark-dscp 16 to new-queue 5
mls qos map premark-dscp 18 to new-queue 3
mls qos map premark-dscp 20 to new-queue 3
mls qos map premark-dscp 22 to new-queue 3
mls qos map premark-dscp 24 to new-queue 5
mls qos map premark-dscp 26 to new-queue 4
mls qos map premark-dscp 28 to new-queue 4
mls qos map premark-dscp 30 to new-queue 4
mls qos map premark-dscp 32 to new-queue 6
mls qos map premark-dscp 34 to new-queue 6
mls qos map premark-dscp 36 to new-queue 6
mls qos map premark-dscp 38 to new-queue 6
mls qos map premark-dscp 40 to new-queue 6
mls qos map premark-dscp 46 to new-queue 7
mls qos map premark-dscp 48 to new-queue 5
mls qos map premark-dscp 56 to new-queue 5
```

2: Mapping from CoS to DSCP to queue:

Alternatively, if CoS is being used then it can first be mapped to a DSCP value on the edge of the network, and then on the internal parts of the network, the previous configuration can be used.

To map the CoS values to DSCP values the following configuration can be used, the VISTA_DEFAULT_POLICY will then need to be applied to each interface as described above.

```
mls qos map premark-dscp 8 to new-queue 1
mls qos map premark-dscp 10 to new-queue 2
mls qos map premark-dscp 12 to new-queue 2
mls qos map premark-dscp 14 to new-queue 2
mls qos map premark-dscp 16 to new-queue 5
mls qos map premark-dscp 18 to new-queue 3
mls qos map premark-dscp 20 to new-queue 3
mls qos map premark-dscp 22 to new-queue 3
mls qos map premark-dscp 24 to new-queue 5
mls qos map premark-dscp 26 to new-queue 4
mls qos map premark-dscp 28 to new-queue 4
mls qos map premark-dscp 30 to new-queue 4
mls qos map premark-dscp 32 to new-queue 6
mls qos map premark-dscp 34 to new-queue 6
mls qos map premark-dscp 36 to new-queue 6
mls qos map premark-dscp 38 to new-queue 6
mls qos map premark-dscp 40 to new-queue 6
mls qos map premark-dscp 46 to new-queue 7
mls qos map premark-dscp 48 to new-queue 5
mls qos map premark-dscp 56 to new-queue 5
mls qos scheduler-set 1 wrr-queue group 1 weight 255 queues 0
mls qos scheduler-set 1 wrr-queue group 1 weight 11 queues 1
mls qos scheduler-set 1 wrr-queue group 1 weight 40 queues 2
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queues 3
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queues 4
mls qos scheduler-set 1 wrr-queue group 1 weight 70 queues 5
class-map COS-DSCP_TRANSLATE_7
 match cos 7

class-map COS-DSCP_TRANSLATE_6
 match cos 6

class-map COS-DSCP_TRANSLATE_5
 match cos 5

class-map COS-DSCP_TRANSLATE_4
 match cos 4

class-map COS-DSCP_TRANSLATE_3
 match cos 3

class-map COS-DSCP_TRANSLATE_2
 match cos 2

class-map COS-DSCP_TRANSLATE_1
 match cos 1

policy-map VISTA_DEFAULT_POLICY
 trust dscp
 class default
 class COS-DSCP_TRANSLATE_7
  set dscp 56
  set queue 5
 class COS-DSCP_TRANSLATE_6
  set dscp 48
  set queue 5
 class COS-DSCP_TRANSLATE_5
  set dscp 46
  set queue 7
 class COS-DSCP_TRANSLATE_4
  set dscp 34
  set queue 6
 class COS-DSCP_TRANSLATE_3
  set dscp 26
  set queue 4
 class COS-DSCP_TRANSLATE_2
  set dscp 18
  set queue 3
 class COS-DSCP_TRANSLATE_1
  set dscp 10
  set queue 2
```

QoS mapping traffic to the right queue - For other platforms

1: Mapping from DSCP values to queues

```
mls qos map cos-queue 0 to 0
mls qos map cos-queue 1 to 1
mls qos map cos-queue 2 to 2
mls qos enable
mls qos map premark-dscp 8 to new-cos 1
mls qos map premark-dscp 10 to new-cos 2
mls qos map premark-dscp 12 to new-cos 2
mls qos map premark-dscp 14 to new-cos 2
mls qos map premark-dscp 16 to new-cos 5
mls qos map premark-dscp 18 to new-cos 3
mls qos map premark-dscp 20 to new-cos 3
mls qos map premark-dscp 22 to new-cos 3
mls qos map premark-dscp 24 to new-cos 5
mls qos map premark-dscp 26 to new-cos 4
mls qos map premark-dscp 28 to new-cos 4
mls qos map premark-dscp 30 to new-cos 4
mls qos map premark-dscp 32 to new-cos 6
mls qos map premark-dscp 34 to new-cos 6
mls qos map premark-dscp 36 to new-cos 6
mls qos map premark-dscp 38 to new-cos 6
mls qos map premark-dscp 40 to new-cos 6
mls qos map premark-dscp 46 to new-cos 7
mls qos map premark-dscp 48 to new-cos 5
mls qos map premark-dscp 56 to new-cos 5
```

2: Mapping from DSCP values to queues

```
mls qos map cos-queue 0 to 0
mls qos map cos-queue 1 to 1
mls qos map cos-queue 2 to 2
mls qos enable
mls qos map premark-dscp 8 to new-cos 1
mls qos map premark-dscp 10 to new-cos 2
mls qos map premark-dscp 12 to new-cos 2
mls qos map premark-dscp 14 to new-cos 2
mls qos map premark-dscp 16 to new-cos 5
mls qos map premark-dscp 18 to new-cos 3
mls qos map premark-dscp 20 to new-cos 3
mls qos map premark-dscp 22 to new-cos 3
mls qos map premark-dscp 24 to new-cos 5
mls qos map premark-dscp 26 to new-cos 4
mls qos map premark-dscp 28 to new-cos 4
mls qos map premark-dscp 30 to new-cos 4
mls qos map premark-dscp 32 to new-cos 6
mls qos map premark-dscp 34 to new-cos 6
mls qos map premark-dscp 36 to new-cos 6
mls qos map premark-dscp 38 to new-cos 6
mls qos map premark-dscp 40 to new-cos 6
mls qos map premark-dscp 46 to new-cos 7
mls qos map premark-dscp 48 to new-cos 5
mls qos map premark-dscp 56 to new-cos 5
!
class-map COS_7
 match cos 7
!
class-map COS_6
 match cos 6
!
class-map COS_5
 match cos 5
!
class-map COS_4
 match cos 4
!
class-map COS_3
 match cos 3
!
class-map COS_2
 match cos 2
!
class-map COS_1
 match cos 1
!
class-map EF
 match dscp 46
!
class-map CS7
 match dscp 56
!
class-map CS6
 match dscp 48
!
class-map CS5
 match dscp 40
!
class-map CS4
 match dscp 32
!
class-map CS3
 match dscp 24
!
class-map CS2
 match dscp 16
!
class-map CS1
 match dscp 8
!
class-map AF41
 match dscp 34
!
class-map AF42
 match dscp 36
!
class-map AF43
 match dscp 38
!
```

```
class-map AF31
 match dscp 26
!
class-map AF32
 match dscp 28
!
class-map AF33
 match dscp 30
!
class-map AF21
 match dscp 18
!
class-map AF22
 match dscp 20
!
class-map AF23
 match dscp 22
!
class-map AF11
 match dscp 10
!
class-map AF12
 match dscp 12
!
class-map AF13
 match dscp 14
!
policy-map VISTA_DEFAULT_POLICY
 class default
  remark new-cos 0 internal
 class COS_7
  remark new-cos 5 internal
  remark-map to new-dscp 56
 class COS_6
  remark new-cos 5 internal
  remark-map to new-dscp 48
 class COS_5
  remark new-cos 7 internal
  remark-map to new-dscp 46
 class COS_4
  remark new-cos 6 internal
  remark-map to new-dscp 34
 class COS_3
  remark new-cos 4 internal
  remark-map to new-dscp 26
 class COS_2
  remark new-cos 3 internal
  remark-map to new-dscp 18
 class COS_1
  remark new-cos 2 internal
  remark-map to new-dscp 10
 class EF
  remark new-cos 7 internal
 class CS7
  remark new-cos 5 internal
 class CS6
  remark new-cos 5 internal
 class CS3
  remark new-cos 5 internal
 class CS2
  remark new-cos 5 internal
 class CS5
  remark new-cos 6 internal
 class CS4
  remark new-cos 6 internal
 class AF41
  remark new-cos 6 internal
 class AF42
  remark new-cos 6 internal
 class AF43
  remark new-cos 6 internal
 class AF31
  remark new-cos 4 internal
 class AF32
  remark new-cos 4 internal
 class AF33
  remark new-cos 4 internal
 class AF21
  remark new-cos 3 internal
 class AF22
  remark new-cos 3 internal
 class AF23
  remark new-cos 3 internal
 class AF11
  remark new-cos 2 internal
 class AF12
  remark new-cos 2 internal
 class AF13
  remark new-cos 2 internal
 class CS1
  remark new-cos 1 internal
```

Complete configuration example - for the x220 and x230 series switches

You could use the following configuration on an access switch. The configuration for distribution and core switches would largely be identical, except that the configured egress-rate-limiting would occur on all ports, not just on uplinks.

x220 - Access CoS to DSCP

```
x230#show run
!
service password-encryption
!
hostname x230
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
!
!
!
ip domain-lookup
!
!
!
no service dhcp-server
!
spanning-tree mode rstp
!
service power-inline
no lacp global-passive-mode enable
!
mls qos map cos-queue 0 to 0
mls qos map cos-queue 1 to 1
mls qos map cos-queue 2 to 2
mls qos enable
mls qos map premark-dscp 8 to new-cos 1
mls qos map premark-dscp 10 to new-cos 2
mls qos map premark-dscp 12 to new-cos 2
mls qos map premark-dscp 14 to new-cos 2
mls qos map premark-dscp 16 to new-cos 5
mls qos map premark-dscp 18 to new-cos 3
mls qos map premark-dscp 20 to new-cos 3
mls qos map premark-dscp 22 to new-cos 3
mls qos map premark-dscp 24 to new-cos 5
mls qos map premark-dscp 26 to new-cos 4
mls qos map premark-dscp 28 to new-cos 4
mls qos map premark-dscp 30 to new-cos 4
mls qos map premark-dscp 32 to new-cos 6
mls qos map premark-dscp 34 to new-cos 6
mls qos map premark-dscp 36 to new-cos 6
mls qos map premark-dscp 38 to new-cos 6
mls qos map premark-dscp 40 to new-cos 6
mls qos map premark-dscp 46 to new-cos 7
mls qos map premark-dscp 48 to new-cos 5
mls qos map premark-dscp 56 to new-cos 5
!
class-map COS_7
 match cos 7
!
class-map COS_6
 match cos 6
!
class-map COS_5
 match cos 5
!
class-map COS_4
 match cos 4
!
class-map COS_3
 match cos 3
!
class-map COS_2
 match cos 2
!
class-map COS_1
 match cos 1
!
class-map EF
 match dscp 46
!
class-map CS7
 match dscp 56
!
class-map CS6
 match dscp 48
!
class-map CS5
 match dscp 40
!
class-map CS4
 match dscp 32
!
class-map CS3
 match dscp 24
!
class-map CS2
 match dscp 16
!
class-map CS1
 match dscp 8
!
class-map AF41
 match dscp 34
!
class-map AF42
 match dscp 36
!
```

```
class-map AF43
 match dscp 38
!
class-map AF31
 match dscp 26
!
class-map AF32
 match dscp 28
!
class-map AF33
 match dscp 30
!
class-map AF21
 match dscp 18
!
class-map AF22
 match dscp 20
!
class-map AF23
 match dscp 22
!
class-map AF11
 match dscp 10
!
class-map AF12
 match dscp 12
!
class-map AF13
 match dscp 14
!
policy-map VISTA_DEFAULT_POLICY
 class default
  remark new-cos 0 internal
 class COS_7
  remark new-cos 5 internal
  remark-map to new-dscp 56
 class COS_6
  remark new-cos 5 internal
  remark-map to new-dscp 48
 class COS_5
  remark new-cos 7 internal
  remark-map to new-dscp 46
 class COS_4
  remark new-cos 6 internal
  remark-map to new-dscp 34
 class COS_3
  remark new-cos 4 internal
  remark-map to new-dscp 26
 class COS_2
  remark new-cos 3 internal
  remark-map to new-dscp 18
 class COS_1
  remark new-cos 2 internal
  remark-map to new-dscp 10
 class EF
  remark new-cos 7 internal
 class CS7
  remark new-cos 5 internal
 class CS6
  remark new-cos 5 internal
 class CS3
  remark new-cos 5 internal
 class CS2
  remark new-cos 5 internal
 class CS5
  remark new-cos 6 internal
 class CS4
  remark new-cos 6 internal
 class AF41
  remark new-cos 6 internal
 class AF42
  remark new-cos 6 internal
 class AF43
  remark new-cos 6 internal
 class AF31
  remark new-cos 4 internal
 class AF32
  remark new-cos 4 internal
 class AF33
  remark new-cos 4 internal
 class AF21
  remark new-cos 3 internal
 class AF22
  remark new-cos 3 internal
 class AF23
  remark new-cos 3 internal
 class AF11
  remark new-cos 2 internal
 class AF12
  remark new-cos 2 internal
 class AF13
  remark new-cos 2 internal
 class CS1
  remark new-cos 1 internal
!
!
interface port1.0.1-1.0.16
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
!
interface port1.0.17-1.0.18
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
 wrr-queue weight 15 queues 0
 wrr-queue weight 1 queues 1
 wrr-queue weight 3 queues 2
 wrr-queue weight 6 queues 3
 wrr-queue weight 6 queues 4
 wrr-queue weight 4 queues 5
 wrr-queue egress-rate-limit 333m queues 6
 wrr-queue egress-rate-limit 100m queues 7
!
!
line con 0
line vty 0 4
!
end
```

x220 Access basic

```
x220#show run
!
service password-encryption
!
hostname x220
```

```
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
!
!
!
ip domain-lookup
!
!
spanning-tree mode rstp
!
service power-inline
lacp global-passive-mode enable
!
mls qos enable
mls qos map premark-dscp 8 to new-queue 1
mls qos map premark-dscp 10 to new-queue 2
mls qos map premark-dscp 12 to new-queue 2
mls qos map premark-dscp 14 to new-queue 2
mls qos map premark-dscp 16 to new-queue 5
mls qos map premark-dscp 18 to new-queue 3
mls qos map premark-dscp 20 to new-queue 3
mls qos map premark-dscp 22 to new-queue 3
mls qos map premark-dscp 24 to new-queue 5
mls qos map premark-dscp 26 to new-queue 4
mls qos map premark-dscp 28 to new-queue 4
mls qos map premark-dscp 30 to new-queue 4
mls qos map premark-dscp 32 to new-queue 6
mls qos map premark-dscp 34 to new-queue 6
mls qos map premark-dscp 36 to new-queue 6
mls qos map premark-dscp 38 to new-queue 6
mls qos map premark-dscp 40 to new-queue 6
mls qos map premark-dscp 46 to new-queue 7
mls qos map premark-dscp 48 to new-queue 5
mls qos map premark-dscp 56 to new-queue 5
mls qos scheduler-set 1 wrr-queue group 1 weight 255 queues 0
mls qos scheduler-set 1 wrr-queue group 1 weight 11 queues 1
mls qos scheduler-set 1 wrr-queue group 1 weight 40 queues 2
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queues 3
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queues 4
mls qos scheduler-set 1 wrr-queue group 1 weight 70 queues 5
!
!
policy-map VISTA_DEFAULT_POLICY
 trust dscp
 class default
!
interface port1.0.1-1.0.47
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
!
interface port1.0.48-1.0.50
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
 wrr-queue egress-rate-limit 333m queues 6
 wrr-queue egress-rate-limit 100m queues 7
 mls qos scheduler-set 1
!
interface port1.0.51-1.0.52
 switchport
 switchport mode access
!
line con 0
line vty 0 4
!
end
```

x220 Distribution or Core basic

```
x220#show run
!
service password-encryption
!
hostname x220
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
!
!
!
ip domain-lookup
!
!
spanning-tree mode rstp
!
```

```
service power-inline
lacp global-passive-mode enable
!
mls qos enable
mls qos map premark-dscp 8 to new-queue 1
mls qos map premark-dscp 10 to new-queue 2
mls qos map premark-dscp 12 to new-queue 2
mls qos map premark-dscp 14 to new-queue 2
mls qos map premark-dscp 16 to new-queue 5
mls qos map premark-dscp 18 to new-queue 3
mls qos map premark-dscp 20 to new-queue 3
mls qos map premark-dscp 22 to new-queue 3
mls qos map premark-dscp 24 to new-queue 5
mls qos map premark-dscp 26 to new-queue 4
mls qos map premark-dscp 28 to new-queue 4
mls qos map premark-dscp 30 to new-queue 4
mls qos map premark-dscp 32 to new-queue 6
mls qos map premark-dscp 34 to new-queue 6
mls qos map premark-dscp 36 to new-queue 6
mls qos map premark-dscp 38 to new-queue 6
mls qos map premark-dscp 40 to new-queue 6
mls qos map premark-dscp 46 to new-queue 7
mls qos map premark-dscp 48 to new-queue 5
mls qos map premark-dscp 56 to new-queue 5
mls qos scheduler-set 1 wrr-queue group 1 weight 255 queues 0
mls qos scheduler-set 1 wrr-queue group 1 weight 11 queues 1
mls qos scheduler-set 1 wrr-queue group 1 weight 40 queues 2
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queues 3
mls qos scheduler-set 1 wrr-queue group 1 weight 104 queues 4
mls qos scheduler-set 1 wrr-queue group 1 weight 70 queues 5
!
!
policy-map VISTA_DEFAULT_POLICY
 trust dscp
 class default
!
interface port1.0.1-1.0.50
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
 wrr-queue egress-rate-limit 333m queues 6
 wrr-queue egress-rate-limit 100m queues 7
 mls qos scheduler-set 1
!
interface port1.0.51-1.0.52
 switchport
 switchport mode access
!
line con 0
line vty 0 4
!
end
```

x230 Access CoS to DSCP

```
x230#show run
!
service password-encryption
!
hostname x230
!
no banner motd
```

```
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
!
!
!
ip domain-lookup
!
!
!
no service dhcp-server
!
spanning-tree mode rstp
!
service power-inline
no lacp global-passive-mode enable
!
mls qos map cos-queue 0 to 0
mls qos map cos-queue 1 to 1
mls qos map cos-queue 2 to 2
mls qos enable
mls qos map premark-dscp 8 to new-cos 1
mls qos map premark-dscp 10 to new-cos 2
mls qos map premark-dscp 12 to new-cos 2
mls qos map premark-dscp 14 to new-cos 2
mls qos map premark-dscp 16 to new-cos 5
mls qos map premark-dscp 18 to new-cos 3
mls qos map premark-dscp 20 to new-cos 3
mls qos map premark-dscp 22 to new-cos 3
mls qos map premark-dscp 24 to new-cos 5
mls qos map premark-dscp 26 to new-cos 4
mls qos map premark-dscp 28 to new-cos 4
mls qos map premark-dscp 30 to new-cos 4
mls qos map premark-dscp 32 to new-cos 6
mls qos map premark-dscp 34 to new-cos 6
mls qos map premark-dscp 36 to new-cos 6
mls qos map premark-dscp 38 to new-cos 6
mls qos map premark-dscp 40 to new-cos 6
mls qos map premark-dscp 46 to new-cos 7
mls qos map premark-dscp 48 to new-cos 5
mls qos map premark-dscp 56 to new-cos 5
!
class-map COS_7
 match cos 7
!
class-map COS_6
 match cos 6
```

```
!
class-map COS_5
 match cos 5
!
class-map COS_4
 match cos 4
!
class-map COS_3
 match cos 3
!
class-map COS_2
 match cos 2
!
class-map COS_1
 match cos 1
!
class-map EF
 match dscp 46
!
class-map CS7
 match dscp 56
!
class-map CS6
 match dscp 48
!
class-map CS5
 match dscp 40
!
class-map CS4
 match dscp 32
!
class-map CS3
 match dscp 24
!
class-map CS2
 match dscp 16
!
class-map CS1
 match dscp 8
!
class-map AF41
 match dscp 34
!
class-map AF42
 match dscp 36
!
class-map AF43
 match dscp 38
!
class-map AF31
 match dscp 26
!
class-map AF32
 match dscp 28
!
class-map AF33
 match dscp 30
!
class-map AF21
 match dscp 18
!
class-map AF22
 match dscp 20
!
```

```
class-map AF23
 match dscp 22
!
class-map AF11
 match dscp 10
!
class-map AF12
 match dscp 12
!
class-map AF13
 match dscp 14
!
policy-map VISTA_DEFAULT_POLICY_DOWNLINK
 class default
  remark new-cos 0 internal
 class COS_7
  remark new-cos 5 internal
  remark-map to new-dscp 56
 class COS_6
  remark new-cos 5 internal
  remark-map to new-dscp 48
 class COS_5
  remark new-cos 7 internal
  remark-map to new-dscp 46
 class COS_4
  remark new-cos 6 internal
  remark-map to new-dscp 34
 class COS_3
  remark new-cos 4 internal
  remark-map to new-dscp 26
 class COS_2
  remark new-cos 3 internal
  remark-map to new-dscp 18
 class COS_1
  remark new-cos 2 internal
  remark-map to new-dscp 10
 class EF
  remark new-cos 7 internal
 class CS7
  remark new-cos 5 internal
 class CS6
  remark new-cos 5 internal
 class CS3
  remark new-cos 5 internal
 class CS2
  remark new-cos 5 internal
 class CS5
  remark new-cos 6 internal
 class CS4
  remark new-cos 6 internal
 class AF41
  remark new-cos 6 internal
 class AF42
  remark new-cos 6 internal
 class AF43
  remark new-cos 6 internal
 class AF31
  remark new-cos 4 internal
 class AF32
  remark new-cos 4 internal
 class AF33
  remark new-cos 4 internal
 class AF21
  remark new-cos 3 internal
 class AF22
  remark new-cos 3 internal
 class AF23
  remark new-cos 3 internal
 class AF11
  remark new-cos 2 internal
 class AF12
  remark new-cos 2 internal
 class AF13
  remark new-cos 2 internal
 class CS1
  remark new-cos 1 internal
!
policy-map VISTA_DEFAULT_POLICY_UPLINK
 trust dscp
 class default
!
interface port1.0.1-1.0.16
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY_DOWNLINK
!
interface port1.0.17-1.0.18
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY_UPLINK
 wrr-queue weight 15 queues 0
 wrr-queue weight 1 queues 1
 wrr-queue weight 3 queues 2
 wrr-queue weight 6 queues 3
 wrr-queue weight 6 queues 4
 wrr-queue weight 4 queues 5
 wrr-queue egress-rate-limit 333m queues 6
 wrr-queue egress-rate-limit 100m queues 7
!!
line con 0
line vty 0 4
!
end
```

x230 Access basic

```
    !
service password-encryption
!
hostname x230
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
aaa authentication enable default local
aaa authentication login default local
```

```
!
ip domain-lookup
!
!
!
no service dhcp-server
!
spanning-tree mode rstp
!
service power-inline
no lacp global-passive-mode enable
!
mls qos map cos-queue 0 to 0
mls qos map cos-queue 1 to 1
mls qos map cos-queue 2 to 2
mls qos enable
mls qos map premark-dscp 8 to new-cos 1
mls qos map premark-dscp 10 to new-cos 2
mls qos map premark-dscp 12 to new-cos 2
mls qos map premark-dscp 14 to new-cos 2
mls qos map premark-dscp 16 to new-cos 5
mls qos map premark-dscp 18 to new-cos 3
mls qos map premark-dscp 20 to new-cos 3
mls qos map premark-dscp 22 to new-cos 3
mls qos map premark-dscp 24 to new-cos 5
mls qos map premark-dscp 26 to new-cos 4
mls qos map premark-dscp 28 to new-cos 4
mls qos map premark-dscp 30 to new-cos 4
mls qos map premark-dscp 32 to new-cos 6
mls qos map premark-dscp 34 to new-cos 6
mls qos map premark-dscp 36 to new-cos 6
mls qos map premark-dscp 38 to new-cos 6
mls qos map premark-dscp 40 to new-cos 6
mls qos map premark-dscp 46 to new-cos 7
mls qos map premark-dscp 48 to new-cos 5
mls qos map premark-dscp 56 to new-cos 5
!
policy-map VISTA_DEFAULT_POLICY
 trust dscp
 class default
!
interface port1.0.1-1.0.16
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
!
interface port1.0.17-1.0.18
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
 wrr-queue weight 15 queues 0
 wrr-queue weight 1 queues 1
 wrr-queue weight 3 queues 2
 wrr-queue weight 6 queues 3
 wrr-queue weight 6 queues 4
 wrr-queue weight 4 queues 5
 wrr-queue egress-rate-limit 333m queues 6
 wrr-queue egress-rate-limit 100m queues 7
!
line con 0
line vty 0 4
!
end
```

x230 Distribution or Core basic

```
    !
service password-encryption
!
hostname x230
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
!
!
aaa authentication enable default local
aaa authentication login default local
!
!
!
!
!
ip domain-lookup
!
!
!
no service dhcp-server
!
spanning-tree mode rstp
!
service power-inline
no lacp global-passive-mode enable
!
mls qos map cos-queue 0 to 0
mls qos map cos-queue 1 to 1
mls qos map cos-queue 2 to 2
mls qos enable
mls qos map premark-dscp 8 to new-cos 1
mls qos map premark-dscp 10 to new-cos 2
mls qos map premark-dscp 12 to new-cos 2
mls qos map premark-dscp 14 to new-cos 2
mls qos map premark-dscp 16 to new-cos 5
mls qos map premark-dscp 18 to new-cos 3
mls qos map premark-dscp 20 to new-cos 3
mls qos map premark-dscp 22 to new-cos 3
mls qos map premark-dscp 24 to new-cos 5
mls qos map premark-dscp 26 to new-cos 4
mls qos map premark-dscp 28 to new-cos 4
mls qos map premark-dscp 30 to new-cos 4
mls qos map premark-dscp 32 to new-cos 6
mls qos map premark-dscp 34 to new-cos 6
mls qos map premark-dscp 36 to new-cos 6
mls qos map premark-dscp 38 to new-cos 6
mls qos map premark-dscp 40 to new-cos 6
mls qos map premark-dscp 46 to new-cos 7
mls qos map premark-dscp 48 to new-cos 5
mls qos map premark-dscp 56 to new-cos 5
!
policy-map VISTA_DEFAULT_POLICY
 trust dscp
 class default
!
interface port1.0.1-1.0.18
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
 wrr-queue weight 15 queues 0
 wrr-queue weight 1 queues 1
 wrr-queue weight 3 queues 2
 wrr-queue weight 6 queues 3
 wrr-queue weight 6 queues 4
 wrr-queue weight 4 queues 5
 wrr-queue egress-rate-limit 333m queues 6
 wrr-queue egress-rate-limit 100m queues 7
!
line con 0
line vty 0 4
!
end
```

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, sub-interface, 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.

STATUS	DESCRIPTION
`tunnel mode ipsec`	Must be only this mode, and either ipv4 or ipv6. Must match the config of the other end of the tunnel.
`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 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
!
```

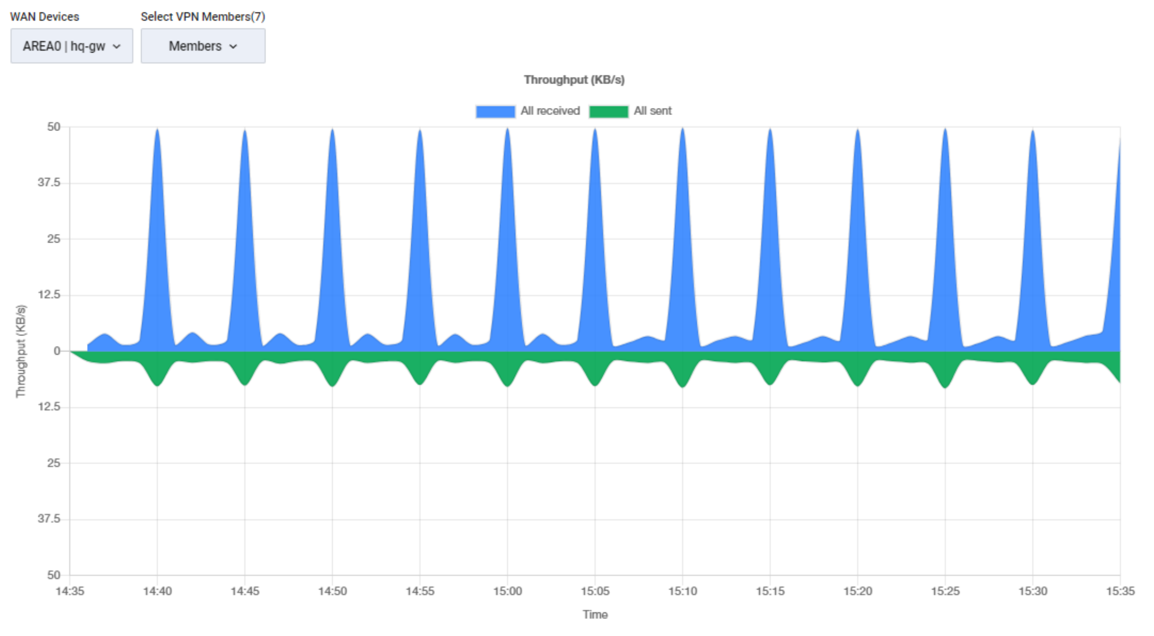
```
vlan database
vlan 4000 name testNet
vlan 4000 state enable
!
interface port1.0.1
switchport
switchport mode access
switchport access vlan 4000
!
interface port1.0.2-1.0.6
switchport
switchport mode access
!
interface port1.0.7
switchport
switchport mode trunk
switchport atmf-link
!

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.

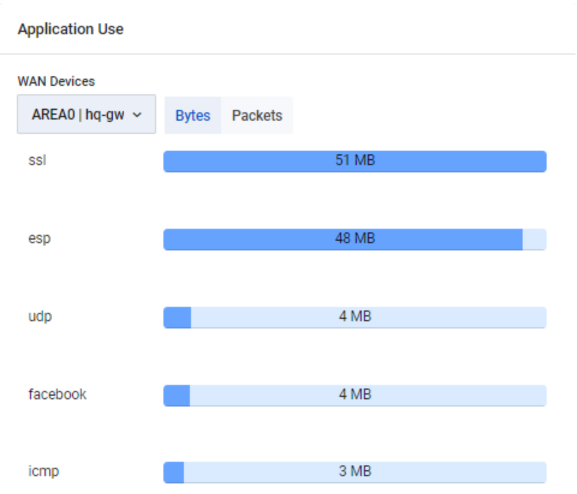
You can also choose the time-frame you wish to display; either the last 1 hour, the last 12 hours, the last 24 hours, or a custom range.



WAN Devices: AREA0 | hq-gw

Select VPN Members(7): Members

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

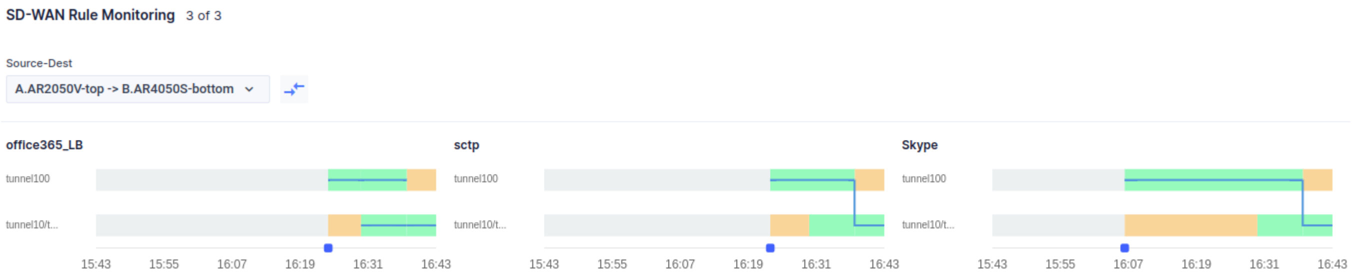


Application Use

WAN Devices: AREA0 | hq-gw

ssl	51 MB
esp	48 MB
udp	4 MB
facebook	4 MB
icmp	3 MB

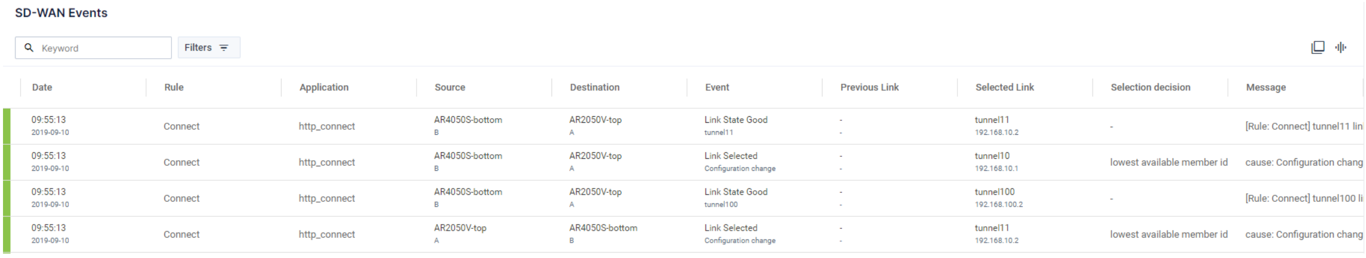
The application use chart shows the amount of data sent and received for a device, broken down by application.You can select which device to view from the WAN Devices drop-down. You can also choose whether to view bytes or packets by choosing the appropriate toggle.



SD-WAN Rule Monitoring 3 of 3

Source-Dest: A.AR2050V-top -> B.AR4050S-bottom

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.



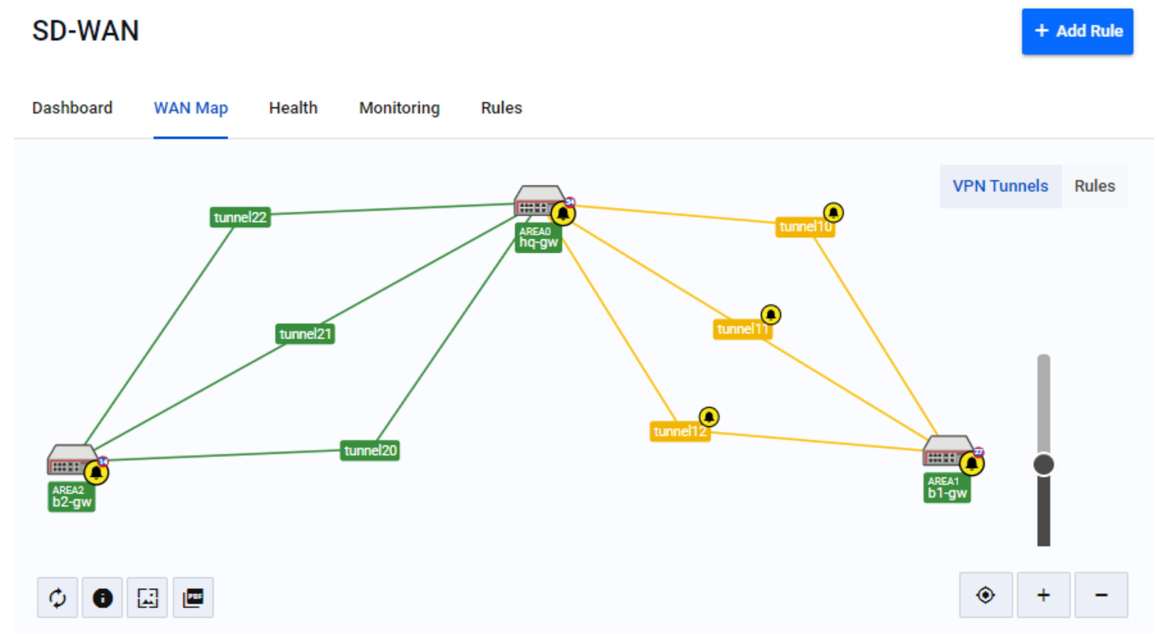
SD-WAN Events

Date	Rule	Application	Source	Destination	Event	Previous Link	Selected Link	Selection decision	Message
09:55:13 2019-09-10	Connect	http_connect	AR4050S-bottom B	AR2050V-top A	Link State Good tunnel11	- -	tunnel11 192.168.10.2	-	[Rule: Connect] tunnel11 lin
09:55:13 2019-09-10	Connect	http_connect	AR4050S-bottom B	AR2050V-top A	Link Selected Configuration change	- -	tunnel10 192.168.10.1	lowest available member id	cause: Configuration chang
09:55:13 2019-09-10	Connect	http_connect	AR4050S-bottom B	AR2050V-top A	Link State Good tunnel100	- -	tunnel100 192.168.100.2	-	[Rule: Connect] tunnel100 li
09:55:13 2019-09-10	Connect	http_connect	AR2050V-top A	AR4050S-bottom B	Link Selected Configuration change	- -	tunnel11 192.168.10.2	lowest available member id	cause: Configuration chang

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

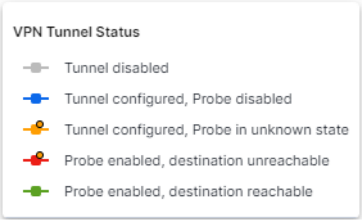
The SD-WAN topology map gives you a visual overview of your network.



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.



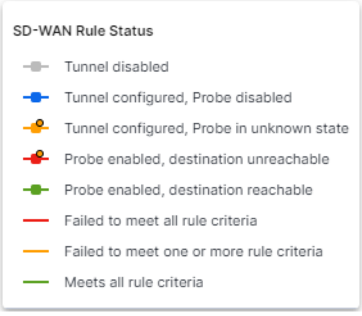
VPN Tunnel Status

- Tunnel disabled
- Tunnel configured, Probe disabled
- Tunnel configured, Probe in unknown state
- Probe enabled, destination unreachable
- Probe enabled, destination reachable

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

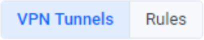
As with the VPN Tunnel Status, you can click on the Information button to bring up a key explaining each of the colors.



SD-WAN Rule Status

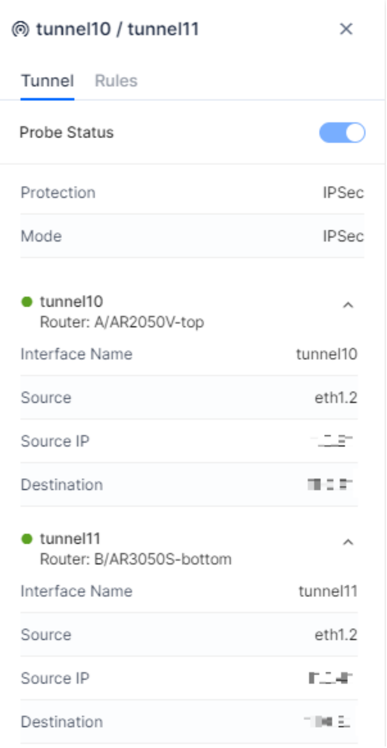
- ⬜ Tunnel disabled
- 🟦 Tunnel configured, Probe disabled
- 🟧 Tunnel configured, Probe in unknown state
- 🟥 Probe enabled, destination unreachable
- 🟩 Probe enabled, destination reachable
- 🟥 Failed to meet all rule criteria
- 🟧 Failed to meet one or more rule criteria
- 🟩 Meets all rule criteria

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:



tunnel10 / tunnel11 ✕

Tunnel Rules

Probe Status	●
Protection	IPSec
Mode	IPSec

● tunnel10
Router: A/AR2050V-top

Interface Name	tunnel10
Source	eth1.2
Source IP	[redacted]
Destination	[redacted]

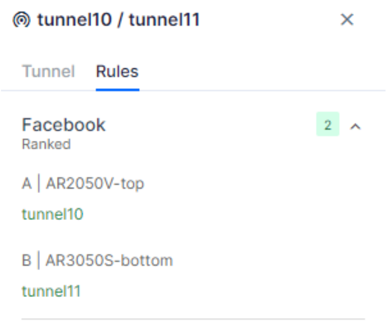
● tunnel11
Router: B/AR3050S-bottom

Interface Name	tunnel11
Source	eth1.2
Source IP	[redacted]
Destination	[redacted]

- 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:



tunnel10 / tunnel11 ×

Tunnel Rules

Facebook 2
Ranked

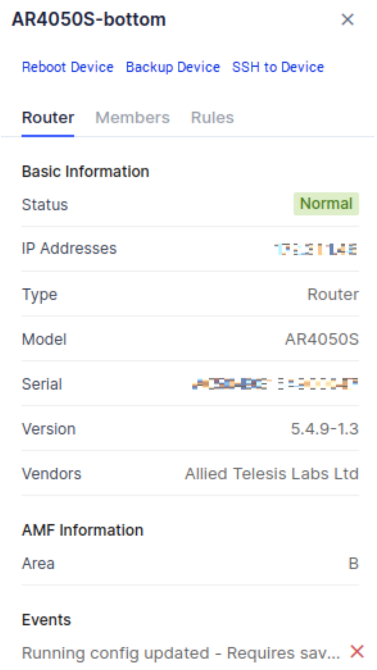
A | AR2050V-top
tunnel10

B | AR3050S-bottom
tunnel11

- 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:



AR4050S-bottom ×

Reboot Device Backup Device SSH to Device

Router Members Rules

Basic Information

Status	Normal
IP Addresses	[redacted]
Type	Router
Model	AR4050S
Serial	[redacted]
Version	5.4.9-1.3
Vendors	Allied Telesis Labs Ltd

AMF Information

Area	B

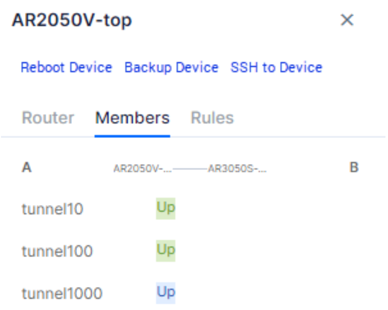
Events

Running config updated - Requires sav... ×

- Status
- IP Address
- Type
- Model

- Serial
- Version
- Vendors
- AMF Information

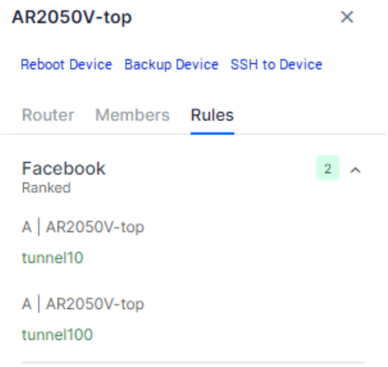
VPN members:



A	AR2050V-... —— AR3050S-...	B
tunnel10	Up	
tunnel100	Up	
tunnel1000	Up	

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

Rules:



Facebook 2
Ranked

A | AR2050V-top
tunnel10

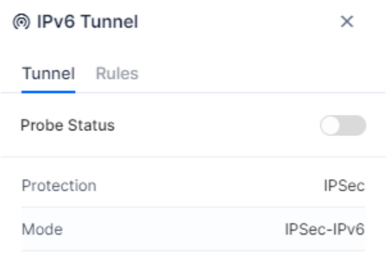
A | AR2050V-top
tunnel100

- Rule Name
- Rule Details

Linkmon probes

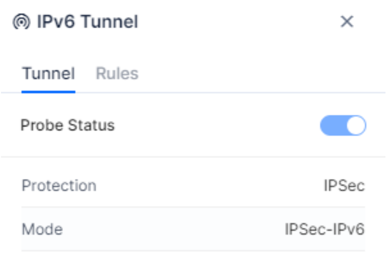
When a rule is created, any required probes will also be created and enabled. However, you can also create, enable, and disable probes from the SD-WAN map screen.

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.



Probe Status	
Protection	IPSec
Mode	IPSec-IPv6

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



Probe Status	
Protection	IPSec
Mode	IPSec-IPv6

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.

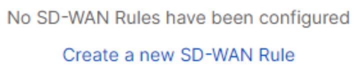
On the VPN-Members health screen, you can see a table of all VPN members in the network. You can also see which VPN Members have a probe enabled or disabled.

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:

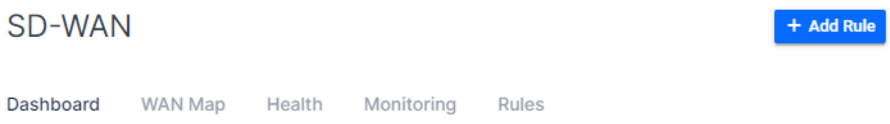


No SD-WAN Rules have been configured

Create a new SD-WAN Rule

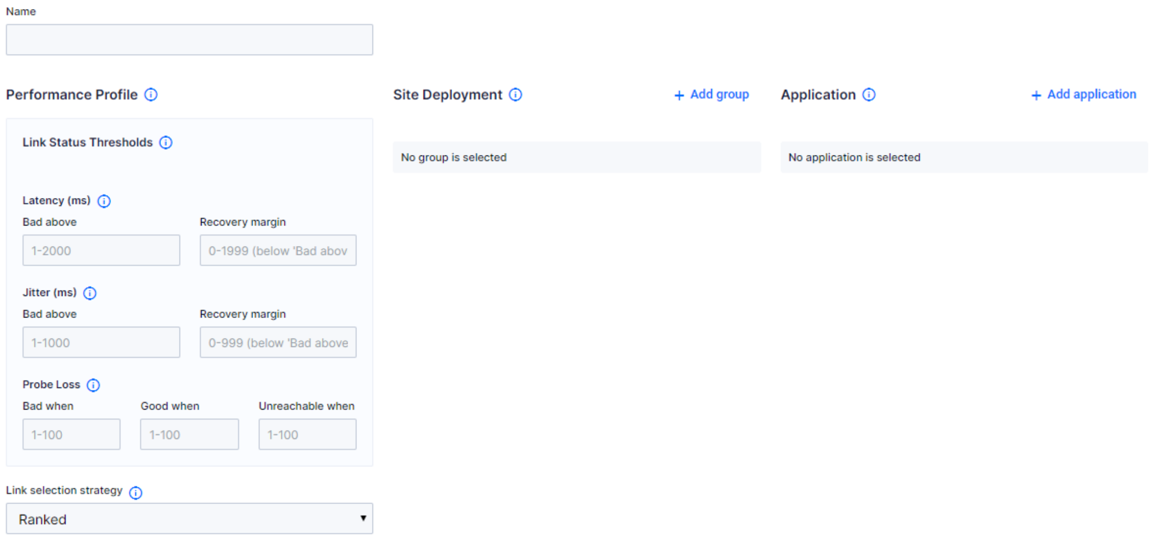
Click on the **Create a new SD-WAN Rule** link to create your first rule.

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



SD-WAN

You will then see the Application Rule screen.



Name

Performance Profile ⓘ

Link Status Thresholds ⓘ

Latency (ms) ⓘ

Bad above: 1-2000 | Recovery margin: 0-1999 (below 'Bad abov

Jitter (ms) ⓘ

Bad above: 1-1000 | Recovery margin: 0-999 (below 'Bad above

Probe Loss ⓘ

Bad when: 1-100 | Good when: 1-100 | Unreachable when: 1-100

Link selection strategy ⓘ

Ranked ▾

Site Deployment ⓘ + Add group

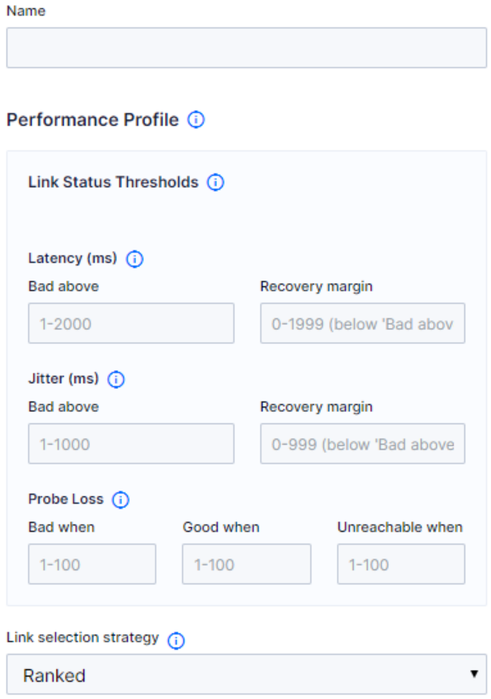
No group is selected

Application ⓘ + Add application

No application is selected

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.



Name

Performance Profile ⓘ

Link Status Thresholds ⓘ

Latency (ms) ⓘ

Bad above: 1-2000

Recovery margin: 0-1999 (below 'Bad abov

Jitter (ms) ⓘ

Bad above: 1-1000

Recovery margin: 0-999 (below 'Bad above

Probe Loss ⓘ

Bad when: 1-100

Good when: 1-100

Unreachable when: 1-100

Link selection strategy ⓘ

Ranked ▾

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

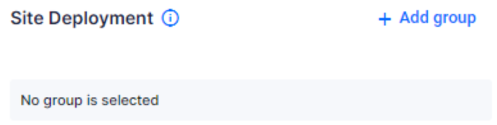
For each group of links, a rule is applied so there will always be a selected link (when not load-balanced). This selected link is the link that all traffic for that rule is directed through. If that selected link's metrics breaks one or more thresholds (configured by link status thresholds), then the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


Site Deployment ⓘ

+ Add group

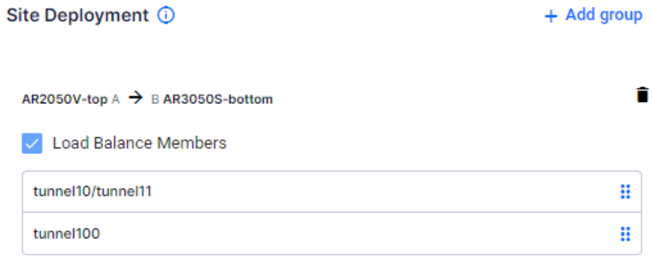
No group is selected

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'.



Site Deployment ⓘ

+ Add group

AR2050V-top A → B AR3050S-bottom

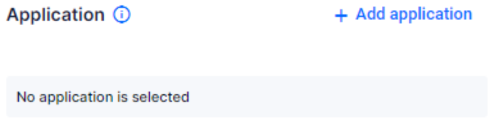
☑ Load Balance Members

tunnel10/tunnel11
tunnel100

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 device 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

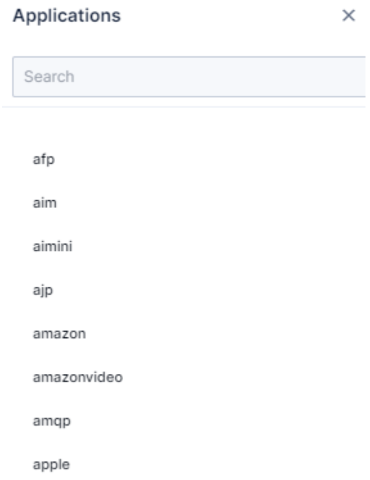


Application ⓘ

+ Add application

No application is selected

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.



Applications ×

Search

afp

aim

aimini

ajp

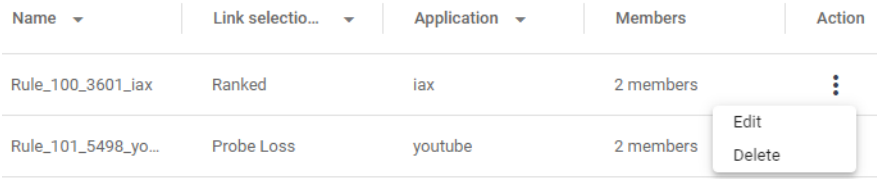
amazon

amazonvideo

amqp

apple

Editing and deleting an SD-WAN rule

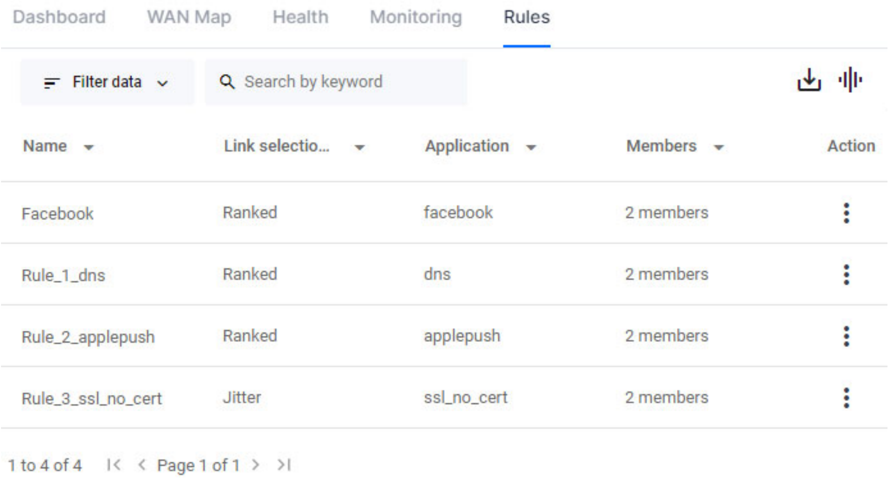


Name	Link selectio...	Application	Members	Action
Rule_100_3601_iax	Ranked	iax	2 members	⋮
Rule_101_5498_yo...	Probe Loss	youtube	2 members	

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



Name	Link selectio...	Application	Members	Action
Facebook	Ranked	facebook	2 members	⋮
Rule_1_dns	Ranked	dns	2 members	⋮
Rule_2_applepush	Ranked	applepush	2 members	⋮
Rule_3_ssl_no_cert	Jitter	ssl_no_cert	2 members	⋮

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

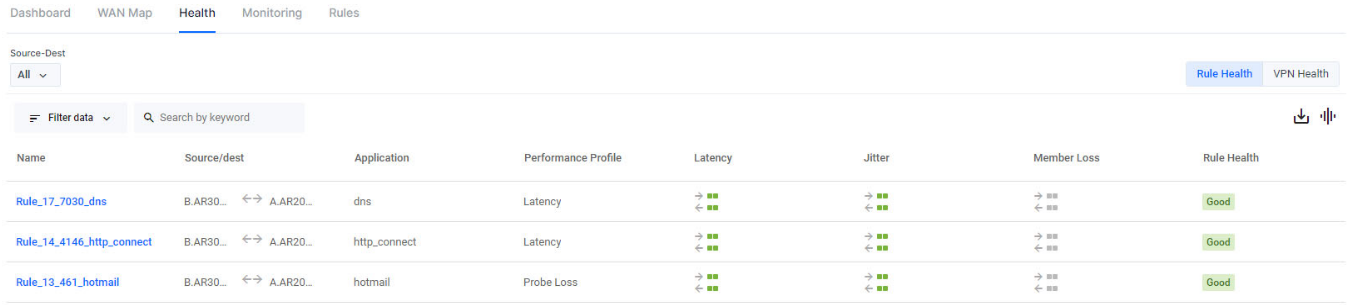
The health tab gives you an overview of the current health of your network in a single location.

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

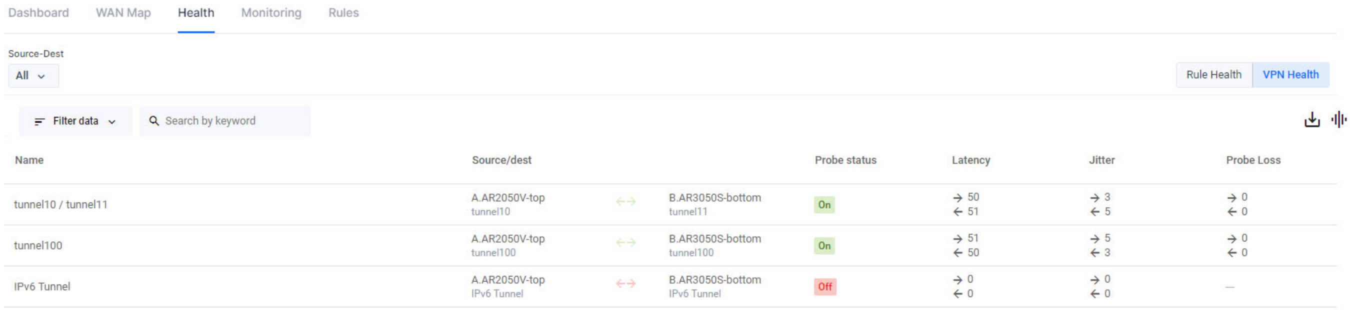


Name	Source/dest	Application	Performance Profile	Latency	Jitter	Member Loss	Rule Health
Rule_17_7030_dns	B.AR30... ↔ A.AR20...	dns	Latency	→ ■■ ← ■■	→ ■■ ← ■■	→ ■■ ← ■■	Good
Rule_14_4146_http_connect	B.AR30... ↔ A.AR20...	http_connect	Latency	→ ■■ ← ■■	→ ■■ ← ■■	→ ■■ ← ■■	Good
Rule_13_461_hotmail	B.AR30... ↔ A.AR20...	hotmail	Probe Loss	→ ■■ ← ■■	→ ■■ ← ■■	→ ■■ ← ■■	Good

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

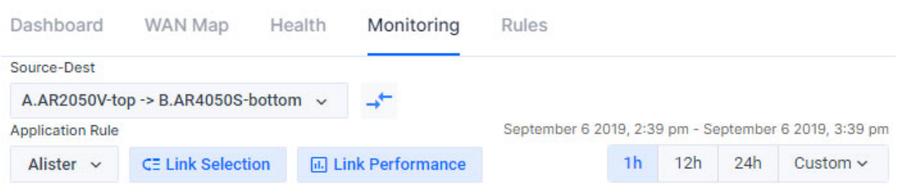
VPN health



Name	Source/dest			Probe status	Latency	Jitter	Probe Loss
tunnel10 / tunnel11	A.AR2050V-top tunnel10	↔	B.AR3050S-bottom tunnel11	On	→ 50 ← 51	→ 3 ← 5	→ 0 ← 0
tunnel100	A.AR2050V-top tunnel100	↔	B.AR3050S-bottom tunnel100	On	→ 51 ← 50	→ 5 ← 3	→ 0 ← 0
IPv6 Tunnel	A.AR2050V-top IPv6 Tunnel	↔	B.AR3050S-bottom IPv6 Tunnel	Off	→ 0 ← 0	→ 0 ← 0	—

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

Monitoring



Source-Dest: A.AR2050V-top -> B.AR4050S-bottom

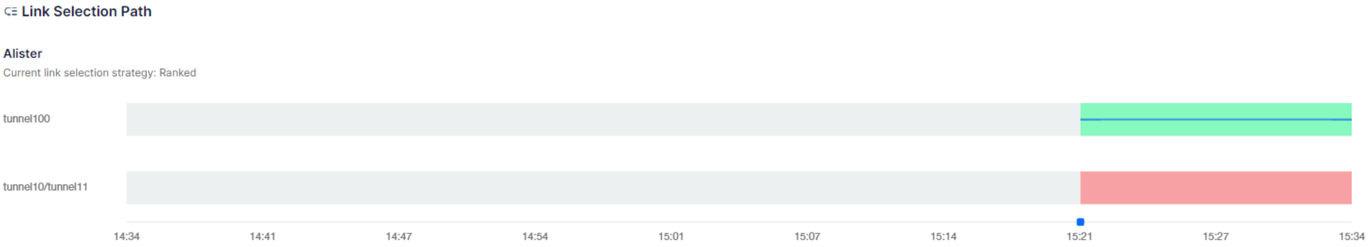
Application Rule: Alister

September 6 2019, 2:39 pm - September 6 2019, 3:39 pm

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.

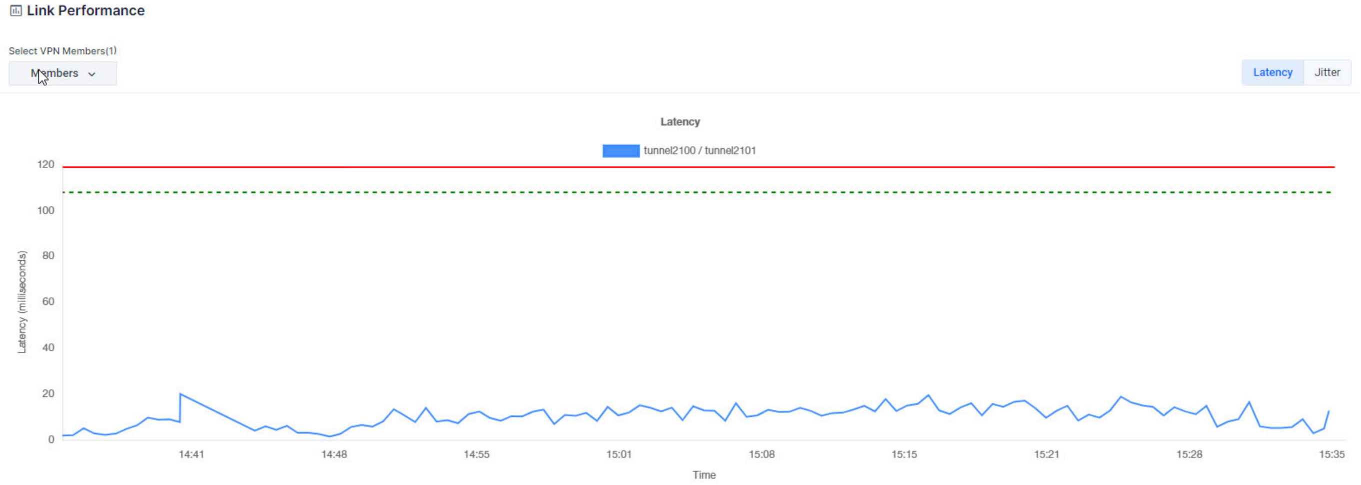


Alister

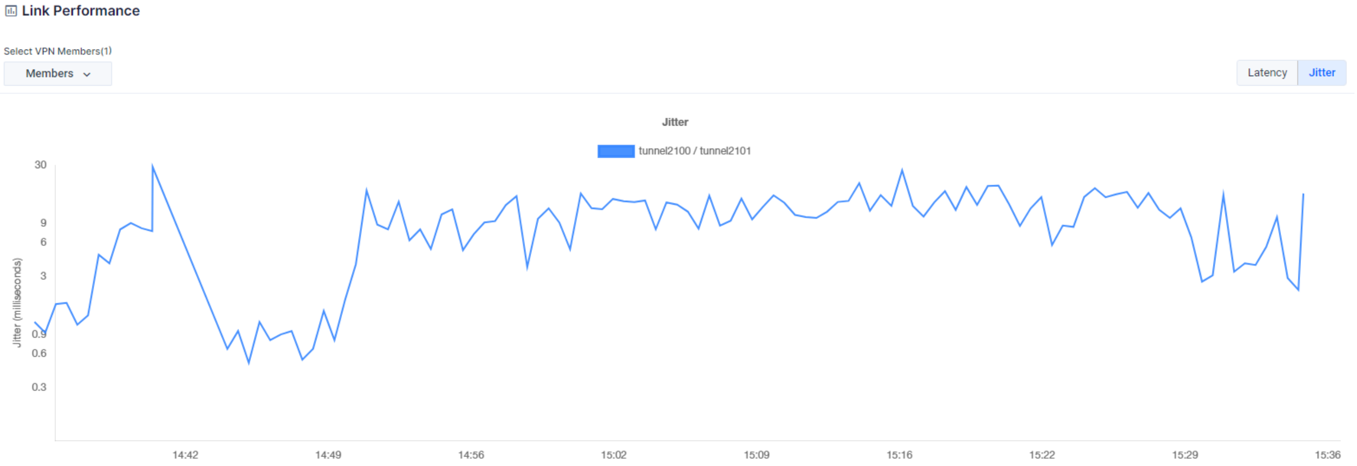
Current link selection strategy: Ranked

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.

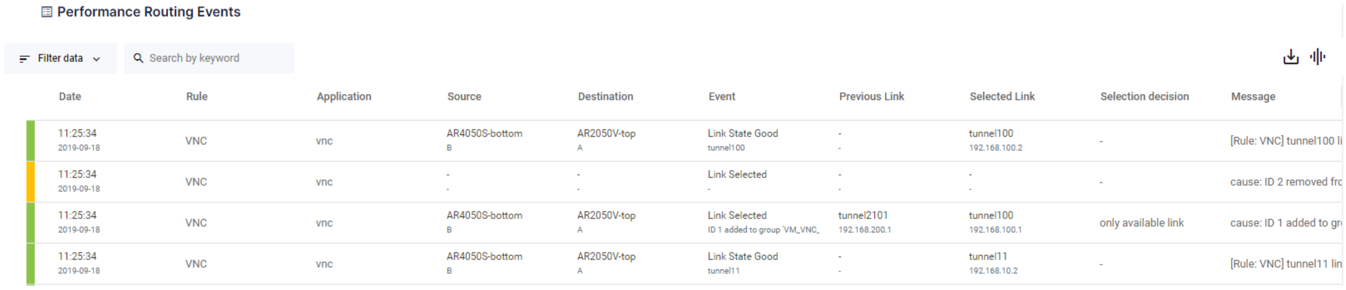
The Link Performance charts show the performance history of a link for either latency or jitter. You can select which member you would like to see from the Members drop-down, or select multiple members to compare them.



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.



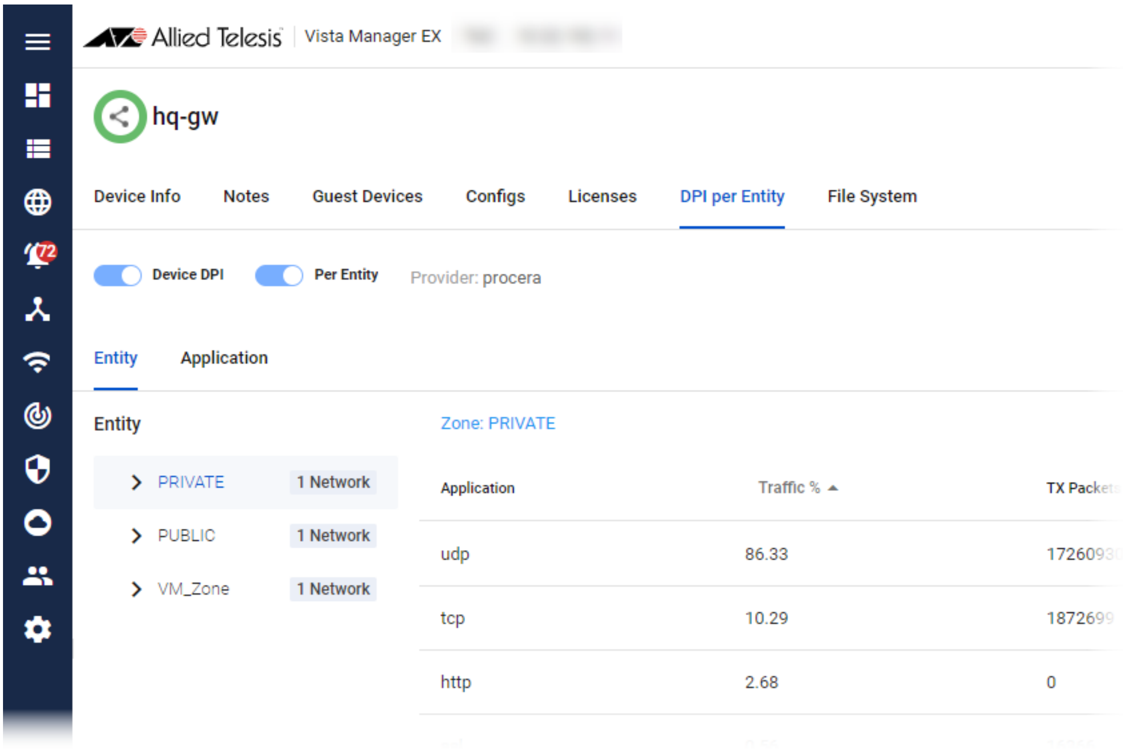
	Date	Rule	Application	Source	Destination	Event	Previous Link	Selected Link	Selection decision	Message
🟩	11:25:34 2019-09-18	VNC	vnc	AR4050S-bottom B	AR2050V-top A	Link State Good tunnel100	- -	tunnel100 192.168.100.2	-	[Rule: VNC] tunnel100 li
🟨	11:25:34 2019-09-18	VNC	vnc	- -	- -	Link Selected -	- -	- -	-	cause: ID 2 removed frc
🟩	11:25:34 2019-09-18	VNC	vnc	AR4050S-bottom B	AR2050V-top A	Link Selected ID 1 added to group 'VM_VNC_	tunnel2101 192.168.200.1	tunnel100 192.168.100.1	only available link	cause: ID 1 added to gr
🟩	11:25:34 2019-09-18	VNC	vnc	AR4050S-bottom B	AR2050V-top A	Link State Good tunnel11	- -	tunnel11 192.168.10.2	-	[Rule: VNC] tunnel11 lin

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



Device DPI ● Per Entity ● Provider: procera

Entity

> PRIVATE	1 Network
> PUBLIC	1 Network
> VM_Zone	1 Network

Zone: PRIVATE

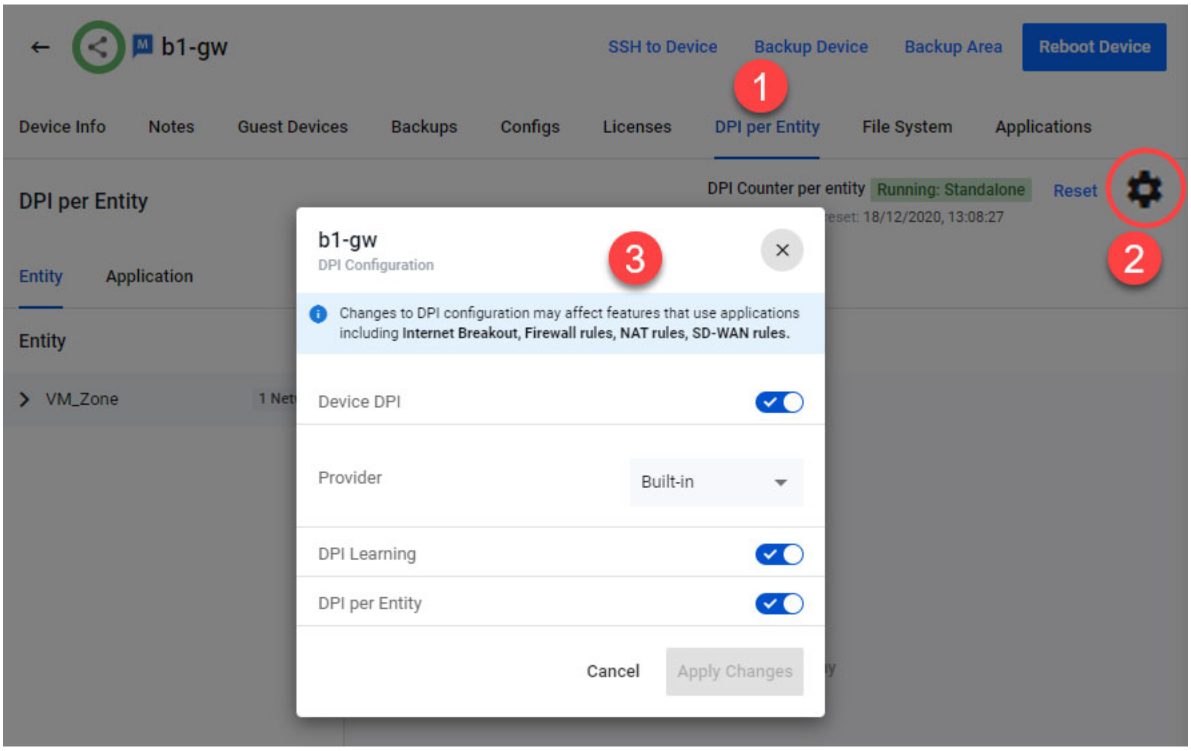
Application	Traffic % ▲	TX Packe
udp	86.33	1726093
tcp	10.29	1872699
http	2.68	0

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.

Application reconfiguration support

Because enabling DPI may affect existing firewall/NAT/PBR rules, Vista Manager EX automatically redirects you to the **Applications** tab for a detailed reconfiguration of applications if required. Alternatively, you can navigate directly to this page to adjust the list of applications before enabling DPI, to ensure the router functions normally.



b1-gw
DPI Configuration

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.**

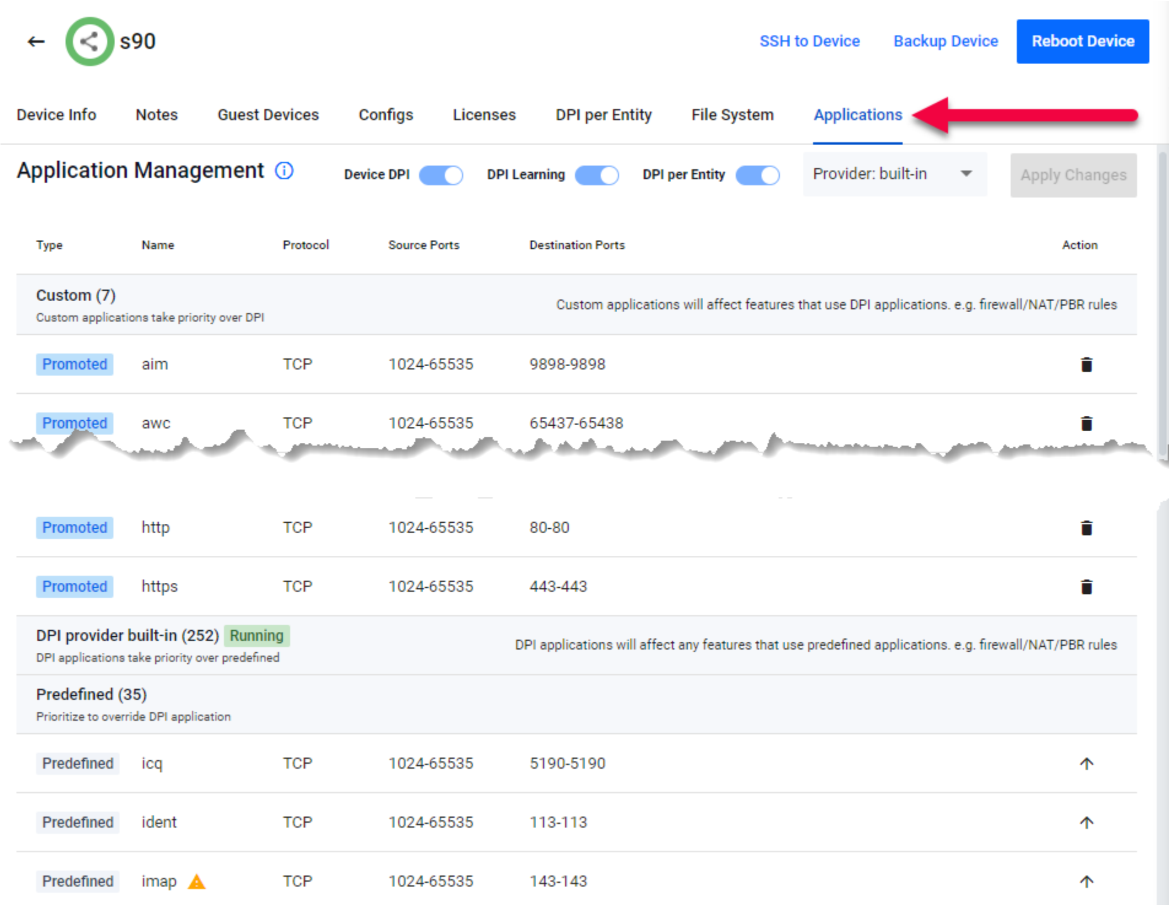
Device DPI ✓

Provider: Built-in

DPI Learning ✓

DPI per Entity ✓

Cancel | Apply Changes



Application Management

Device DPI ✓ | DPI Learning ✓ | DPI per Entity ✓ | Provider: built-in | Apply Changes

Type	Name	Protocol	Source Ports	Destination Ports	Action
Custom (7) Custom applications take priority over DPI				Custom applications will affect features that use DPI applications. e.g. firewall/NAT/PBR rules	
Promoted	aim	TCP	1024-65535	9898-9898	🗑
Promoted	awc	TCP	1024-65535	65437-65438	🗑
Promoted	http	TCP	1024-65535	80-80	🗑
Promoted	https	TCP	1024-65535	443-443	🗑
DPI provider built-in (252) Running DPI applications take priority over predefined				DPI applications will affect any features that use predefined applications. e.g. firewall/NAT/PBR rules	
Predefined (35) Prioritize to override DPI application					
Predefined	icq	TCP	1024-65535	5190-5190	↑
Predefined	ident	TCP	1024-65535	113-113	↑
Predefined	imap ⚠	TCP	1024-65535	143-143	↑

Here, you will see custom applications and predefined applications of your selected device. If DPI is enabled, you will also see the DPI running status, providers and the number of DPI applications on the device.

Custom applications and predefined applications will appear in two groups, separated by the DPI group, which indicates priority:

1. Custom
2. DPI
3. Predefined

When DPI is enabled, a warning icon will appear beside the predefined applications. This indicates that:

- they may not work due to their lower priority, prompting you to promote them to custom
- if they overlap with DPI applications, they should be considered for promotion if any rules are using them

As a user with write permission, you will be able to:

- enable/disable various DPI settings
- change the DPI provider
- promote predefined applications to the custom category
- remove promoted applications from the custom category

DPI learning and application sharing

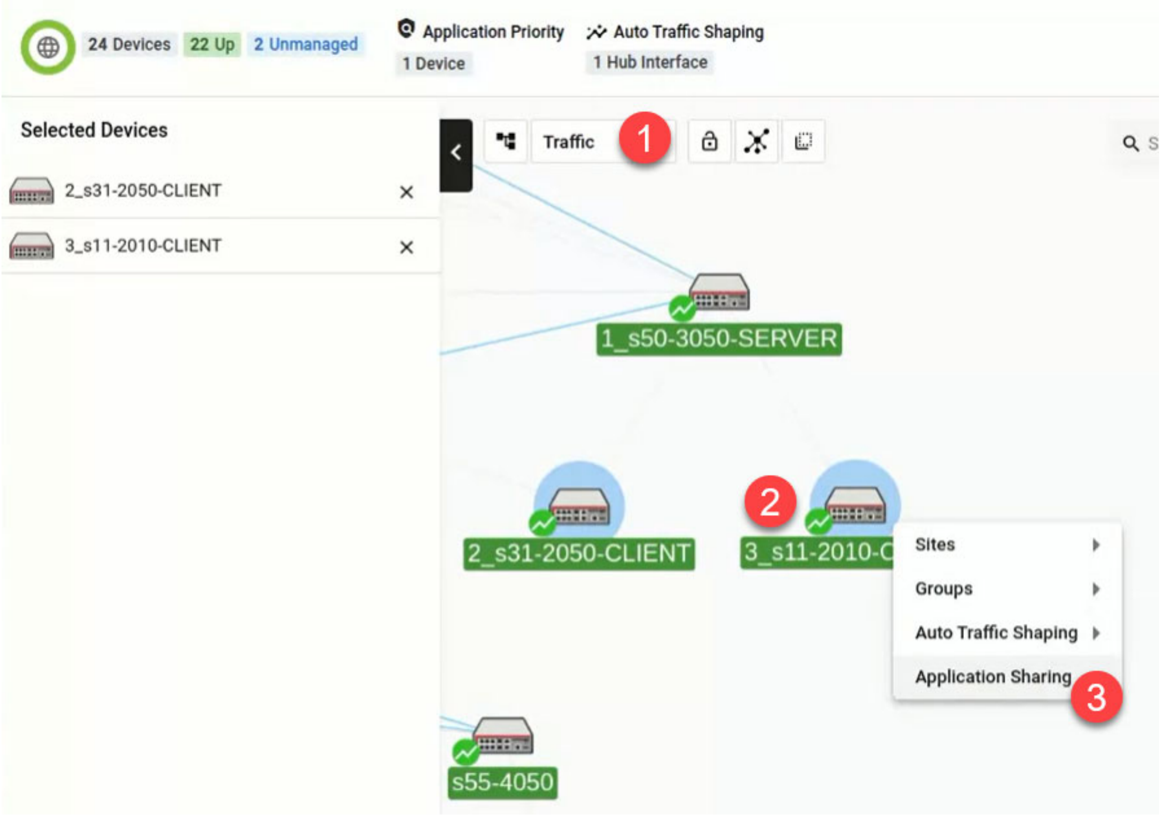
Branch office routers (clients) can gain access to applications on a head office router (server) by using this functionality. Applications learned on the servers can be distributed to the clients, thus allowing features like Internet Breakout to be enabled on a client.

- **AR3050S** and **AR4050S** can be used as server devices that have advanced DPI engines available. This means that they can share their applications with other devices.
- **AR2010V** and **AR2050V** can be client devices. They will use a server device to send them the application data.
- This functionality requires AR-series devices to run AlliedWare Plus 5.5.1-1 or later.

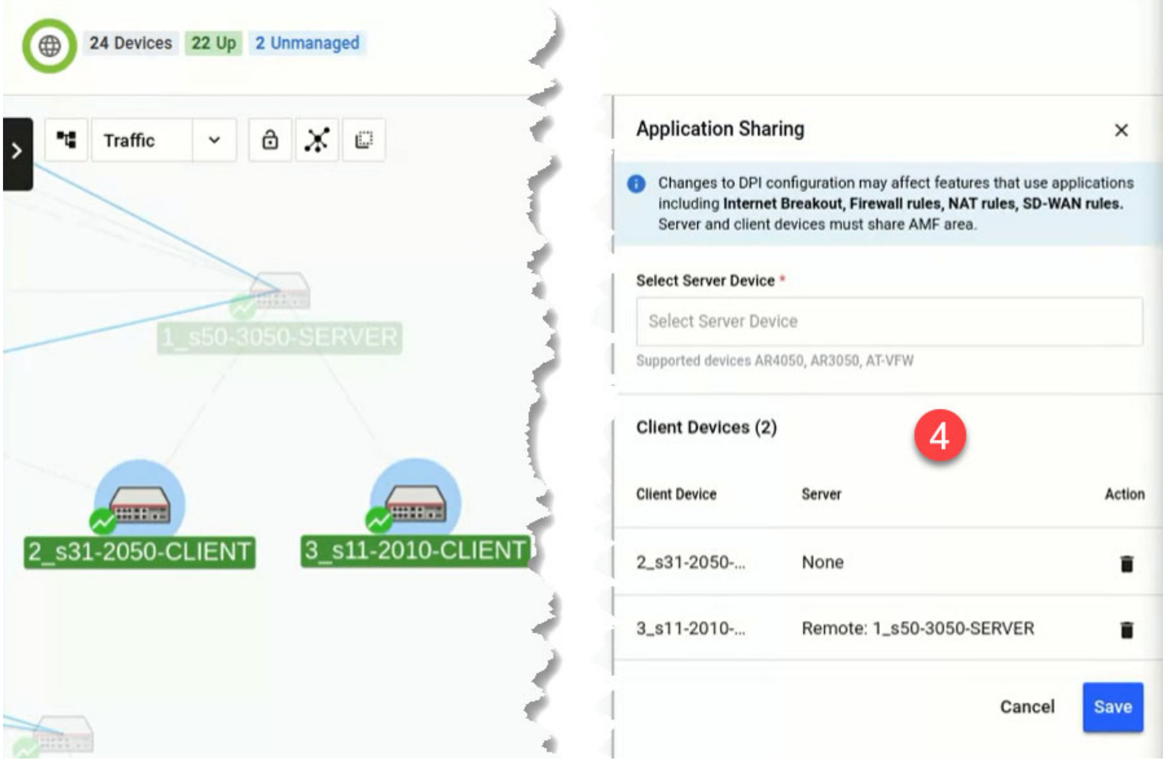
Configure application sharing via 3 options:

- "Option 1: via Traffic map context menu" on page 210
- "Option 2: via Traffic side panel" on page 212
- "Option 3: via Asset Management > Applications tab" on page 213

Option 1: via Traffic map context menu



1. Navigate to the traffic map.
2. Select at least one client router.
3. Right-click on the selected router(s) and select **Application Sharing** from the menu.



Application Sharing

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.** Server and client devices must share AMF area.

Select Server Device *

Select Server Device

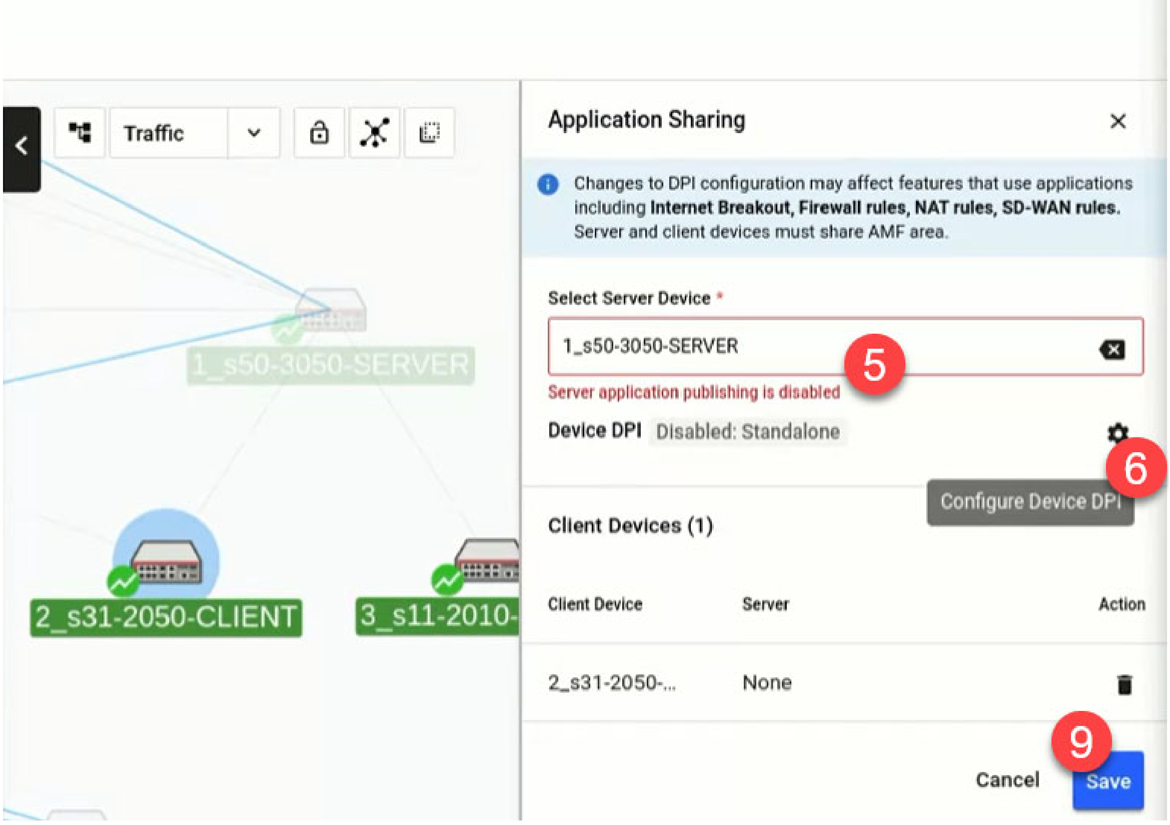
Supported devices AR4050, AR3050, AT-VFW

Client Devices (2)

Client Device	Server	Action
2_s31-2050-...	None	🗑
3_s11-2010-...	Remote: 1_s50-3050-SERVER	🗑

4. This opens up the Application Sharing side panel. You may remove or add more client devices here.

5. Next, select a server device from the drop-down list. Take note of the current DPI state of the server.



Application Sharing

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.** Server and client devices must share AMF area.

Select Server Device *

1_s50-3050-SERVER

Server application publishing is disabled

Device DPI Disabled: Standalone

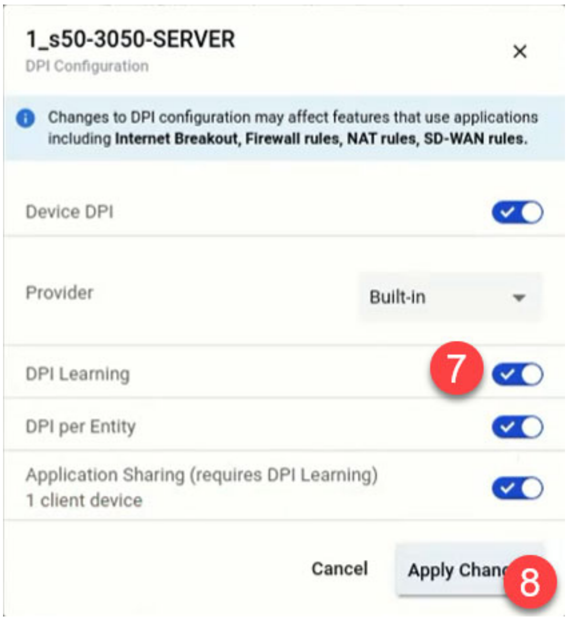
Configure Device DPI

Client Devices (1)

Client Device	Server	Action
2_s31-2050-...	None	

Cancel Save

6. Click on the **Configure Device DPI** gear icon button if device DPI is disabled or to configure its settings.



1_s50-3050-SERVER
DPI Configuration

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.**

Device DPI ✓

Provider Built-in

DPI Learning ✓

DPI per Entity ✓

Application Sharing (requires DPI Learning) ✓
1 client device

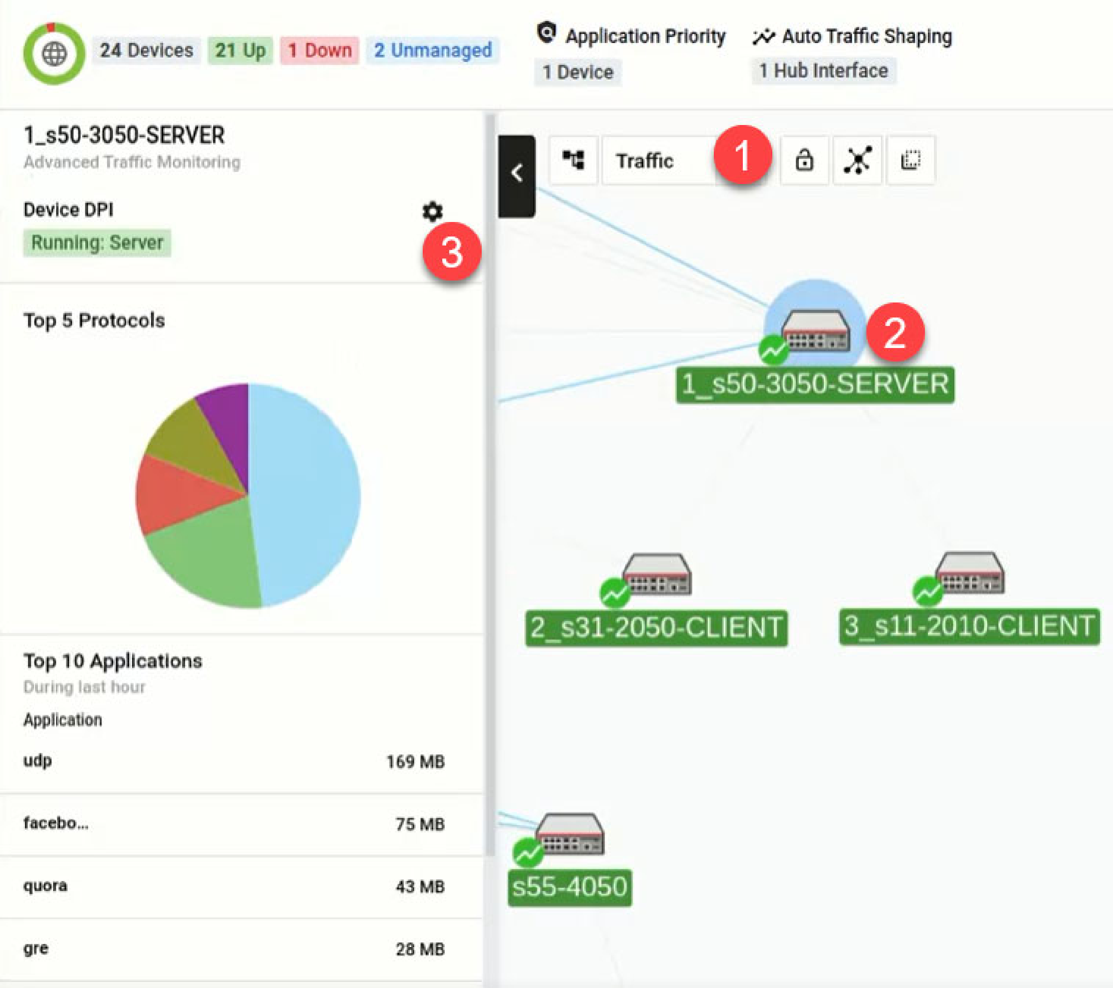
Cancel Apply Chang

7. Turn on all settings to ensure a successful application sharing setup.

8. Click **Apply Changes**.

9. Finally, click **Save** on the side panel.

Option 2: via Traffic side panel



24 Devices 21 Up 1 Down 2 Unmanaged

Application Priority: 1 Device

Auto Traffic Shaping: 1 Hub Interface

1_s50-3050-SERVER

Advanced Traffic Monitoring

Device DPI

Running: Server

Top 5 Protocols

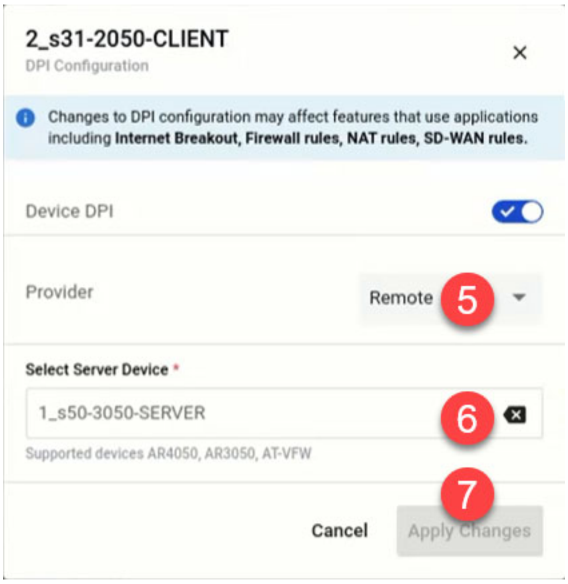
Top 10 Applications

During last hour

Application	
udp	169 MB
facebo...	75 MB
quora	43 MB
gre	28 MB

1. Navigate to the traffic map.
2. Select a supported server/client device. This opens up the Traffic side panel.
3. Click on the **Device DPI** gear icon button if device DPI is disabled or to configure its settings.
4. If a server device was selected, carry out **Steps 7-8 in Option 1**.

5. If a client device was selected, fewer DPI settings will be displayed. Select a **Remote** provider to choose a server next.



2_s31-2050-CLIENT

DPI Configuration

Changes to DPI configuration may affect features that use applications including **Internet Breakout, Firewall rules, NAT rules, SD-WAN rules.**

Device DPI: ✓

Provider: Remote

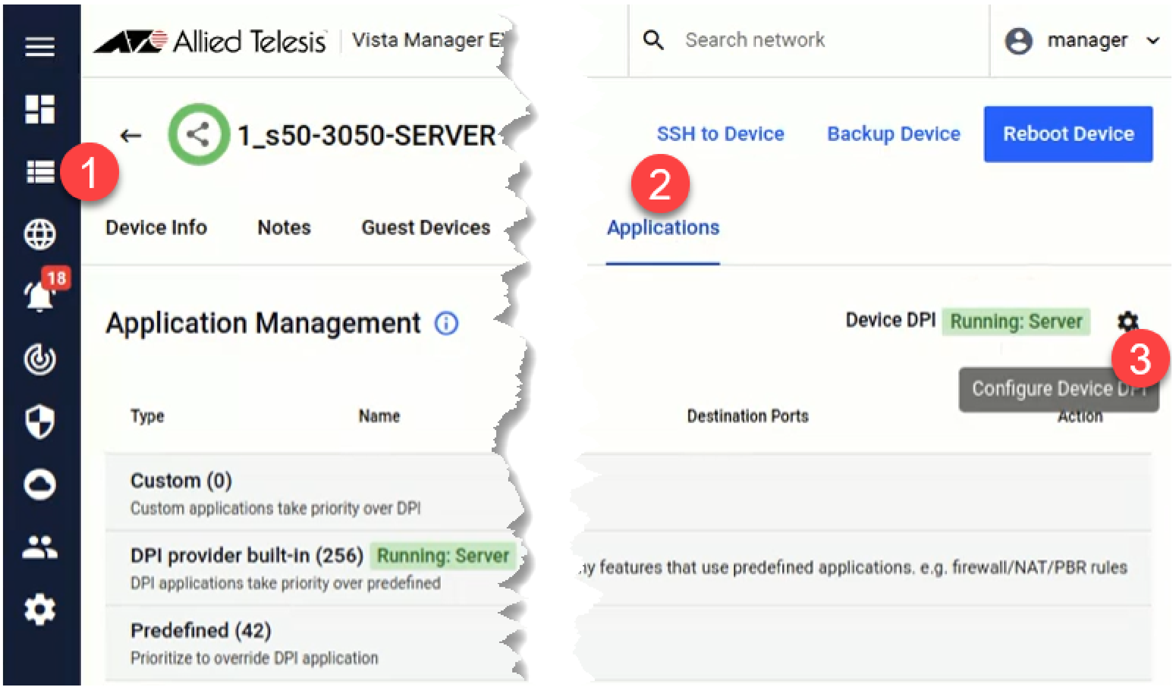
Select Server Device *: 1_s50-3050-SERVER

Supported devices AR4050, AR3050, AT-VFW

6. Select a server from the drop-down list.

7. Click **Apply Changes**.

Option 3: via Asset Management > Applications tab



Custom (0)
Custom applications take priority over DPI

DPI provider built-in (256) Running: Server
DPI applications take priority over predefined

Predefined (42)
Prioritize to override DPI application

...y features that use predefined applications. e.g. firewall/NAT/PBR rules

1. Navigate to **Asset Management**. Select a supported device from the list.

2. Next, go to the **Applications** tab of that device.

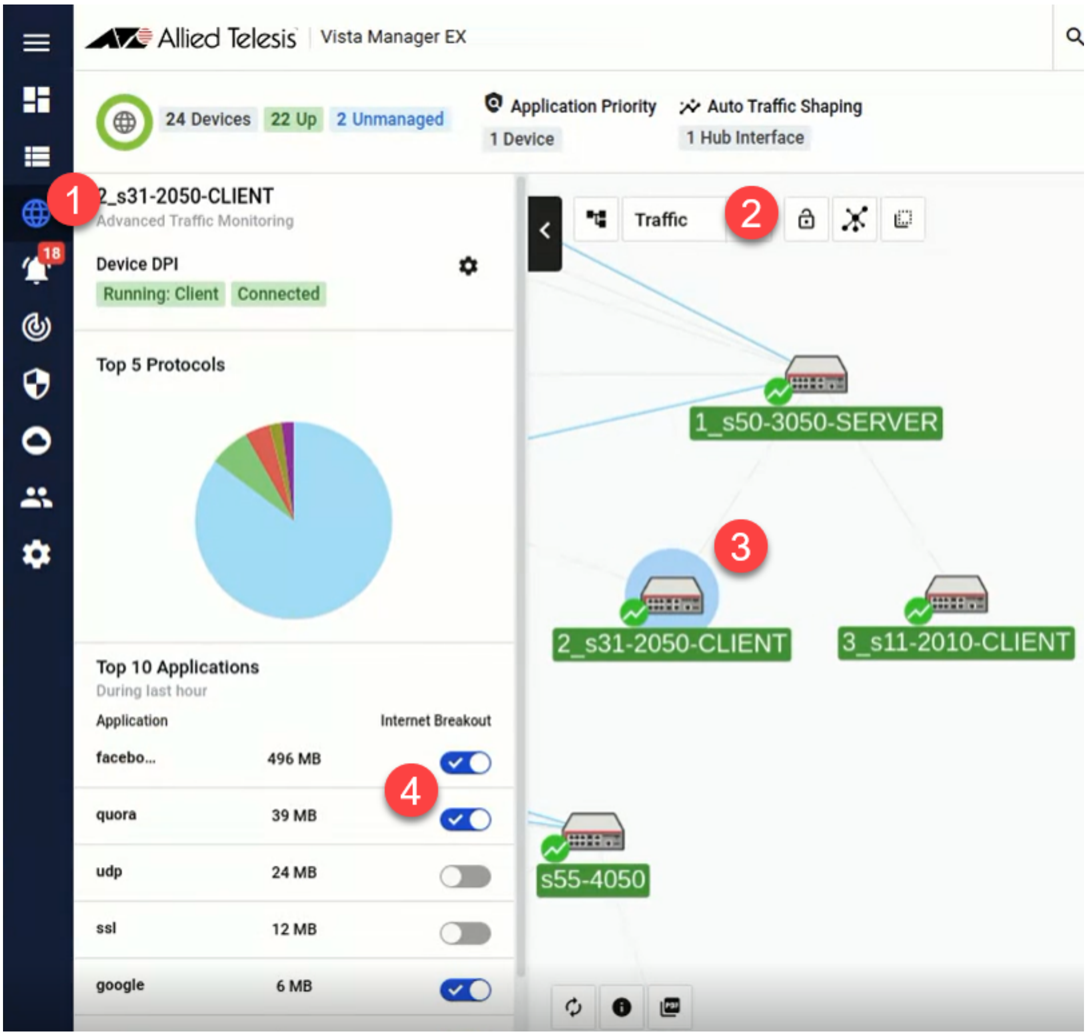
3. Click on the **Configure Device DPI** gear icon button if device DPI is disabled or to configure its settings.

4. If a server device was selected, carry out **Steps 7-8 in Option 1**.

5. If a client device was selected, fewer DPI settings will be displayed. Carry out **Steps 5-7 in Option 2**.

With DPI learning and application sharing configured and running successfully, you can then enable Internet Breakout for specific applications on clients from the Traffic side panel. Here, you can also see what applications have been learned from the server.

1. Navigate to the network map.
2. Select Traffic map mode.
3. Select a client device that you wish to enable Internet Breakout for.
4. On the Traffic side panel that launches, enable Internet Breakout accordingly.



2_s31-2050-CLIENT
Advanced Traffic Monitoring

Device DPI
Running: Client · Connected

Top 10 Applications
During last hour

Application		Internet Breakout
facebo...	496 MB	✓
quora	39 MB	✓
udp	24 MB	
ssl	12 MB	
google	6 MB	✓

Note: Application sharing (between a server and clients) will only be functional within an AMF area. It is possible to have multiple servers in different areas, but the clients of each server must be located in the same area as the server.

Troubleshooting

Ports used by Vista

Vista Manager EX makes use of the following ports. These ports may need to be configured on your firewall:

VRT APL WIN VA

Ports for all deployments of Vista Manager EX:

- UDP port 514 (syslog), used by the AMF master/controller to send logs to Vista Manager EX.
- TCP port 443 (HTTPS), used if the HTTPS mode of Vista Manager EX is enabled.
- TCP ports 443 and 12943, used if you are not using certificates for device authentication.
- TCP ports 12945 and 12946, used if you are using certificates for device authentication (recommended).

WIN

Further ports:

- TCP port 5000, which gives access to the Vista Manager web interface.

VRT APL WIN

Further ports:

- TCP port 5443, which gives access to the AWC plug-in web interface. (This depends on which port you configured the AWC plug-in to run on during installation.)
- TCP port 65437-65439, which the wireless APs use to communicate with the AWC plug-in.
- TCP port 6443, which gives access to the SNMP plug-in web interface.
- UDP port 162 (SNMP trap), used by SNMP devices to send traps to the SNMP plug-in.

VA WIN

You may need to create Windows inbound firewall rules and Virus scanning exclusions.

Clear browser cache

Clear your browser's cache after upgrading your Vista Manager EX installation. Incomplete dialog boxes, incorrectly populated drop-down lists, and truncated forms are all symptoms of a caching problem.

Allow Vista Manager EX to discover the AMF network

If, after installation, there are no devices on the AMF network/area map check that the following command has been run on your AMF controller (if present) and all AMF masters.

```
awplus# configure terminal
awplus(config)# atmf topology-gui enable
```

x930 Expansion Module

Caution: The x930 expansion module is not recognized by Vista Manager. This means that it cannot configure VLANs on those ports.

Vista Manager and RMON

When Vista Manager connects to an AlliedWare Plus network, it automatically enables the RMON (Remote Network Monitoring) commands on each AMF interface port that it finds. This is done for the purpose of collecting traffic statistics.

It does this by modifying the running config on all switchports that interconnect AMF devices (including LAGs). No notification is shown that these changes are being made.

Caution: If the **copy run start** or **wr** commands are run on one of these devices, these config changes will be made permanent.

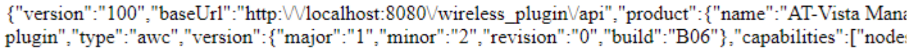
WIN Testing Windows server

If you cannot connect remotely on Windows, try connecting locally on the Windows server by using localhost:

```
http://localhost:5000
```

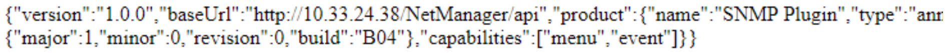
You can test whether the plug-in APIs are active using the following URLs:

- 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":"anr
{"major":1,"minor":0,"revision":0,"build":"B04"},"capabilities":["menu","event"]}}

Note that these URLs can only be used locally on the Vista Manager server using "localhost".

Reboot AMF master/controller after configuring certificates

If you receive the following error message:

```
Error during polling - Error: Device did not accept a certificate request
and basic auth fallback is disabled. Details: Error: connect ECONNREFUSED
xxx.xxx.xxx.xxx:12946
```

Check that you have correctly configured your AMF master/controller for certificate authentication and that you saved your configuration and rebooted your master/controller after running the **atmf trustpoint** command (see "Configure certificate for device authentication" on page 10).

Problems adding plug-ins

If you are having difficulty adding the plug-ins in Vista Manager EX, make sure that you have done the following:

VRT APL WIN

- Check that you have the correct URL for each plug-in as described in "Registering the plug-ins" on page 16, and click on Verify Connection.

VRT APL

- Prior to Vista Manager 3.5.0, the Windows-based version of Vista Manager supported a lowercase URL for registering the SNMP plug-in. If you are upgrading from an earlier version, or porting to a different platform, you should re-register the SNMP plug-in using the mixed-case URL.

  ```
  Server URL: https://<ip-address>:6443/NetManager
  ```

  where <ip-address> is the IP address of the SNMP plug-in.

WIN

- Make sure that you have imported the plug-in server certificates as described in the “Initial Login” section in the Vista Manager EX™ Installation Guide.

WIN

- Add the Vista Manager EX server address to your trusted sites as described in the Vista Manager EX™ Installation Guide.

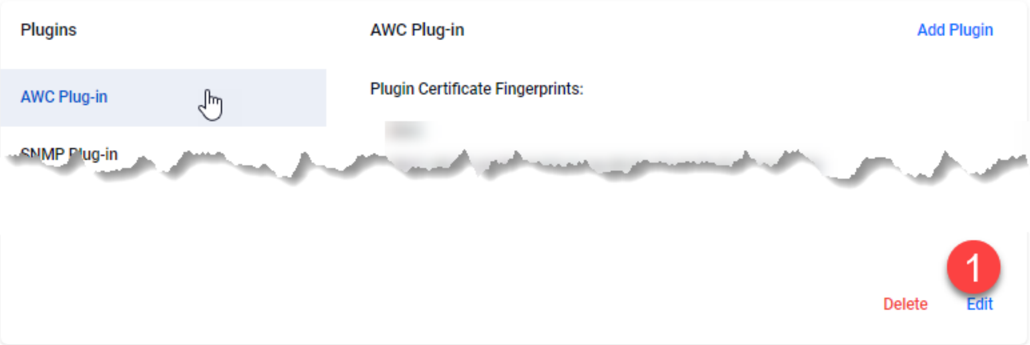
WIN

- Add an exception for the server to your web proxy as described in the Vista Manager EX™ Installation Guide.

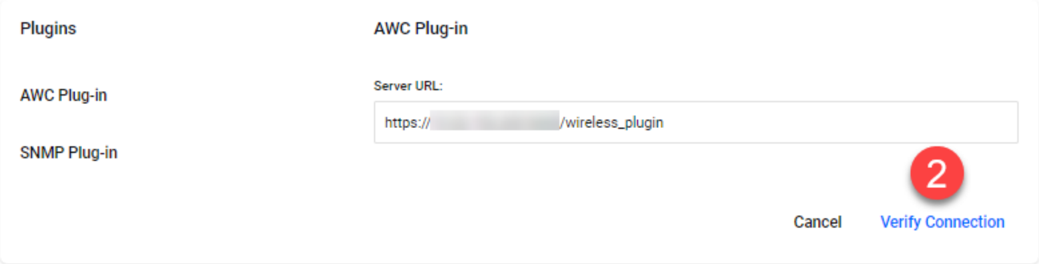
Updating plug-ins

If you are having issues with plug-ins, you can update a plug-in without deleting it.

1. From the System Management menu, go to the **Plugins** tab. Select the plug-in to update. Click **Edit**.

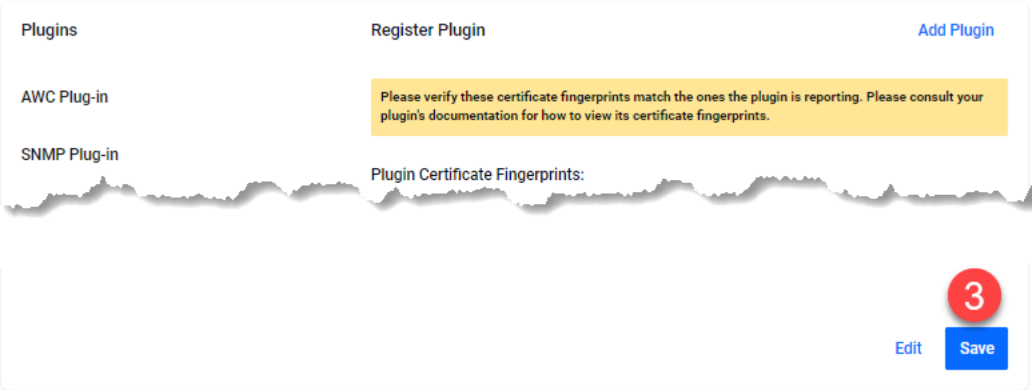


2. Click **Verify Connection**.



Server URL:
https://[redacted]/wireless_plugin

3. Click **Save**.



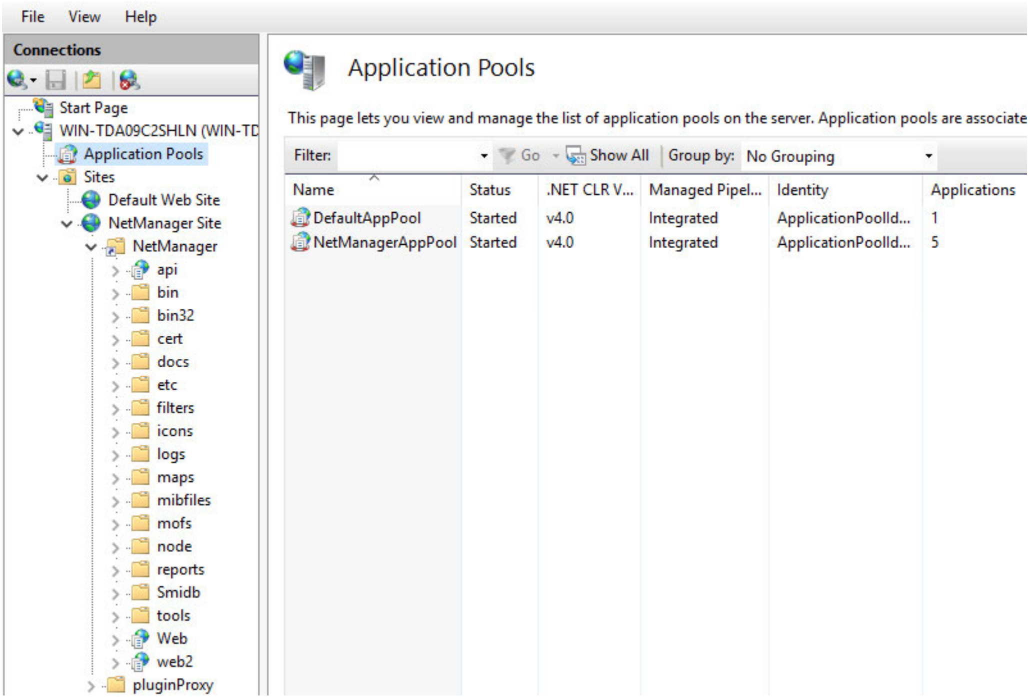
Please verify these certificate fingerprints match the ones the plugin is reporting. Please consult your plugin's documentation for how to view its certificate fingerprints.

WIN 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 in the following screenshots.

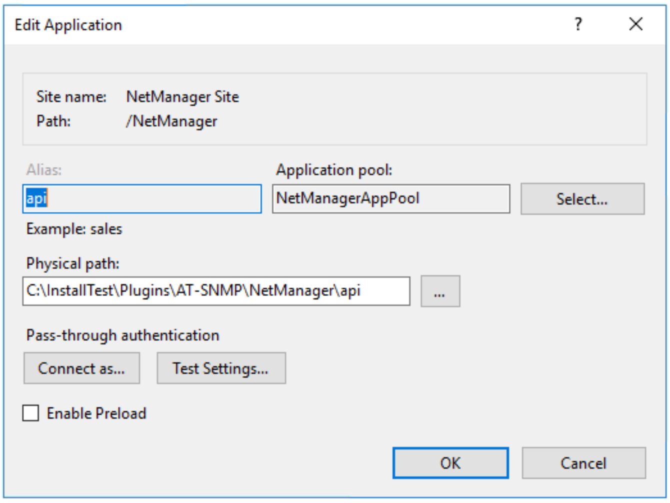


Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associate

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	1
NetManagerAppPool	Started	v4.0	Integrated	ApplicationPoolId...	5

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



Site name: NetManager Site

Path: /NetManager

Alias: api

Application pool: NetManagerAppPool

Example: sales

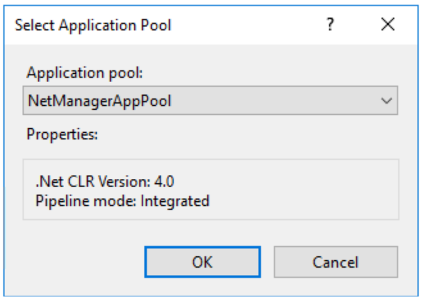
Physical path: C:\InstallTest\Plugins\AT-SNMP\NetManager\api

Pass-through authentication

□ Enable Preload

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

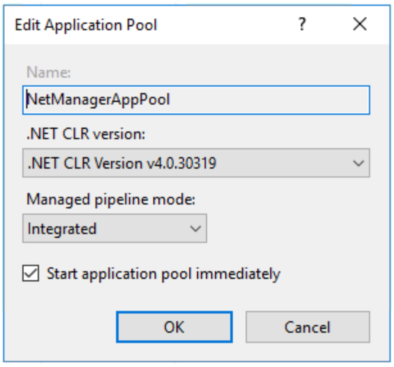


Application pool: NetManagerAppPool

Properties:

.Net CLR Version: 4.0
Pipeline mode: Integrated

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:



Name: NetManagerAppPool

.NET CLR version: .NET CLR Version v4.0.30319

Managed pipeline mode: Integrated

☑ Start application pool immediately

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

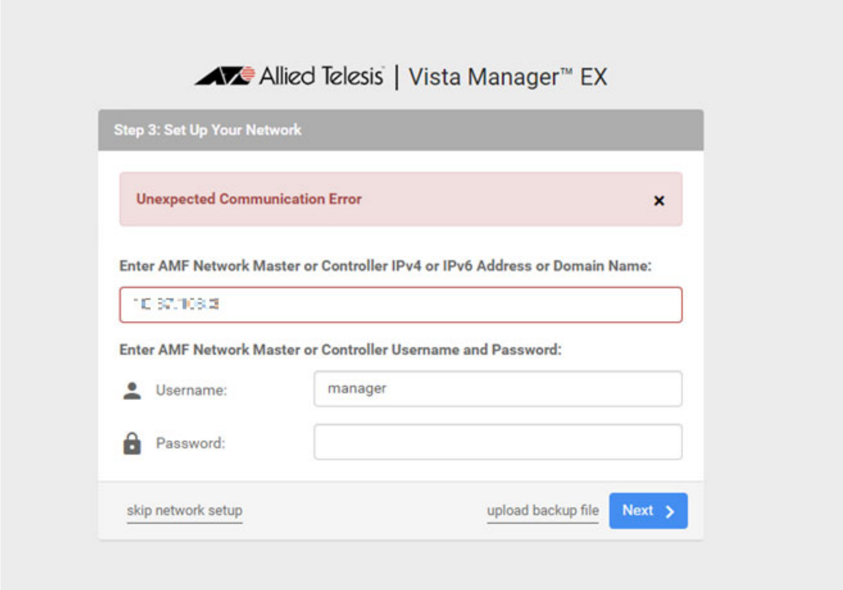
De-register the AWC plug-in on large wireless networks

WIN

Individual APs may disappear from the AWC plug-in if the plug-in is managing a large wireless network (approximately 600 APs or more). If this occurs, de-register the AWC plug-in from the Vista Manager’s **System Management -> Plug-in Management** page. Features such as licensing, auto-recovery, and importing an AP from a guest device will still work, even if the plug-in is not registered.

Unexpected Communication Error during installation

When setting up your connection (Step 3: Set Up Your Network), you may receive the following error:



Step 3: Set Up Your Network

Unexpected Communication Error ×

Enter AMF Network Master or Controller IPv4 or IPv6 Address or Domain Name: [illegible]

Enter AMF Network Master or Controller Username and Password:

Username: manager

Password:

This is due to the **atmf topology-gui enable** command not having been run on the master. You can resolve this by running the command on the master, then clicking the Next button.

For further information, refer to "Allow Vista Manager EX to discover the AMF network" on page 215.

Syslog generation for AMF guest devices

VA APL WIN

When a guest device joins or leaves an AMF network, syslog messages will be generated containing these fields:

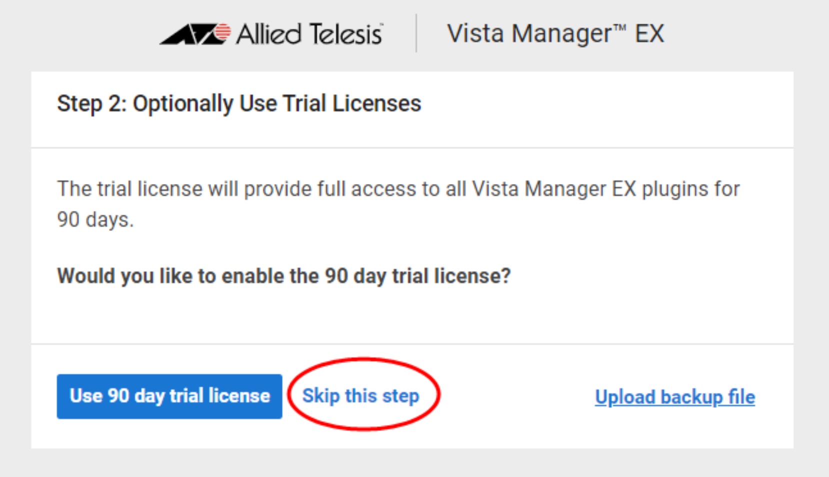
- Network name
- Area name
- Port number
- Model type
- MAC address
- IP address

Information from these log messages are intended to help facilitate easy deployment and replacement of APs.

APL

Unable to enter Master/Controller IP address after skipping license page

Vista Manager 3.7.0 does not require a license on the VST-APL. If you skip the license step when installing the Vista Manager application, then at **Step3: Set up Your Network**, you may not be able to enter your Master or Controller's IP address.



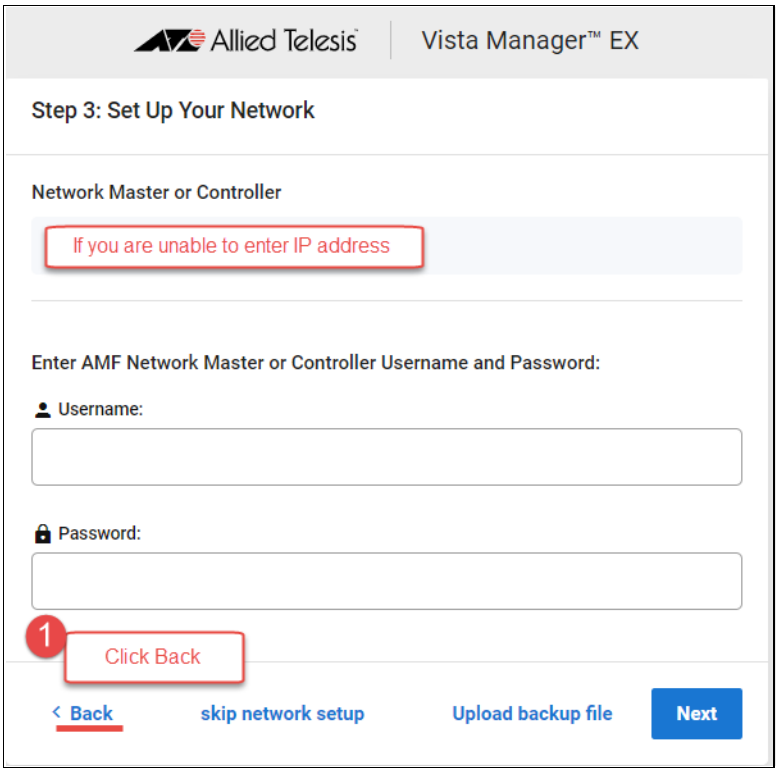
Step 2: Optionally Use Trial Licenses

The trial license will provide full access to all Vista Manager EX plugins for 90 days.

Would you like to enable the 90 day trial license?

To work-around this issue, perform the following steps:

1. Click **Back**:



Step 3: Set Up Your Network

Network Master or Controller

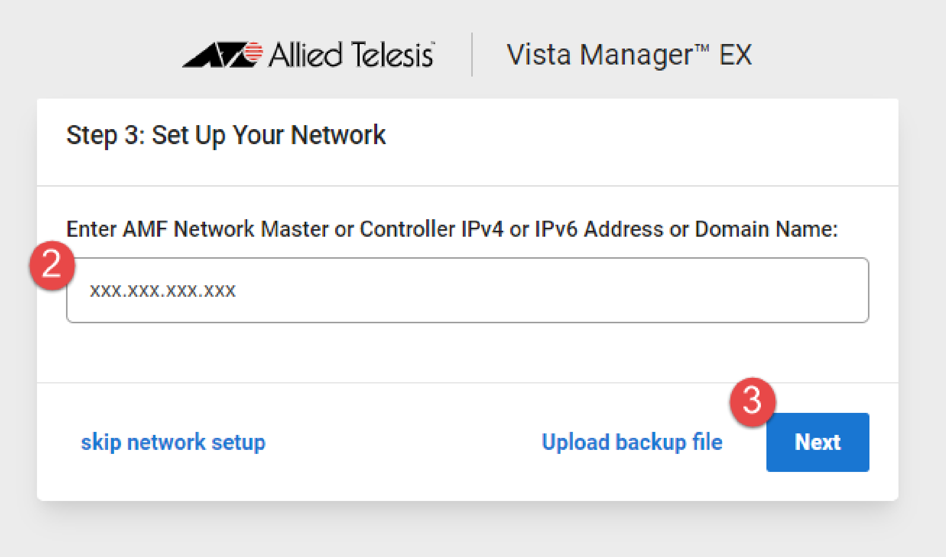
If you are unable to enter IP address

Enter AMF Network Master or Controller Username and Password:

Username:

Password:

2. This takes you to **Set Up Your Network**, and you can then enter the IP address of your AMF Master or Controller...



Step 3: Set Up Your Network

Enter AMF Network Master or Controller IPv4 or IPv6 Address or Domain Name:

xxx.xxx.xxx.xxx

3. Click **Next**.

Supported Device List

AlliedWare Plus devices

The following table lists the AlliedWare Plus devices for which the new features of Vista Manager EX 3.10.0 are available. To use all the new features, the devices must run AlliedWare Plus version 5.5.2-0.1 or later.

Vista Manager 3.10.0 will work with older AlliedWare Plus devices too, but newer features may not be available. We recommend you use the most recent firmware for your device.

Table 1: Models and software file names

Models	Family
AMF Cloud	
SBx81CFC960	SBx8100
SBx908 GEN2	SBx908 GEN2
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L
x330-10GTX	x330
x320-10GH x320-11GPT	x320
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L
x220-28GS x220-52GT x220-52GP	x220

Table 1: Models and software file names (continued)

Models	Family
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340
IE210L-10GP IE210L-18GP	IE210L
XS916MXT XS916MXS	XS900MX
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX
GS980EM/10H GS980EM/11PT	GS980EM
GS980M/52 GS980M/52PS	GS980M
GS970EMX/10	GS970EMX
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
10G Virtual UTM Firewall	
AR4050S AR3050S	AR-series UTM firewalls
AR2050V AR2010V AR1050 V	AR-series VPN routers

Allied Telesis Wireless APs

For details about AP support, see the “What is the AWC Plug-in” section of the Autonomous Wave Control (AWC) Plug-in User Guide.

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com