Technical Guide

Vista Manager EX v3.15.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. Where there are differences in this Guide, they are indicated by **APL**, **VRT**, and **WIN**.

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. For information about the VST-APL, see the Vista Manager Network Appliance (VST-APL) Technical Documents.

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, 7.0, and 8.0. For installation, see the Vista Manager EX Virtual Appliance Installation Guide. Note that this virtual appliance does not support Vista Manager plugins. If you need the plugins, 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-VRT 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 on Windows Server 2012 R2 Hyper-V or VMware vSphere Hypervisor (ESXi) 6.0, 6.5, 6.7, 7.0, and 8.0. This page also shows how to use Vista Manager EX and its optional features.

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

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

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

What's in Vista Manager EX?

You can perform Network operations directly by navigating to 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.
- Network Map
  Displays a graphical topology map of your 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. STOAT plugins for third-party tools, including Forescout, and Nozomi. can also be used for device discovery. You can carry out actions such as backup master, SSH to master, and backup device directly from the network map. The AWC plugin also enables management and monitoring of Allied Telesis APs.
- Health Monitoring
  Displays a customisable dashboard to monitor the health of devices in your network.
- 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.
- Asset Management
  Displays a complete list of all devices on the network and allows you to search for specific devices. You can filter this list by categories or export it. To manage devices, you can create groups, assign icons or view licenses.
- 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.
- Intent Networks
  Provides network optimization, automation, management, and visualization. Also offers automation of branch security and WAN bandwidth management.
- 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 plugins

Optional Vista Manager EX plugins are available on:

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

VRT
- Vista Manager Virtual (VST-VRT).

WIN
- Windows-based installations.

VA Plugins are not available on a standalone Vista Manager virtual appliance.

Vista Manager EX works with a variety of plugins, including:

- AWC (Wireless Controller) plugin
- SNMP plugin
- Trap Receiver plugin
- Forescout plugin
- Nozomi plugin
- Microsoft Intune

For more information about these plugins, see "Plugins" on page 178.

What’s new in Vista Manager version 3.15.x?

Vista Manager version 3.15.x includes both new features and significant enhancements to some existing features, as listed below.

For more information about specific changes, including instructions on how to update your software, see the Vista Manager EX Release Notes.

Contents

Preparing your AMF Network for Vista Manager EX

Vista Manager EX is an application that allows you to monitor and manage your AMF Plus 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.

AMF Plus is available on AlliedWare Plus devices running software version 5.5.2-2.3 and later. The following guide describes both AMF Plus and AMF on 5.5.2-2.3 and later: For step-by step instructions, see the AMF Plus Feature Overview and Configuration Guide.

This section describes how to prepare your existing AMF network for use with Vista Manager EX.

APL VRT 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 v3.15.x

Ensuring compatibility within your AMF network requires specific version considerations. We recommend that AMF devices must operate on version **5.5.5-1.x or later.**

Dependencies outlined based on the status of controller and master devices. For example:

- If any of your AMF Controller or Master devices are running 5.5.5-1.x, then all other devices must run 5.5.5-1.x or later.
- If your AMF Master device is running 5.5.5-0.x, then all other devices must also run 5.5.5-1.x (not a later version such as 5.5.5-2.x or 5.5.5-3.x).
- If your AMF Master device is running 5.5.5-2.x, then member devices can run 5.5.5-0.x or 5.5.5-1.x.

Server requirement

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

Enable the HTTP service on your devices

To use Vista Manager EX, you must enable the HTTP service on all AMF Plus 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 Plus controller or AMF Plus 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.

Run this command only on the registered AMF Plus controller/master 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: To register with Vista Manager EX, ensure that the AMF Plus controller/master has layer 3 connectivity to the Vista Manager EX server.

Configure certificate for device authentication

You can configure Vista Manager EX to use a certificate to authenticate communication within your AMF Plus network. After configuration, the certificate allows the AMF Plus controller/master to automatically authenticate and connect to any device in the network without requiring a username and password.

Note: We recommend you configure a certificate for authentication. If you do not configure this option, you need to ensure that all devices in the AMF Plus network to be managed by Vista Manager EX have the same username and password as the AMF Plus controller/master.

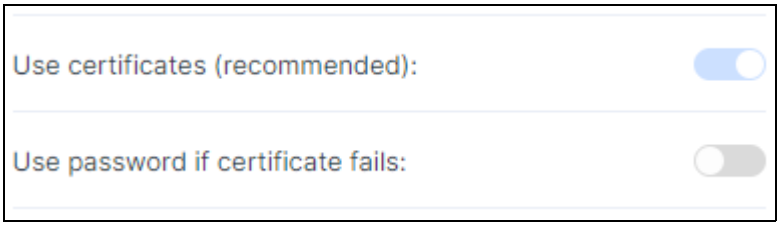
To configure your AMF Plus network to use certificate authentication, enter the following commands on your AMF controller/master:

```
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 Plus controller/master after running the **atmf trustpoint** command for this change to take affect.

Note: In an AMF Plus 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:



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.

Logging into Vista Manager EX

Initial login and setup

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

APL Before setting up Vista Manager EX on the VST-APL, you must 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:

- "Logging into Vista Manager EX after setup" on page 23
- "Registering/Installing plugins" on page 26

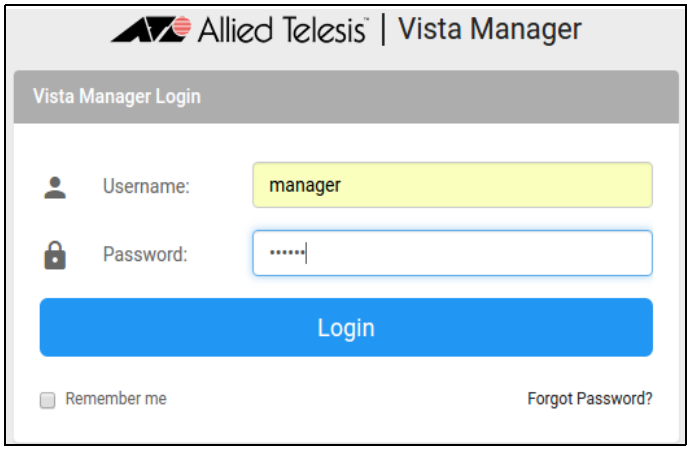
Note that dialog boxes in this section are from a VST-APL. In most cases, the dialog boxes are the same for all Vista Manager platforms.

Initial login to Vista Manager

Initially you can log into Vista Manager by using the default username and password combination (**manager** and **friend**).You can change this once you have logged in. After you log in, there is a sequence of steps to go through to set up your Vista Manager EX account.

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

From the **Vista Manager Login** dialog:



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

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.

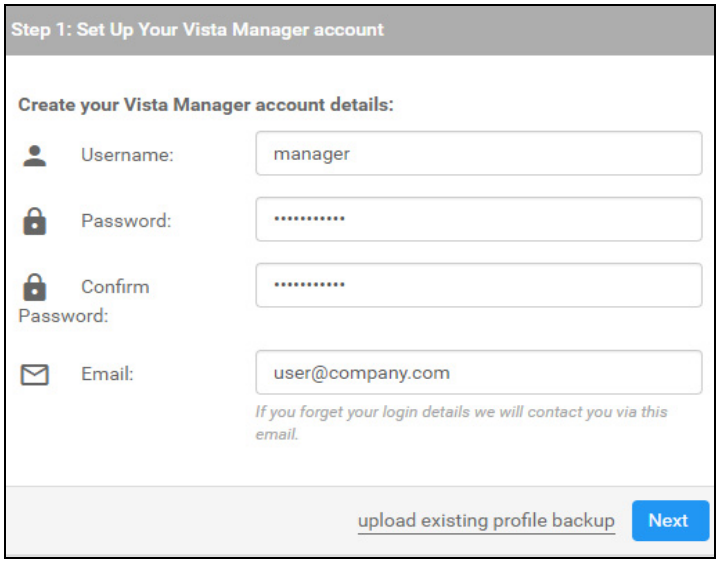
VA To connect remotely, use the URL:

`http://<ip-address>`

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

Step 1: Setting up your Vista Manager account

The **Set Up Your Vista Manager account** dialog displays after you log in. You can change the default login information from this window.



- Enter your new **Username**
- Enter your new **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**.

Step 2: License registration

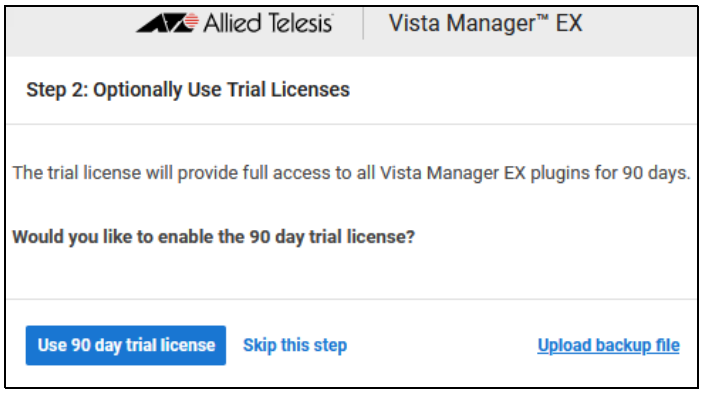
VRT WIN VA

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 plugin and the AIO feature, by clicking **Use 90 day trial license**.

APL

Note: 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 plugin.

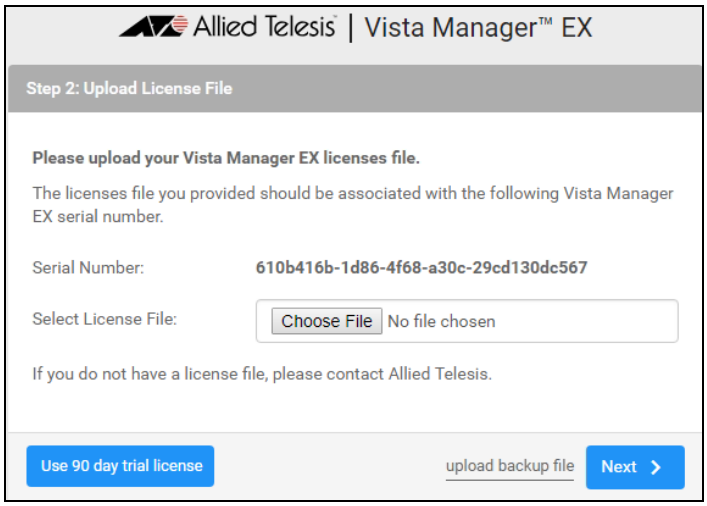
The **Optionally Use Trial Licenses** dialog displays:



- Select the 90-day trial.
- If you wish to upload a licence instead, click **Skip this step**.

Note:If you select the 90-day trial, you need to install your licenses before the end of that trial. For more information, see "About Vista Manager EX Licenses" on page 37.

Otherwise, the **Upload License File** dialog displays:



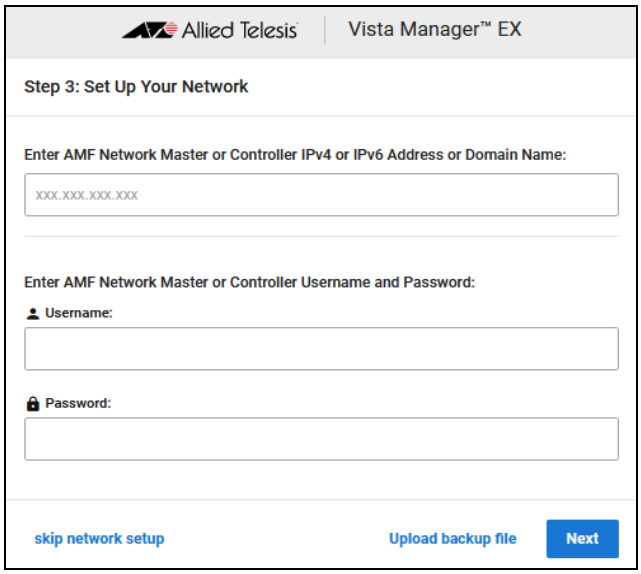
- Install your licenses now by uploading the license file.
- Click **Next**.

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

Step 3: Set Up Your Network

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

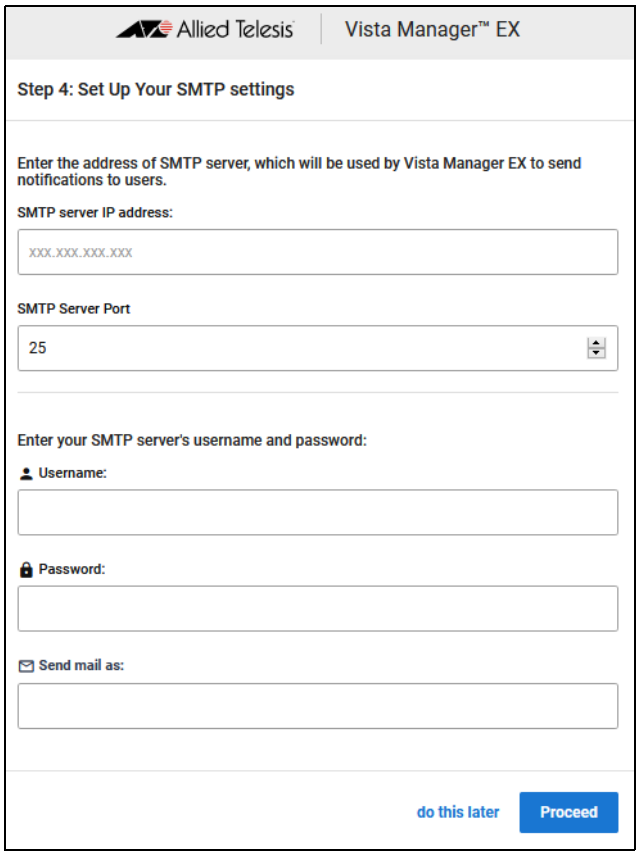
On a VST-APL or VST-VRT deployment, the AMF Master may be the AMF Cloud application, or it may be any other AMF Master or Controller.



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

Step 4: Set Up Your SMTP settings

The **Set Up SMTP settings** dialog displays:



- 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.

Logging into Vista Manager EX after setup

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
```

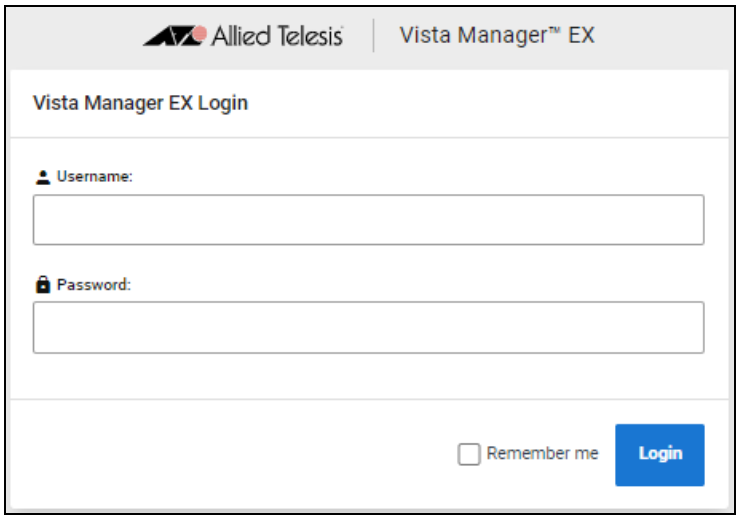
where <*ip-address*> is the address you picked on the **Registration Server IP Address** dialog.

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**.

Note: To enable/disable auto-logout for different users, you can change the **Timeout** in the **User Management** menu.

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.

Changing your password

1. Go to **User Management** 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**

Enabling Two-Factor Authentication (2FA)

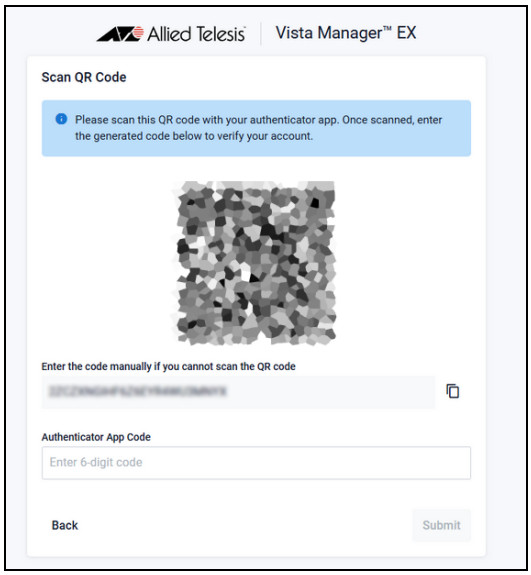
As an Admin user, you can enable 2FA for your own account, other admin accounts, or general users.

1. To enable 2FA, click the toggle on the **User Management** page.

Note: 2FA requires SMTP to be configured before it can be enabled.
If you are using a VST-APL device, 2FA requires an NTP server to be set up for accurate time service.

2. After enabling 2FA from Vista Manager, when you next log in you will be shown a QR code to scan on your authentication app of choice.

2FA is supported with any mobile authenticator that supports TOTP (such as Google Authenticator, Microsoft Authenticator, Authy, LastPass Authenticator, and many more).



- User level accounts cannot enable or disable 2FA.
- Authenticator codes appear under the title ‘VistaManager: Your Username’
- Enter a valid code from your authenticator app into the Authenticator App Code field. Click **Submit** and you will log in as normal.
- After 5 incorrect code attempts, you must wait 5 minutes before you can try again
- Clicking **Remember me** on the login screen skips 2FA, even if it is enabled. **Remember me** lasts for 14 days.

Reissuing the QR code

You can re-issue the 2FA QR in different ways, depending on the status of your account.

- As a normal user, click the reset link sent to your registered email.
- Admin users can enable and disable 2FA for that specific account.

Registering/Installing plugins

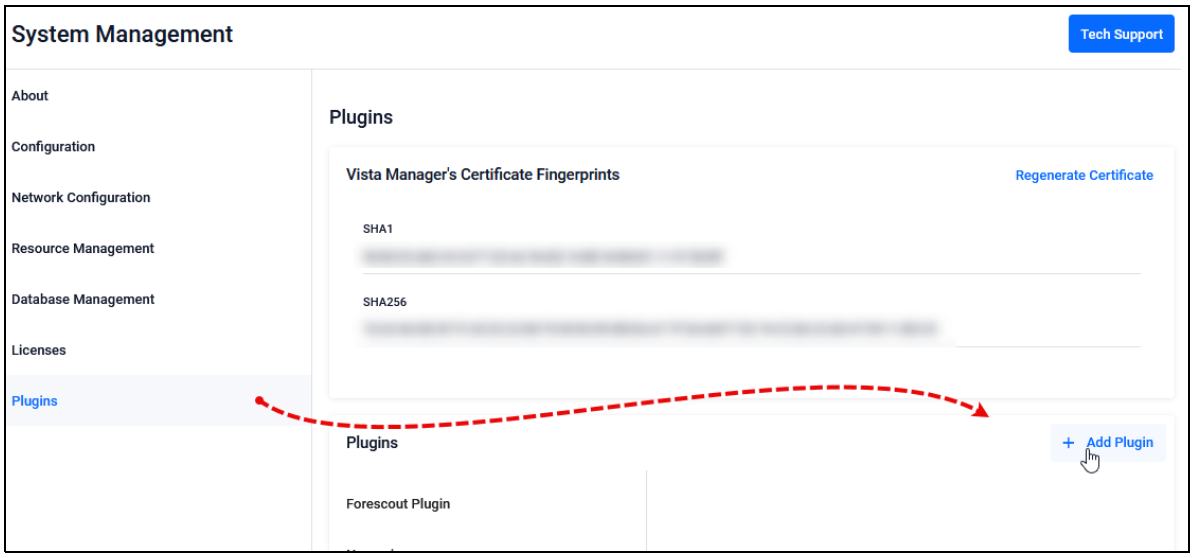
Vista Manager EX supports a number of plugins. This section outlines their subscription requirements and setup instructions.

VRT APL WIN

- The **AWC** plugin requires a separate subscription license from Vista Manager. See "Initial login and setup" on page 19 and "About Vista Manager EX Licenses" on page 37 for details.
- The **SNMP** plugin is enabled by default in an AMF Plus environment from Vista Manager version 3.11.0 onwards. This means that if you have a current active and enabled AMF Plus license on your AMF masters and controllers, then the functionality of the SNMP plugin is available to you. There is no setup required for you to use this.
- The **Forescout** plugin is included as part of the Vista Manager EX software package. You do not need to download it separately; just download Vista Manager EX 3.9.1 or later from our Software Download site.
- The **Nozomi** plugin is supported from version 3.12.0 of Vista Manager EX.

To set up the plugins after you have successfully logged in to Vista Manager EX, go to:

System Management > **Plugins**:



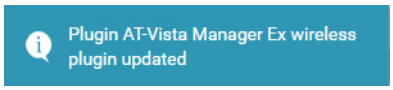
Registering the AWC plugin

1. Click **Add Plugin** and enter the following details for the AWC plugin:

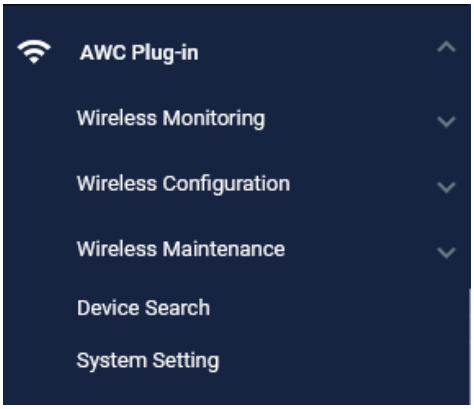
   Server URL: https://<ip-address>:5443/wireless_plugin

   where <ip-address> is the IP address of the Wireless Controller (AWC) plugin application.
2. Click **Verify Connection**
3. Click **Save**.

The following information message is displayed showing that the plugin has been updated:



The AWC Plugin displays a **Wireless** icon on the Vista Manager EX menu. When you click on this icon it will display the AWC menu items.



Registering the SNMP plugin

As of update 3.11.0, the SNMP plugin is enabled by default in an AMF Plus environment. This means that if you have a current active and enabled AMF Plus license on your AMF masters and controllers, then the functionality of the SNMP plugin is available to you. There is no setup required for you to use this. In order to enable the SNMP plugin manually, you can do so with the following steps:

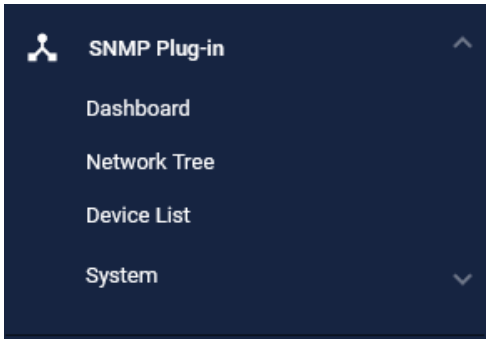
1. Click **Add Plugin** and enter the following details for the SNMP (full) or Trap Receiver plugin:

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

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

The following information message is displayed showing that the plugin has been updated:

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



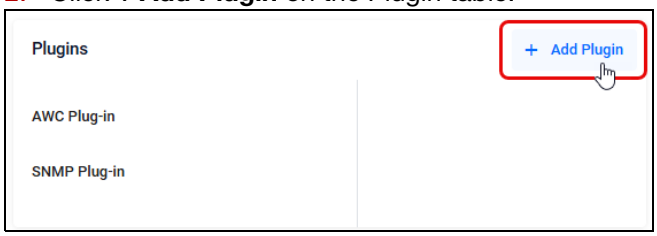
Registering the Forescout plugin

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

You must first configure the Forescout console prior to adding the plugin to Vista Manager EX. For information about configuring the web API module in the Forescout console, see "Prerequisites for installing Forescout" on page 180.

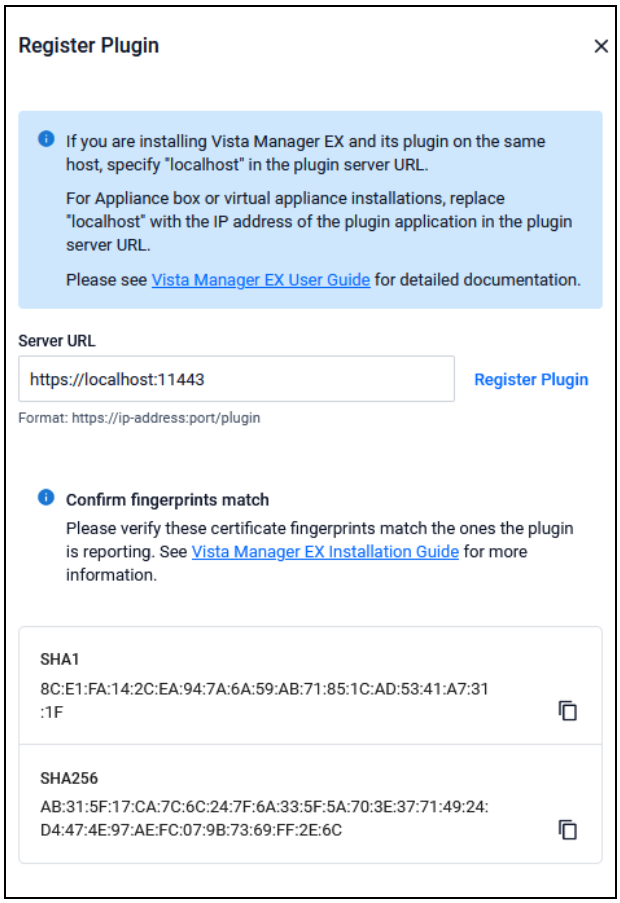
After upgrading to version 3.9.1 or later, you need to register the plugin. To do this:

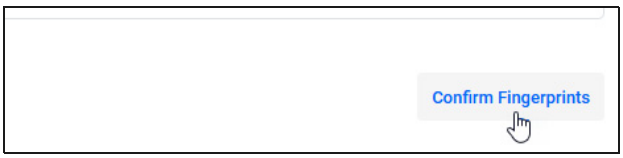
1. Go to **System Management** > **Plugins.**
2. Click **+ Add Plugin** on the Plugin table.



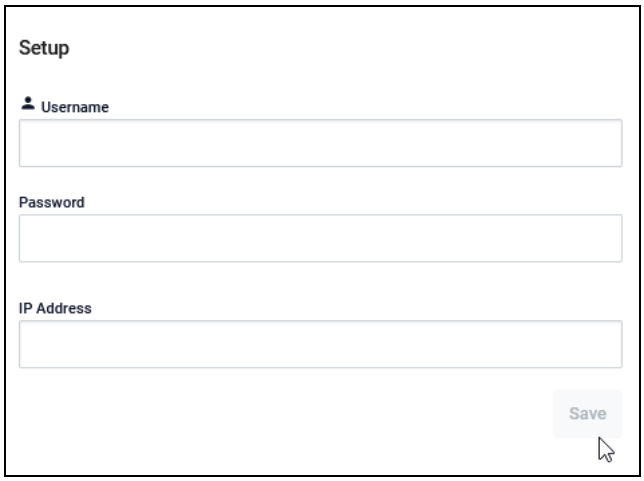
3. Register the plugin in the textbox with the server URL of **https://localhost:11443**
4. Click **Register Plugin** and Vista Manager will generate the certificate's fingerprints.

5. Confirm that the fingerprints match the Forescout program, then click **Confirm Fingerprints**.





6. Scroll down and enter the additional Forescout setup settings:
   - Username
   - Password
   - IP address



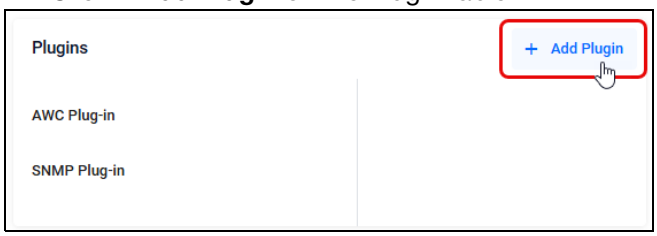
7. Click **Save.**
   The Plugin will be added to your plugin list.

Registering the Nozomi plugin

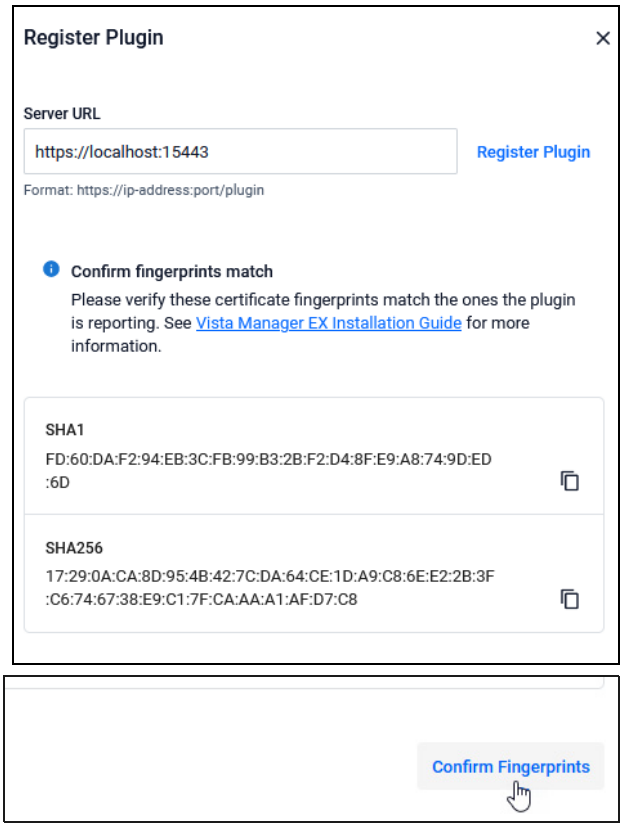
From version 3.12.0 onwards, Vista Manager supports the Nozomi plugin.

You must first configure the Nozomi Guardian sensor prior to registering it in Vista Manager EX. To see information about the initial configuration of Nozomi Guardian, see the Nozomi Plugin User Guide.

1. Go to **System Management** > **Plugins.**
2. Click **+ Add Plugin** on the Plugin table.

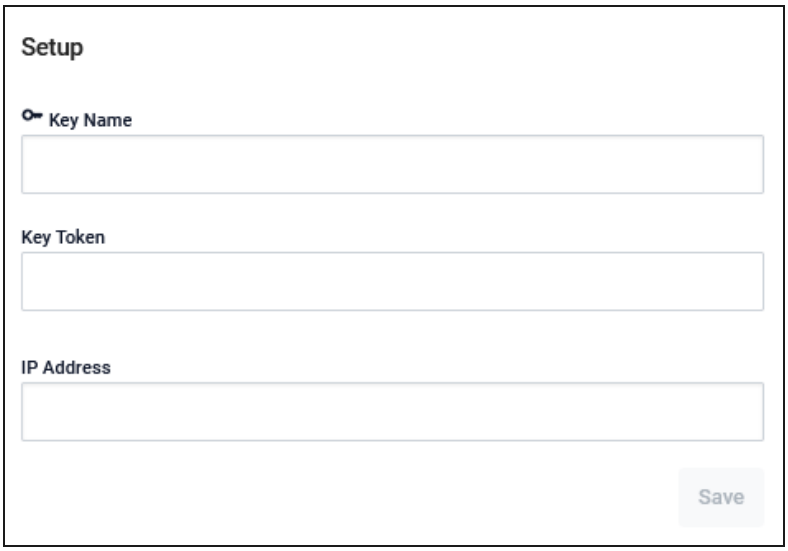


3. Register the plugin in the textbox with the server URL of **https://localhost:15443**
4. Click **Register Plugin** and Vista Manager will generate the certificate's fingerprints.
5. Confirm that the fingerprints match the Nozomi program, then click **Confirm Fingerprints**.



6. Scroll down and enter the additional Nozomi setup settings:
   - Key Name
   - Key Token

- IP address



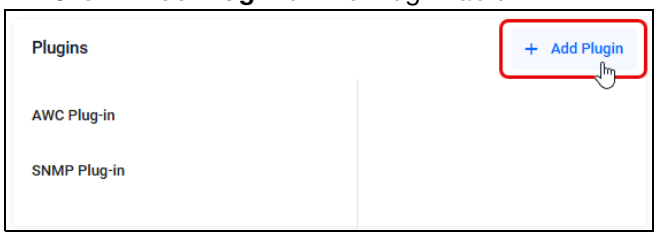
7. Click **Save.**
   The Plugin will be added to your plugin list.

Registering the Microsoft Intune plugin

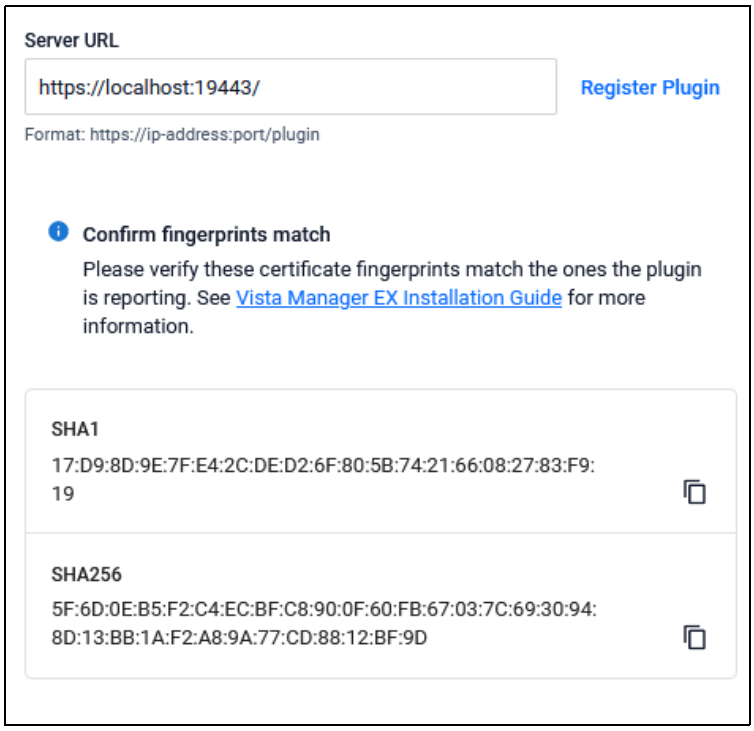
From version 3.13.1 onwards, you can view alert information that is gathered by Microsoft Intune in Vista Manager. For more information, see "Microsoft Intune Plugin alerts" on page 186.

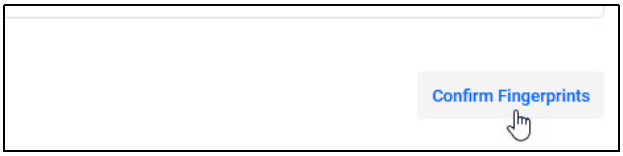
Do not enable the Automatic Blocking feature from the Endpoints table while using the Intune plugin. If you have previously enabled Automatic Blocking, disable it.

1. Go to **System Management** > **Plugins.**
2. Click **+ Add Plugin** on the Plugin table.



3. Register the plugin in the textbox with the server URL of **https://localhost:19443/**
4. Click **Register Plugin** and Vista Manager will generate the certificate's fingerprints.
5. Confirm that the fingerprints match the Intune program, then click **Confirm Fingerprints**.





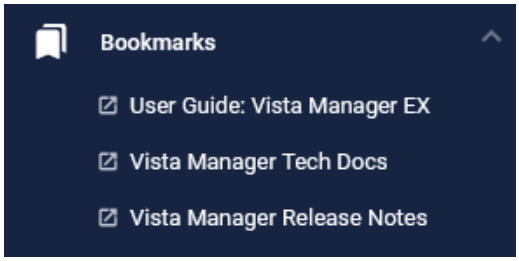
6. Scroll down and enter the additional Intune setup settings:
   - Client ID
   - Client Secret

- Tenant ID

7. Click **Save.**
   The Plugin will be added to your plugin list.

Adding bookmarks

From version 3.14.0 onwards, you can add bookmarks to the side menu. You can bookmark IP Addresses or other URLs for quick access.

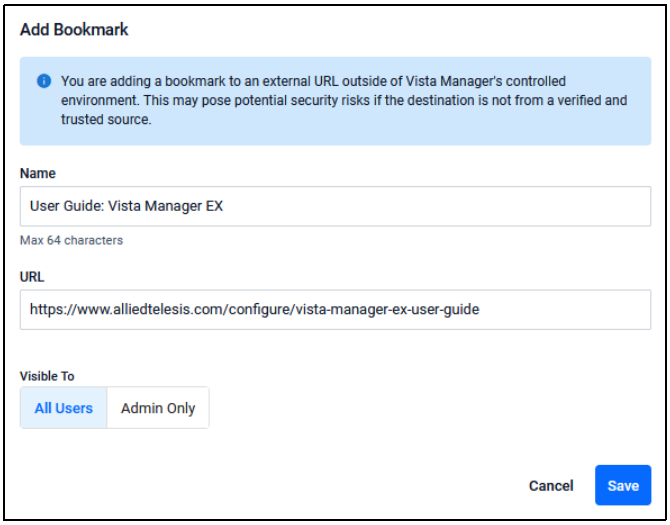


For example, you may want to bookmark this user guide so you can access it directly from Vista Manager. To do this:

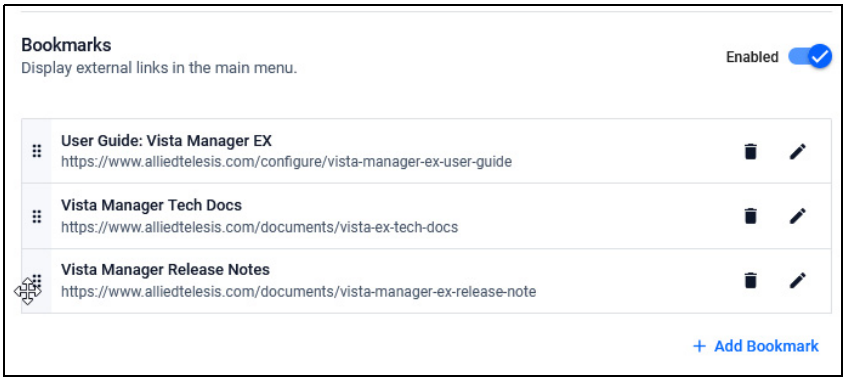
1. Toggle Bookmarks on from the **System Management** > **Configuration** page.

2. Click **+ Add Bookmark**.

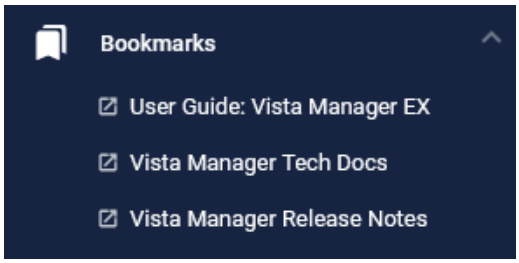
3. Enter a name for the bookmark.
4. Then enter its URL, which is 'https://www.alliedtelesis.com/configure/vista-manager-ex-user-guide'.



5. Click **Save**. The new bookmark will be added to the list.
6. If you have multiple bookmarks, you can rearrange them by dragging them from the drag icon on the left.



If you scroll down on the left-hand side and your bookmarks will appear under the Bookmarks tab.


Bookmarks
User Guide: Vista Manager EX
Vista Manager Tech Docs
Vista Manager Release Notes

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 plugins 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 plugin 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 licenses installed for one plugin that is device-restrictive, each for 10 devices, you will be able to manage a total of 20 devices through that same plugin.

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 plugin licenses have separate license periods. If the base license expires, the optional features will not be available, even if they are still licensed.

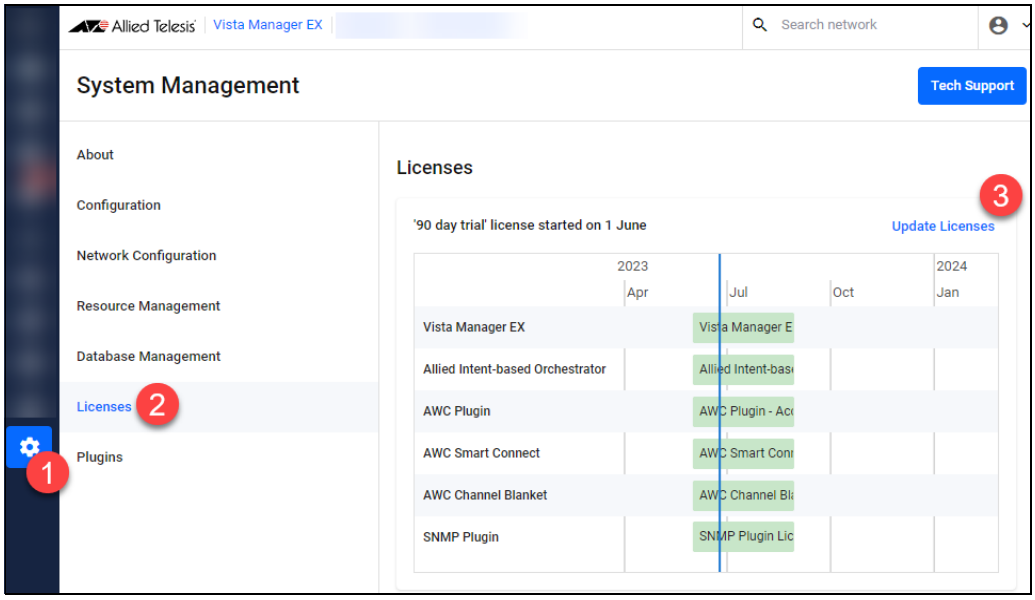
You can install multiple plugin licenses (for the same feature) each with their own license period. This allows you to manage a total number of devices equal to the sum of the devices of the active licenses. For example, if you have two licenses installed for one plugin that is device-restrictive, each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

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 more detail, see "Logging into Vista Manager EX after setup" on page 23.

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 **Update License** 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 plugins 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.

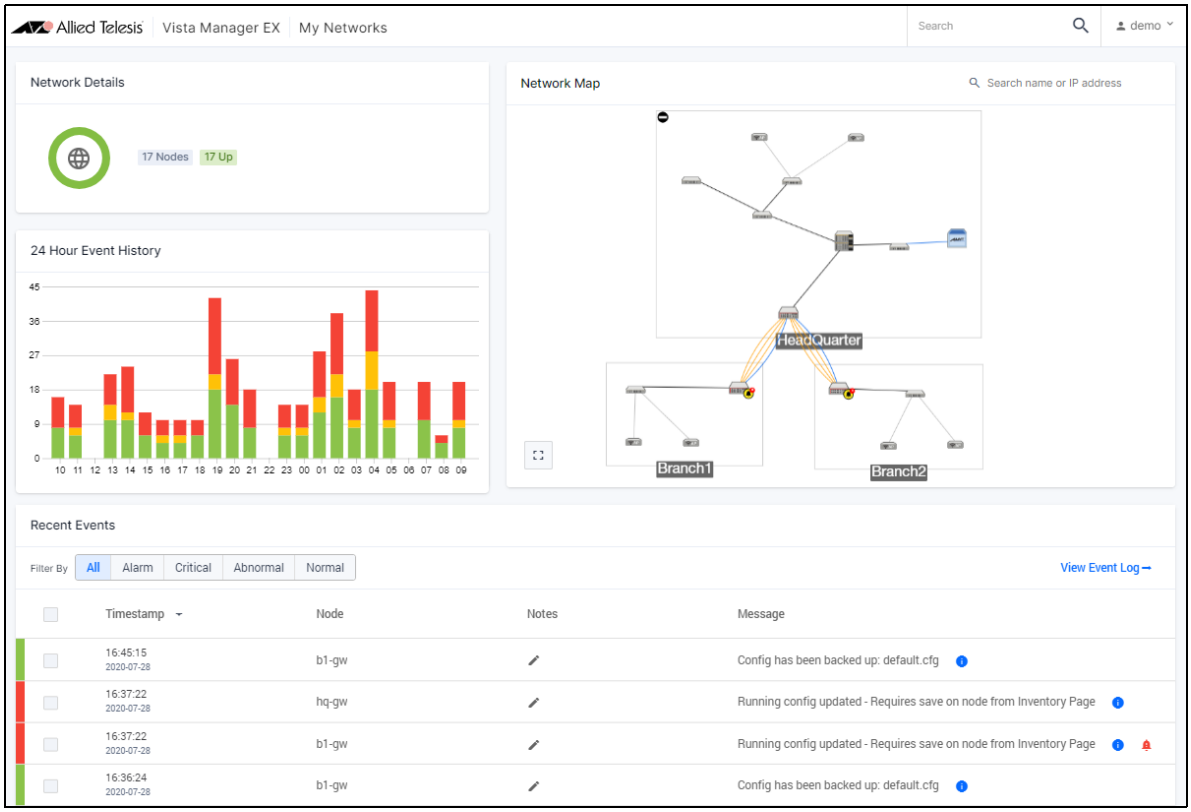
APL On the VST-APL, the base Vista Manager EX license is enabled by default, and does not give access to additional features including plugins. If you choose the 90-day trial license during login, this gives full access to additional features available for Vista Manager EX, including AMF Plus (Allied Intent-based Orchestrator), and the plugins. 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 plugins. 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.

Dashboard

Vista Manager Dashboard

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



The dashboard displays the following information about your network:

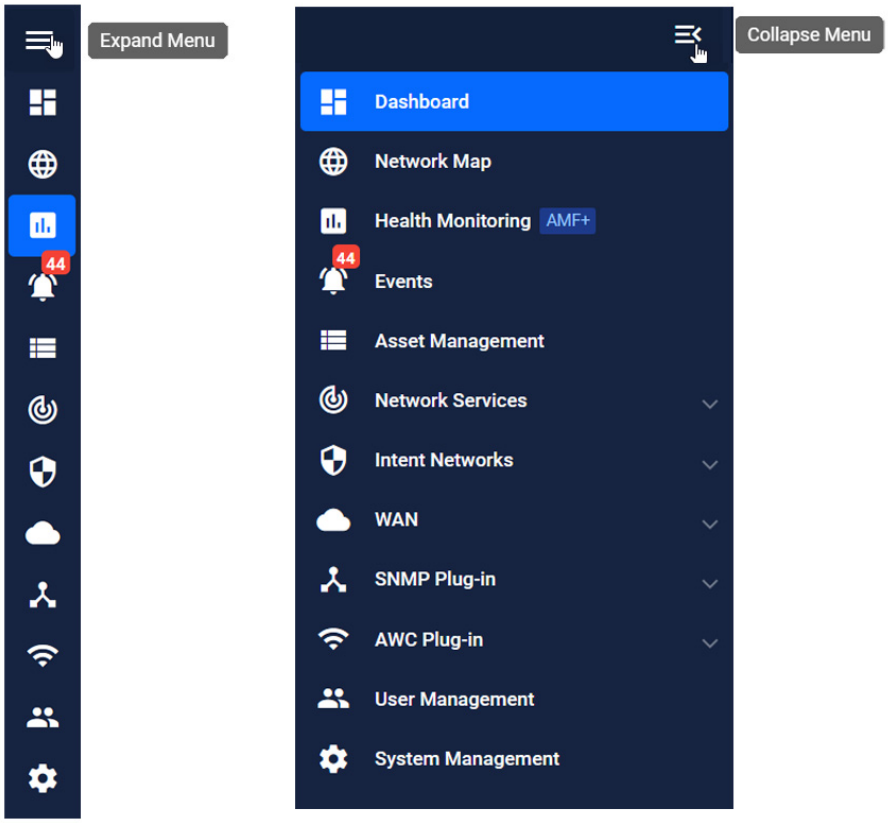
Field	Description
Network Details	Shows the number of devices and status (up, down, abnormal or unmanaged).
24 Hour Event History	Shows a graph of the last 24 hours of log events history.
Recent Events	Displays time, device and any notes or messages relating to each event.
Network Map	Displays the network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

Left-hand menu navigation

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, Network Map, Health Monitoring features, Events, Asset Management, Network Services, Intent Networks features, WAN, User Management, and System Management. Any optional plugins you have installed will also appear in this menu.

For easy navigation from any window in Vista Manager EX you can expand or collapse the sidebar menu as follows. A tool-tip will appear when you hover over the menu:

- Click the hamburger menu icon to expand the menu.
  The expanded menu displays the name of each menu option.
- Click the hamburger menu icon with the small white arrow to collapse the menu.

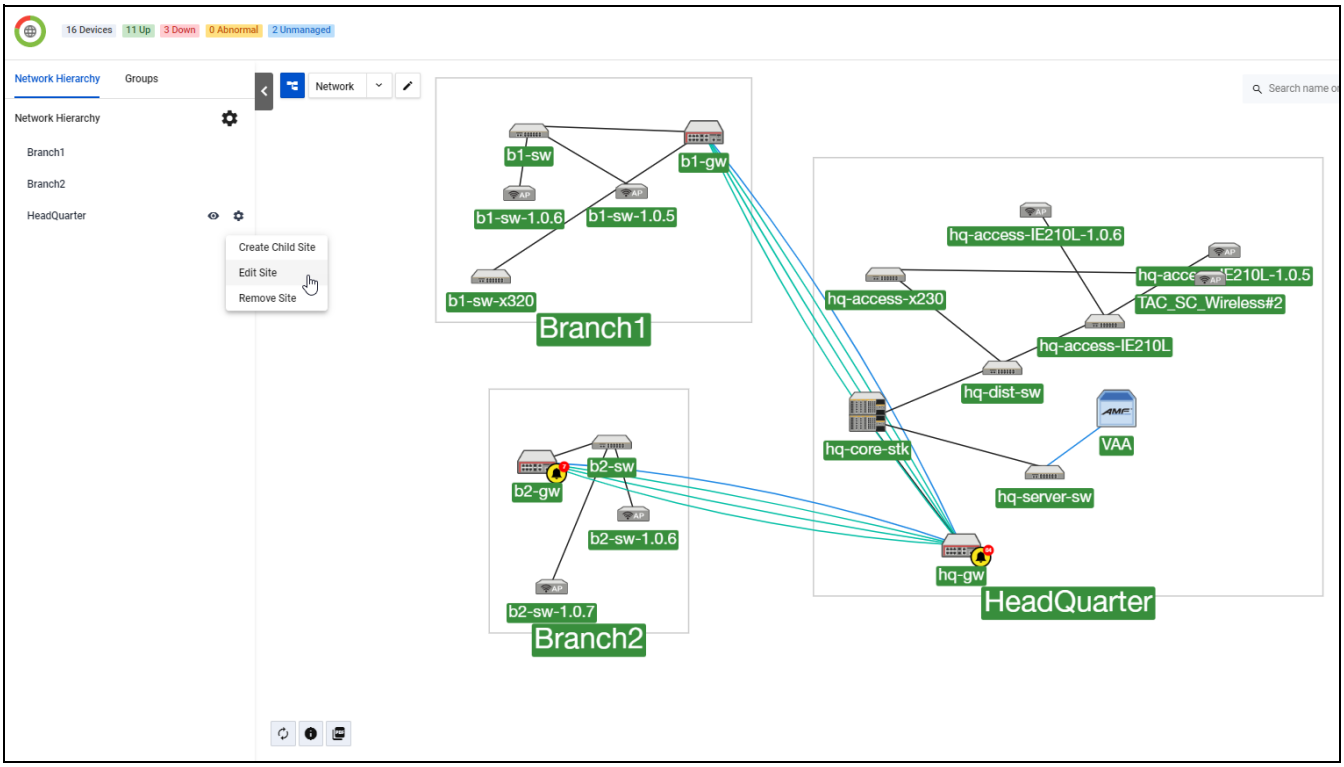


Network Map

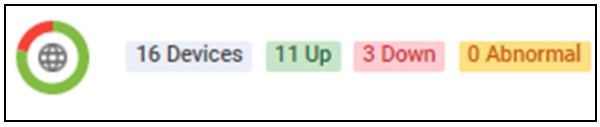
Overview

The dashboard includes an integrated map showing all devices known to Vista Manager EX on the network. This makes it easier for users to see and visualize what is happening on their network. You can change the network map's function by selecting a different map layer. This will be explained further on in this guide.

You can use the left hand menu to access the integrated map on its own screen by using the **Network Map** from on the left-hand menu. From the Network Map you can display details about sites and groups in the network hierarchy and identify the devices in each site or group.



The header on the network map shows the health of your network and devices at a glance.The colored labels correspond to devices on your network, where the color displayed on the header matches the label under the device.

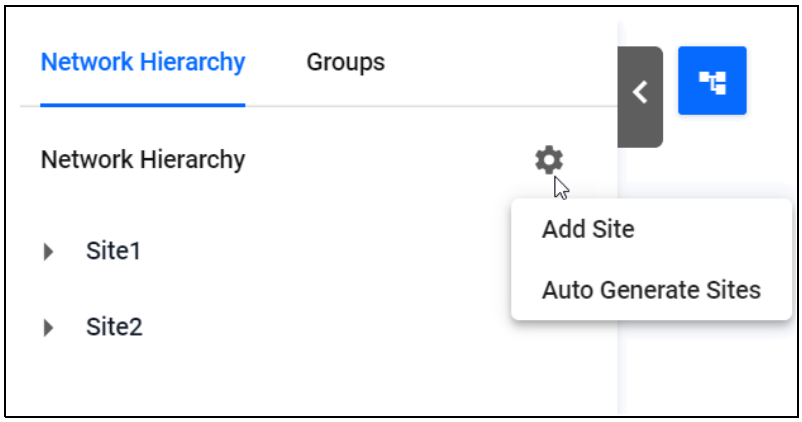


Network Map buttons

The network map has a variety of different tools for network organization. The following section explains the buttons that appear on the Network Map page and their functions. These buttons also appear on other map layers.

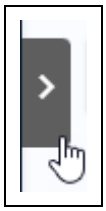
Network Hierarchy

The **Network Hierarchy** button brings up the network hierarchy side menu.



From this menu, you can see sites and groups that are created on your network. If you click on the **cog icon**, you can add or generate sites. The Groups tab displays a list of the groups in your network, and you can edit them if you wish.

You can collapse this menu by clicking the arrow button on the side of the panel.

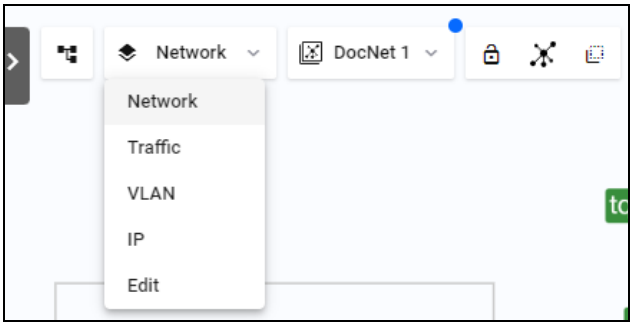


When you select a single device, the side menu displays device settings. To see more about device settings, see "Devices on the Network Map" on page 52.

Map layer drop-down

The Map layer drop-down defaults to the Network Map. You can expand the Map layer drop-down by clicking on it, where you can view different layers of the map.

Depending on the map layer you select, the sidebar offers a variety of different customizable settings and statistics about your network. For information on the different map layers in more detail, see "Map Layer" on page 47.

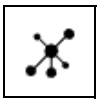


You can select any of the following layers: Network, Traffic, VLAN, IP, Edit

Lock topology layout

You can use the **lock topology layout** button to lock the position of all devices on the map.

Auto generate topology layout

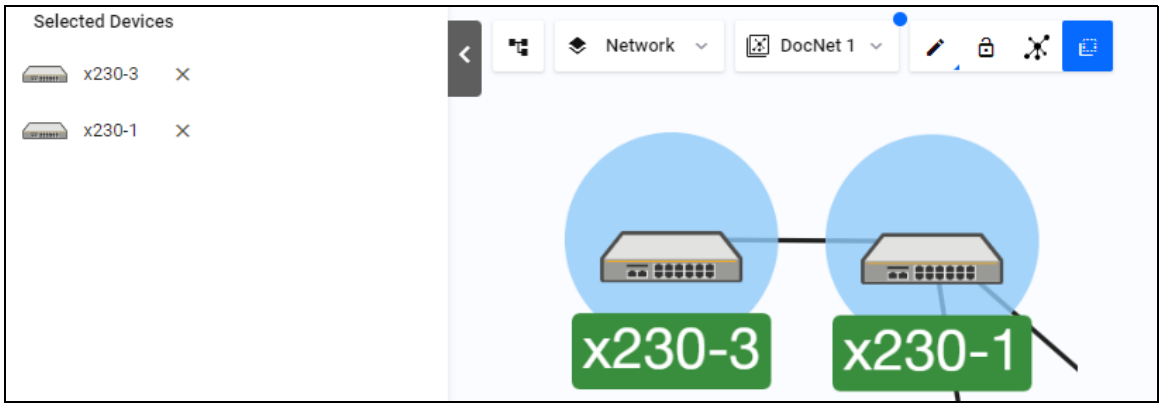


You can use the **auto generate topology layout** button to generate a new map layout. Clicking on this button creates a confirmation box before you continue. The current positioning and any floormap image used is overridden when generated. Note that it cannot be selected if the topology has been locked, or multi-select is enabled. This process cannot be reversed.

Multi-select devices

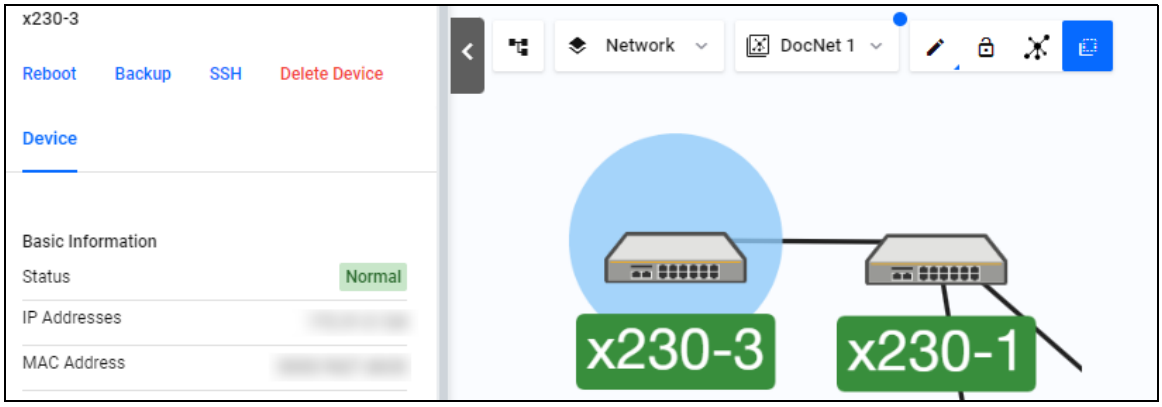
- The **multi-select devices** button enables you to select multiple devices on the map.
- Once you click this button, you can click any device on the map to select it.
- If you select more than one device, they will be displayed on the left-hand menu.
- You can select the **X** to remove them from the selection.
- Select the lock topology button with the multi select button to pan around your map and select multiple devices without moving them.

With the multi-select button enabled, the side panel appears showing a list of selected devices when more than one device is selected.



- On the selected devices list, click the **X** to remove the device from the selection.
- Click a selected device again to deselect it.
- Click anywhere on the map to de-select devices.

When only one device is selected, the side panel shows details of that specific device.



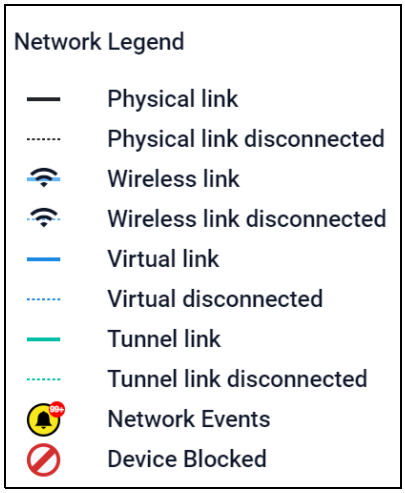
Refresh Topology

The **Refresh Topology** button refreshes the network topology.

- Click this at the bottom left of the map screen to trigger polling.
- After polling is complete, the web browser will update the status of the equipment and new devices will appear. The icon turns gray and spins if it is currently processing.

Information icon

The **information icon** button displays a legend for the links used on the map. Its function changes depending on what layer you are on. It displays the following on the Network Map:



Export PDF

Click the **Export PDF** icon to export a .pdf file of your network. A map file will download locally, that retains any zoom properties that your current map view has. The exported PDF prints the name of your network and its IP Address in the header.

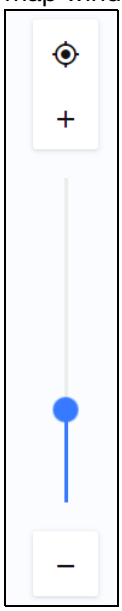
Backwards navigation

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

Zoom functionality

You can zoom in and out by clicking the (+/-) buttons or dragging the zoom slider. The top cross-hair button is the reset topology button, which re-centers and resets the zoom of the network map in the map window.



Select topology layout

You can click the **Select topology layout** button to change between different network topology layouts.

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.

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.

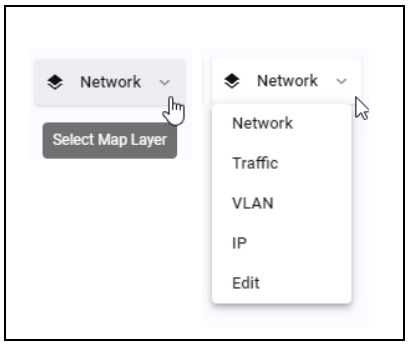
Selecting a layout

The **Select topology layout** button 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 are also visible in the drop-down list.

If a specific 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.

For more information, see "Changing the Network Map Layouts" on page 72

Map Layer



Network map Layer

The majority of the network layer functions have been previously explained in the button section. This section explains extra information about features in the network layer.

Device status

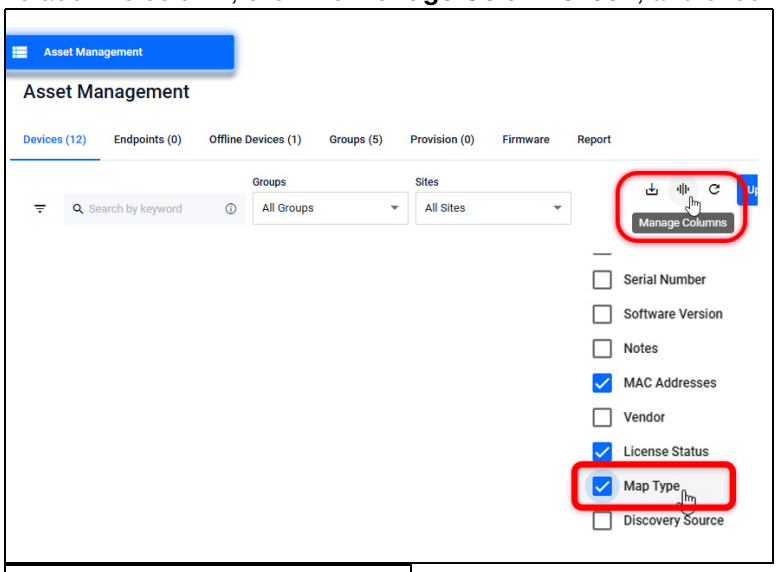
From the network map, you can check the status of a device at a glance. The status of a device is indicated by the device's title background color. The key is located in the header of the Network map page.

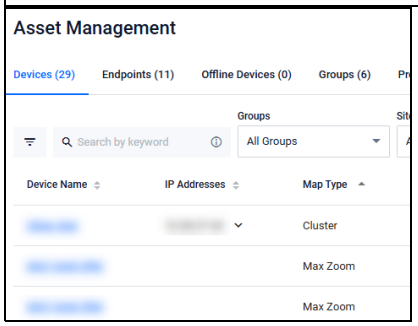
Devices will not display a Status if the device does not provide one.

Map Type

From version 3.13.1 onwards, a **Map Type** column has been added to the **Asset Management** page.

To add this column, click the **Manage Columns icon**, and check the **Map Type** column.

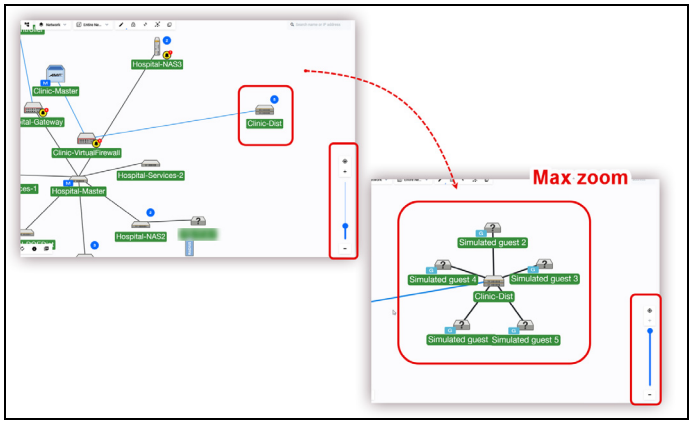




The Map Type column aims to differentiate nodes that are:

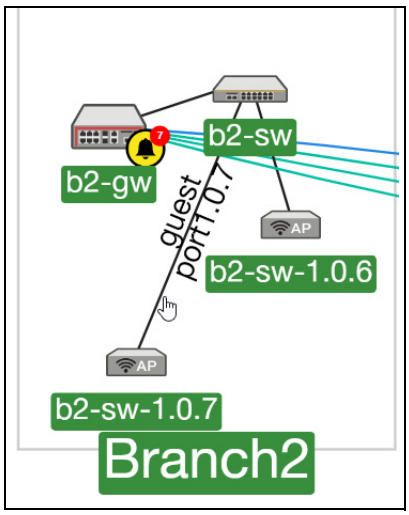
- Cluster nodes (Stacked devices),
- Device nodes (Devices seen on the map at all zoom levels),
- or Max-Zoom (Devices that are only seen on maximum zoom).

Device Links



When you click on a link between two devices on the Network Map, you can view information about the link, such as the ports connecting each device.

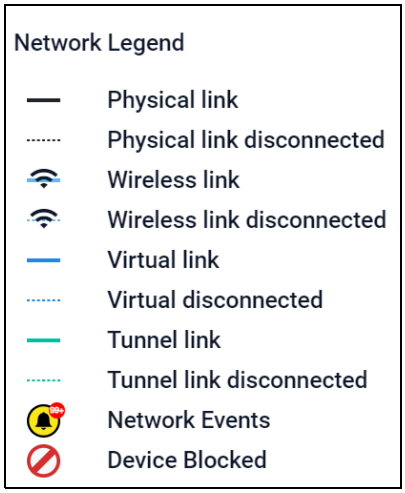
From a glance, you can verify what type of connection and connective status the link has (either disconnected or connected).



Devices that are physically attached to another device are indicated by gray links. Hovering over a gray link displays the port number.

Note that you can create custom links in the edit map layer, see "Edit map layer" on page 102 for more information.

Click the information icon to see all of the different network link types.



From version 3.15.0 onwards, when you click on a link between two devices on the Network Map, it displays two tabs that represent the two port directions of the link.

Note that the following types of links will not display two tabs:

- Tunnel links
- STOAT links where one link is a non-STOAT device and is not learned via any other plugin.

Device status: Down vs. removal from Vista Manager EX

Devices may be put into a Down state instead of being removed from Vista Manager EX entirely.

For example, when an AMF device goes down, the device will no longer be in the AMF topology, but Vista Manager EX will move the device to a Down state and keep it on the map. For more information on network map display when a device goes down or is removed, see "Device status: Down vs. removal from Vista Manager EX" on page 50.

When a device goes down or leaves the network, is it still displayed on the network map, or is it removed? The table below describes how Vista Manager EX and the network map behave when a device goes down or is removed:

Table 1: Device status and discovery method behaviour

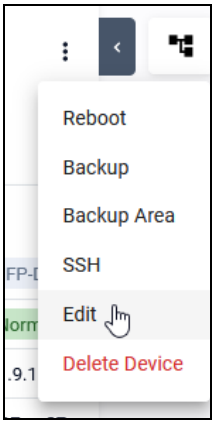
DISCOVERY METHOD	BEHAVIOUR
STOAT (LLDP)	When a STOAT LLDP devices goes down, the device is removed from the STOAT API and removed from Vista Manager EX. There is no Down status for STOAT nodes, they are just removed from the map.
STOAT (DHCP-Snooping)	There are two scenarios: ■ If a STOAT DHCP-Snooping device goes down gracefully and a DHCP release is sent, it will behave the same as STOAT (LLDP), i.e. the node will be removed from Vista Manager EX and the map. ■ If a STOAT DHCP-Snooping device goes down disgracefully and no release is sent, the device is displayed until the DHCP-Snooping entry times out, then it is removed entirely.
STOAT (wireless)	If a wireless device leaves the network, the node stays as 'unassociated' for a 5 minute period, when that 5 minute period expires, the wireless device is removed from STOAT and disappears from the network map, there is no Down state.
AMF	When an AMF device goes down, the device will no longer be in the AMF topology API, but Vista Manager EX will move the device to a Down state and keep it on the map.
Nozomi	Nozomi doesn't return a state for nodes, also Nozomi won't remove down devices from its inventory. What this means is that when a Nozomi node is learnt, it will display on the network map as Up, even if the device is physically Down. If a user manually removed the client from Nozomi, Vista Manager EX will then remove the node from the map (it will have no Down state).
Forescout	Forescout does return a state, this state can be Up or Down. ■ If the client state returned from Forescout equals Up, then Vista Manager EX displays the node in an Up state. ■ If the client state returned from Forescout equals Down, then Vista Manager EX displays the node in a Down state. ■ If Forescout doesn't return any data for the client (the client is missing in Forescout), Vista Manager EX removes the client from the map, the client will not go into a Down state.

Devices on the Network Map

You can interact with devices on the map by clicking on a selected device, or double clicking on a device will show all the device information on the sidebar. Clicking and dragging a device's icon allows you to re-position it on the map.

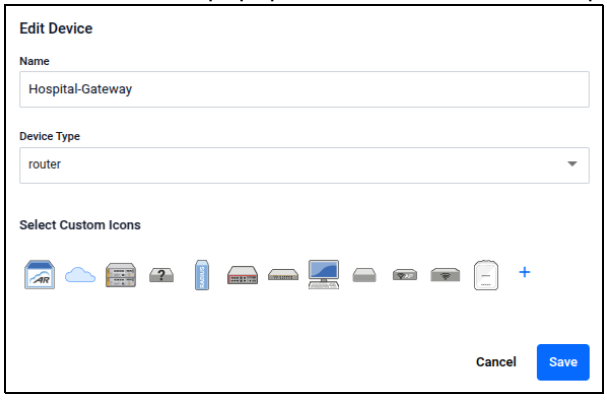
Clicking on a device brings up the Device information side menu.

You can change the name and icon of a device learned by Vista Manager by clicking on the device, and clicking **Edit** from the three dots menu that appears next to its icon from the side menu.

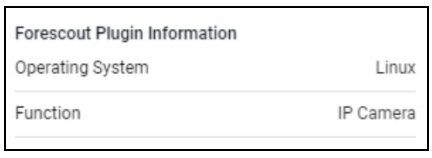


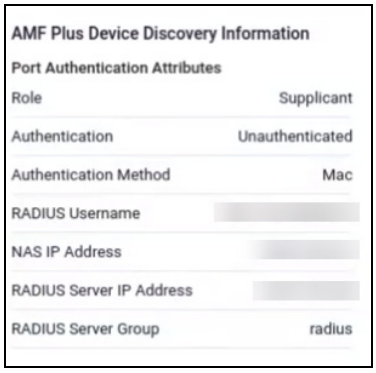
- In the event that Vista Manager has not discovered a device, you can create a custom device and configure the MAC and IP addresses for the device.
- You cannot customize IP or MAC addresses of devices that are automatically discovered. You can only customize addresses of devices that you add manually.

The **Edit Device** popup shows the customizable properties of the device you are currently editing.

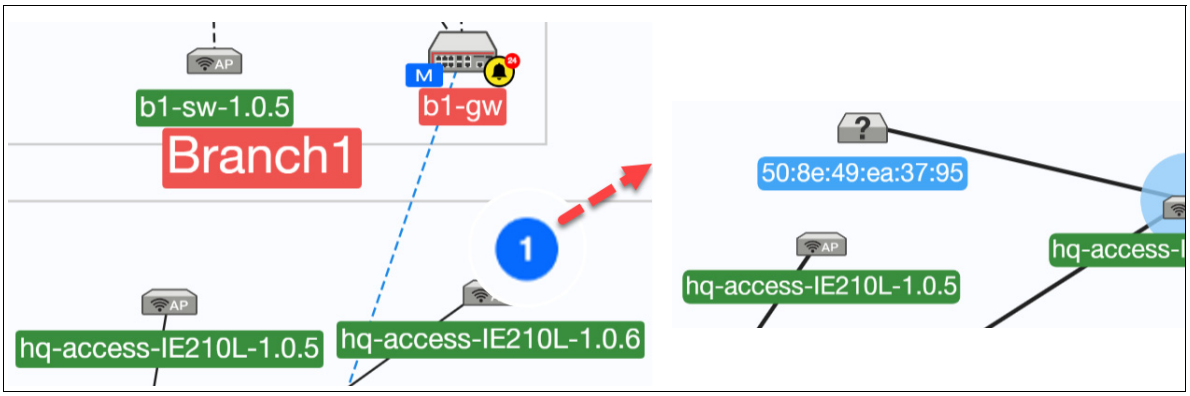


If a device is discovered by a plugin, or by AMF Plus Device Discovery, an extra category will appear under the Basic Information of the device, that shows relevant information about the device, including how it was discovered and how it may relate to other parts of your network.





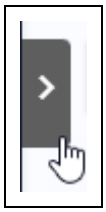
The STOAT feature displays discovered nodes and devices on the network map. For more information on STOAT see "STOAT Device Discovery" on page 148.



The following sections discuss various device functions available from the side menu:

- "Rebooting a device" on page 55
- "Backing up a device" on page 56
- "SSH (Secure Shell) to a device" on page 57

You can click the button next to the side menu to collapse the menu:

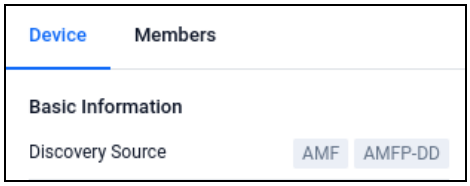


From version 3.12.0 onwards, two changes have been added to Device icons on the Network Map:

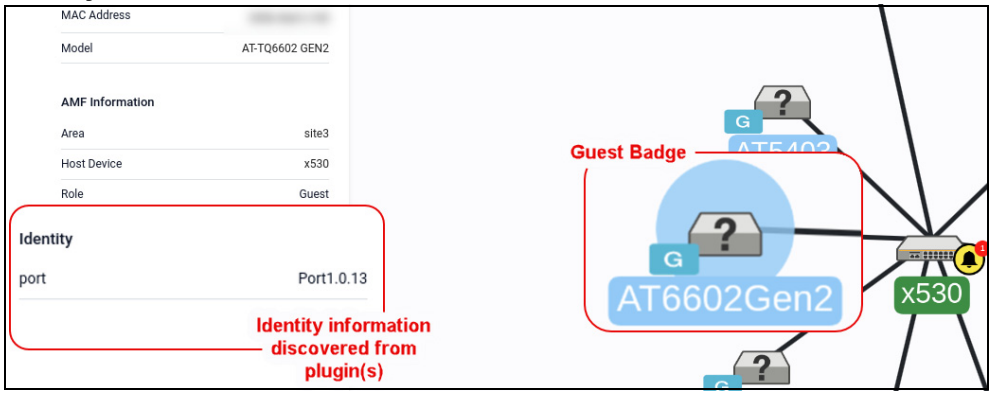
- All devices now display an icon next to the device name on the Device Information side-panel on the Network Map.
- The edit device feature has now moved from a badge on the icon image, to the three dots next to the device name. Click the three dots to edit a device.

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

From version 3.13.1 onwards, Vista Manager displays a **Discovery Source badge** under a device's Basic Information, about how the device was discovered.



In the Device information side-panel, new tabs including information gathered from plugins are **Identity**, **Functional** and **Network Access**.



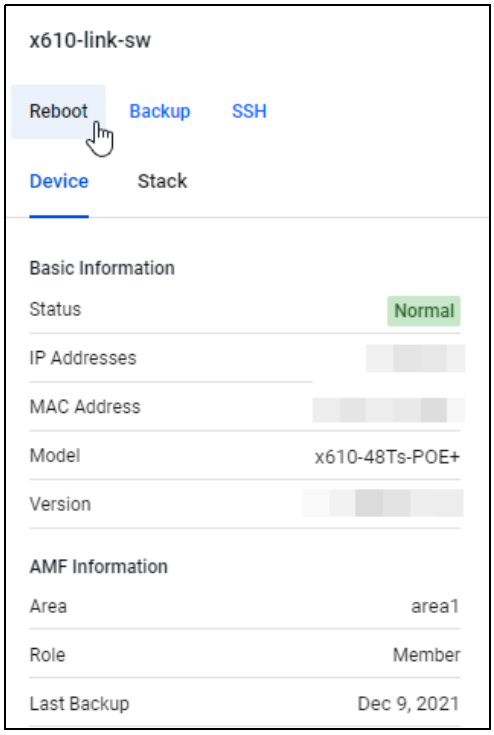
An Guest badge has been added next to AMF Guest devices on the Network Map.

The badges M, C, C/M and G appear on Network layer of the Map and the Asset Management pages. These stand for:

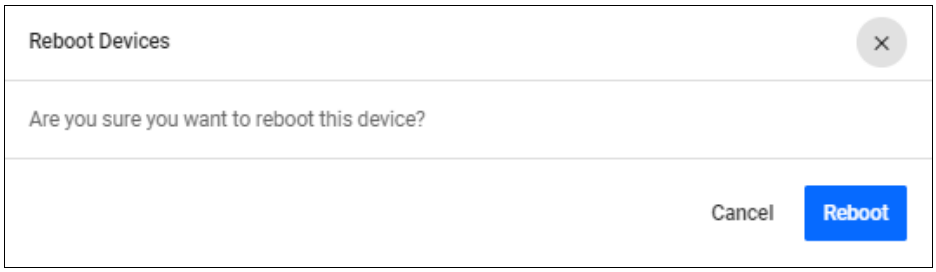
- M - Master
- C - Client
- C/M - Client/Master
- G - Guest

Rebooting a device

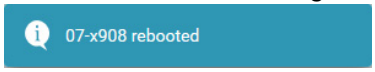
To reboot a device, first select the device that you want to reboot:



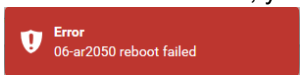
- Click the **Reboot** button. A confirmation dialogue will appear.



- Check that you have the correct device selected and click the **Reboot** button if you are sure that you want to reboot the device.
- An information message is displayed showing that the selected device has rebooted:

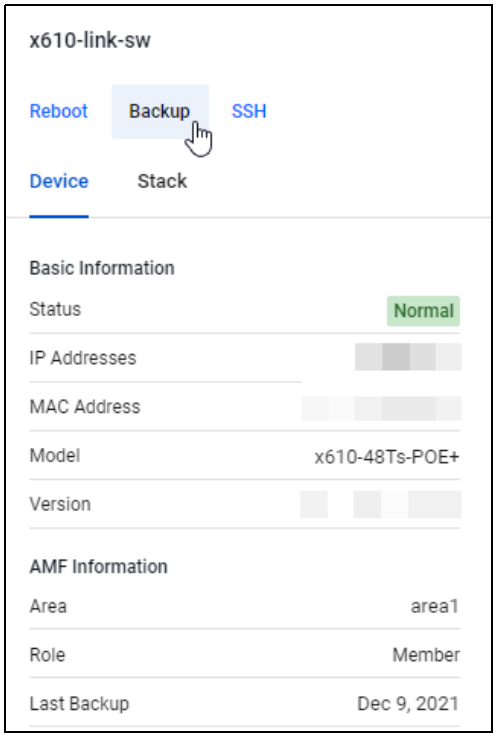


- If the reboot fails, you will see an error message as follows:



Backing up a device

To backup a device, first select the device that you want to back up:

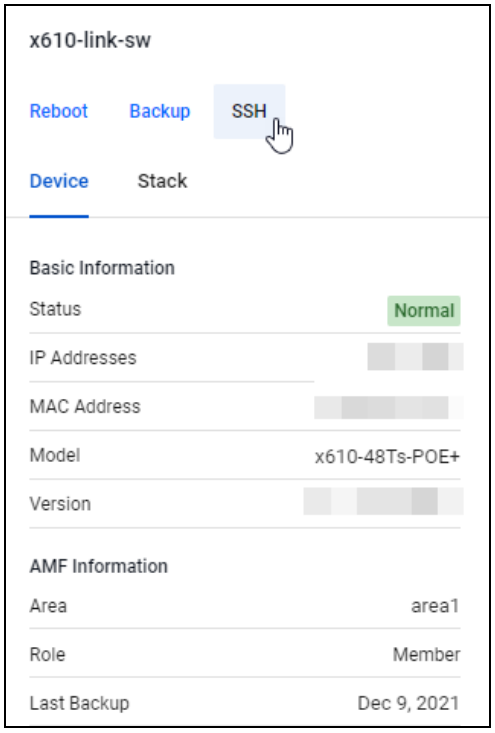


- Click on the **Backup** button.
- An information message is displayed showing that the backup has occurred:

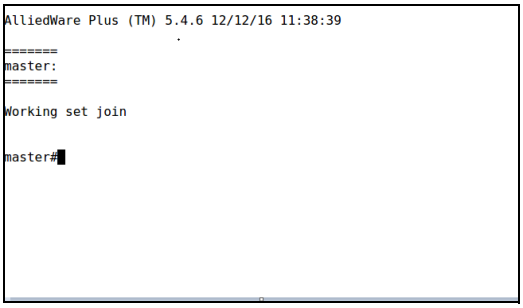
SSH (Secure Shell) to a device

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.

To SSH to a device, first select the device that you want to connect to:



- Click the **SSH** button to start a CLI session.
- The following window will open in your browser:



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

Changing a Device's name

From version 3.12.0 onwards, you can rename devices from the Network Map and Asset Management page in Vista Manager. Two new options have been added to nodes on the Network Map, where you can edit and reset the names of devices

To edit a device's name, click on the **Edit** option of the action tab on the Asset Management page.

Note that the custom name does not overwrite the device's hostname.

Device Name Priority

You can name a device through different plugin and AMF node menus. The device's name on the map will be determined by Vista Manager's internal hierarchy. The hierarchy of names is as follows:

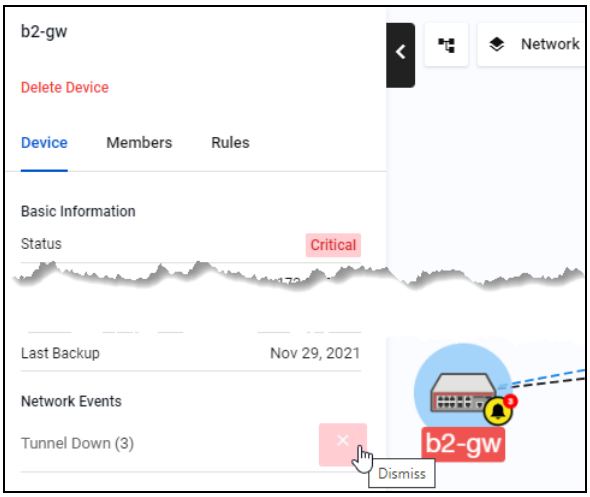
1. User-Defined name (from Network map)
2. AMF (non-guest node)
3. AWC plugin
4. SNMP plugin
5. AMF (guest node)

For example, a device which has separate names set in the SNMP plugin and AWC plugin will have its AWC name display as it is above the SNMP name in the hierarchy. It is important to note that devices receive their name on the network map via polling, and will be updated after polling. If the name is an IP Address or MAC Address, it will be used according to the hierarchy.

From version 3.12 onwards, the user-defined name (the name that you give a device from the Network map) will display as it takes priority over how the device was discovered.

Critical Events

Critical events are displayed on the network map 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.

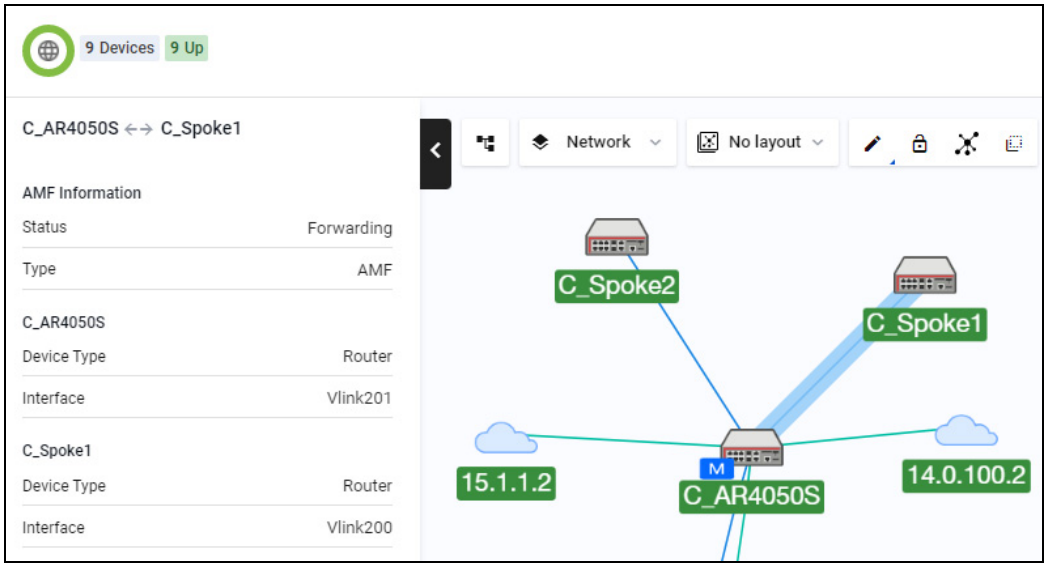


Tunnel Monitoring

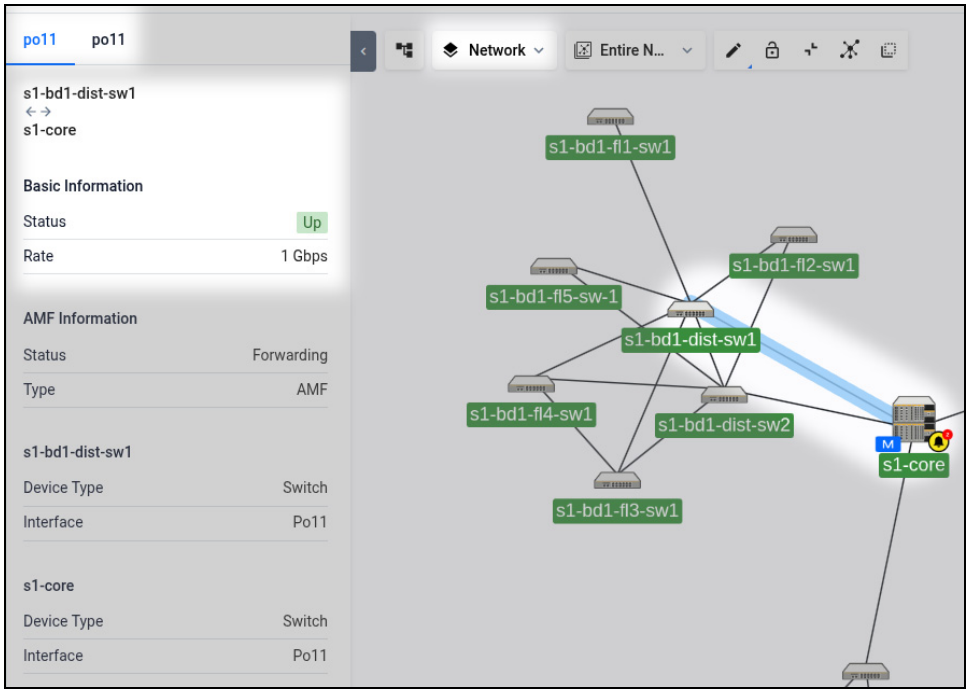
When you click on a device link, the left-hand side displays information about tunnel monitoring on the map.

You can see the speed rate of the link in gigabits per second (Gbps) under the status column. This speed will scale based on the speed of the link.

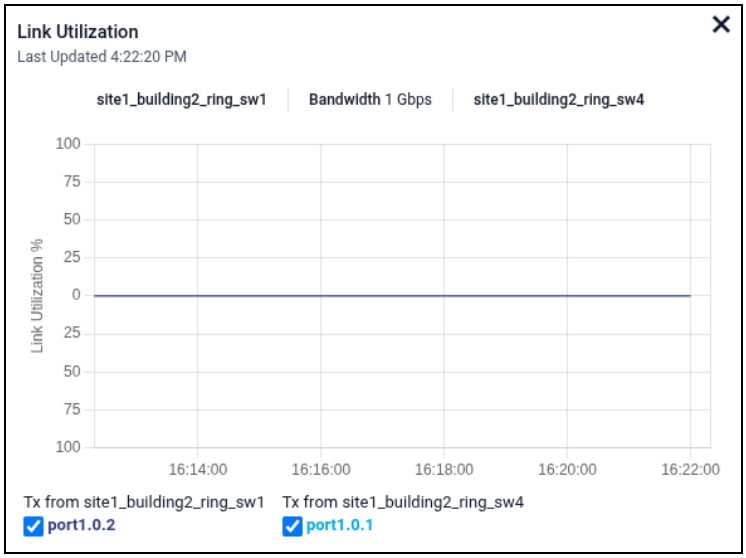
Tunnel monitoring automatically detects supported tunnels between an AlliedWare Plus device and a remote device that is not part of the network. The map is automatically updated if there are any changes to an existing tunnel or when a new tunnel is configured. For information on creating custom links see "Creating custom links" on page 102.



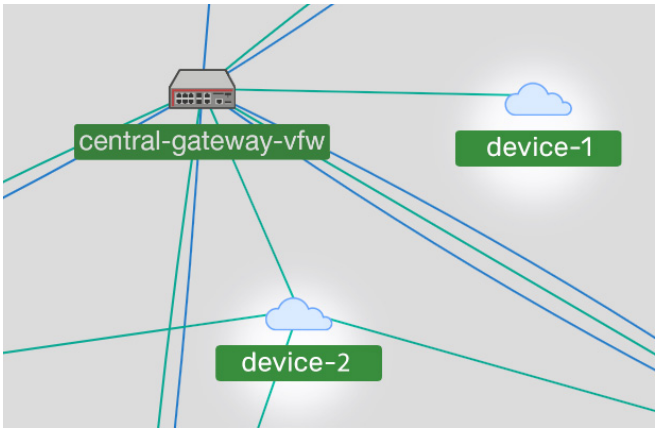
The map detects IPv4 PPPoE configuration and display these links and devices on the map similar to the tunnels. You are able to configure interfaces and bandwidth on a custom link so that the link utilization data is available. Click on any link on the map to view the link utilization. For information about how to view link utilization see"Creating link utilization rules" on page 87.



The Link Utilization graph also shows the link Bandwidth. This label will change depending on the speed of the link (such as Kbps, Mbps, or Gbps).



Monitoring non-AMF devices



To add a non-AMF device to the map, see "Detecting non-AMF devices on the Network Map Layer" on page 63. After manually adding non-AMF devices, you can view them on the map.

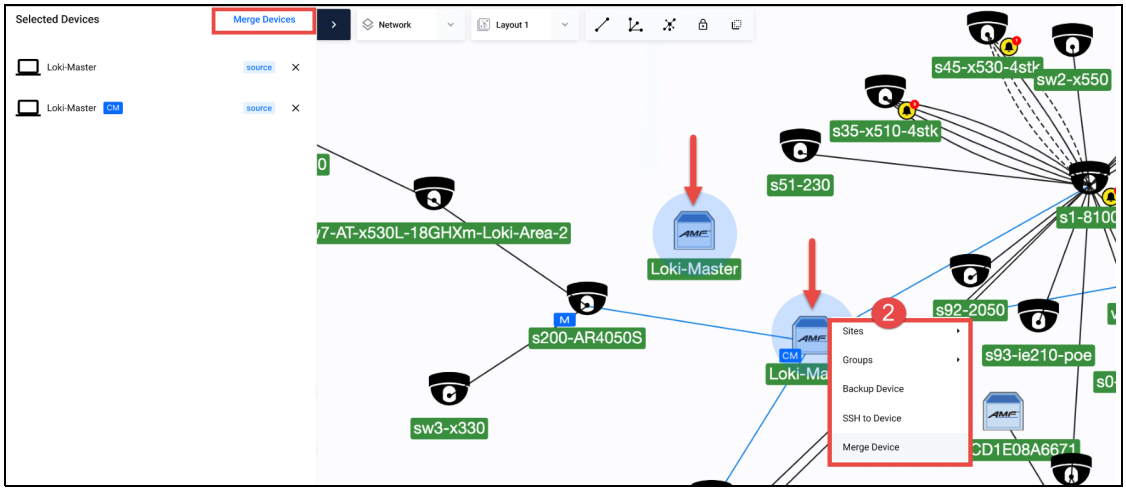
Merging network nodes

You are able to merge nodes on the network map, which is useful if there are duplicate nodes on the map. In most cases Vista Manager EX is able to merge topology information including duplicate nodes. Device nodes are discovered by STOAT, for more information about STOAT see "STOAT Device Discovery" on page 148. However, when Vista Manager EX can't automatically merge nodes together, you can:

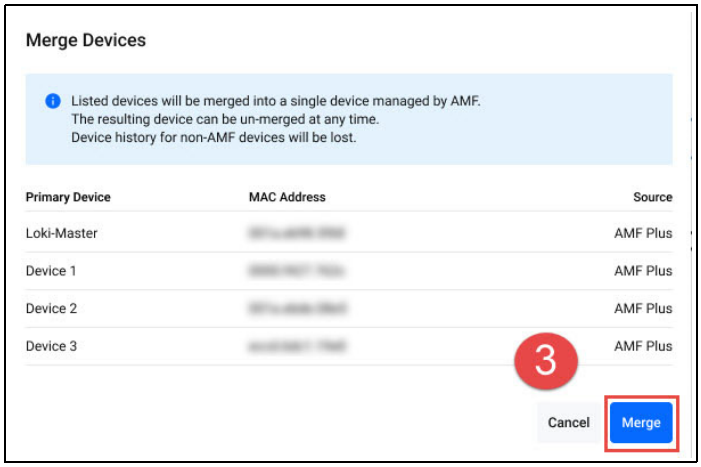
- manually merge duplicated nodes and have them appear as a single node
- un-merge nodes that have been manually merged
- see what nodes have been merged and where their information was obtained (source).

To merge devices:

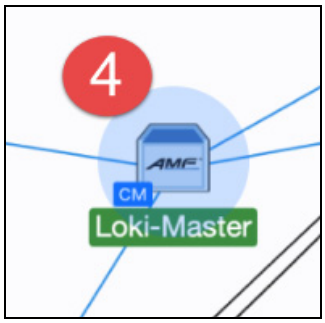
1. Go to the **Network Map**, and select the devices you want to merge.
2. Right click to see the context menu.



3. In the Merge Devices dialog, click Merge.



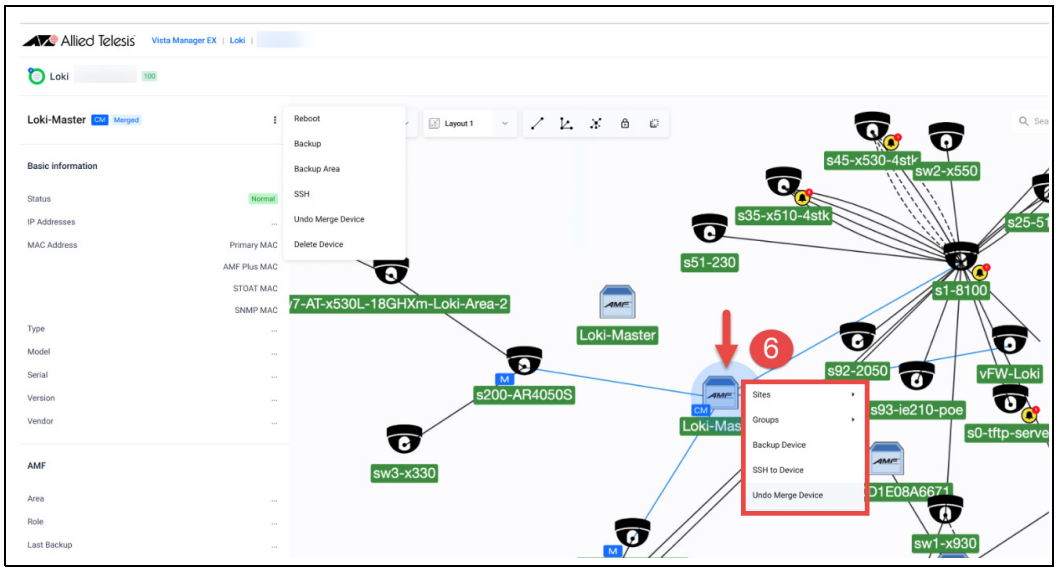
4. The nodes are merged into one. You will see more details in the left side panel.



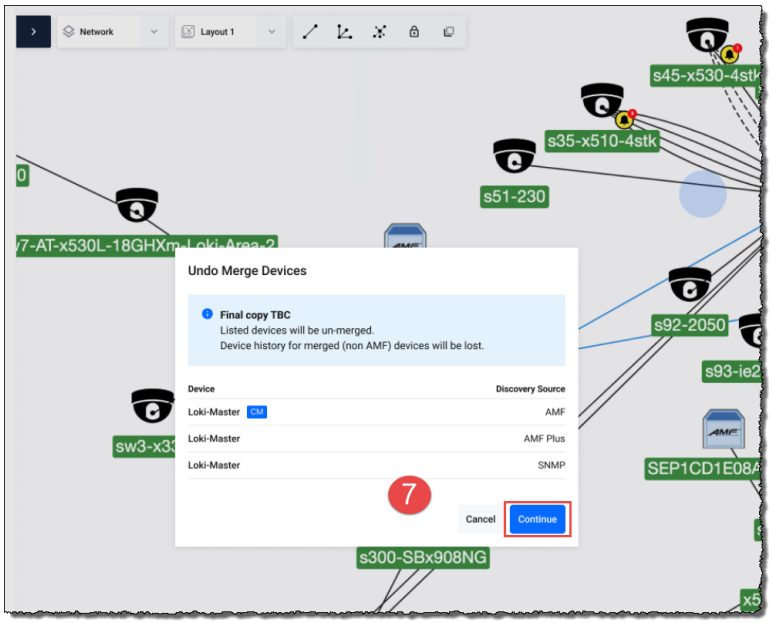
5. In **Asset Management** you can see which nodes are merged at a glance with the ‘Merged’ badge.

To un-merge devices:

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

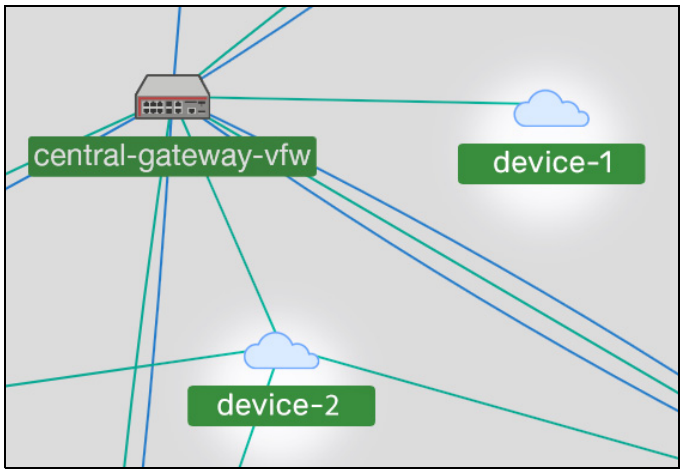


7. If you click **Continue**, then the nodes will be un-merged into their previous state.



Detecting non-AMF devices on the Network Map Layer

The network 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.



Enabling RADIUS on devices from the Network map

You can enable RADIUS on devices in order to configure them in the RADIUS Network Services section. You are able to enable RADIUS for devices on the network map.

Step 1. **Navigate to the Network Map**

Step 2. **Right click one device you want to check. A context menu will be displayed**

Step 3. **Select Enable RADIUS server**

Step 4. **Repeat step 2 and 3 until all the devices you want to check have been done**

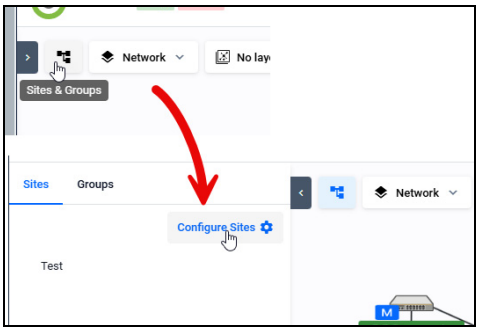
For more information on how to configure RADIUS in the Network Services section, see "Local RADIUS Server" on page 209.

Sites and Groups on the Network Map

From version 3.13.1 onwards, the network maps are made simpler. Vista Manager now offers the ability to focus on one site at a time, with improved flexibility to the Auto Sites Generator.

The existing **Auto Generate Sites** feature has been redesigned:

- The Network Hierarchy side panel has two tabs: **Sites** and **Groups**.
- The **Configure Sites** button is only available for Admin users. This menu includes three sub-menu items: Add Site, Auto Generate Sites, and Remove Auto Generated Sites.



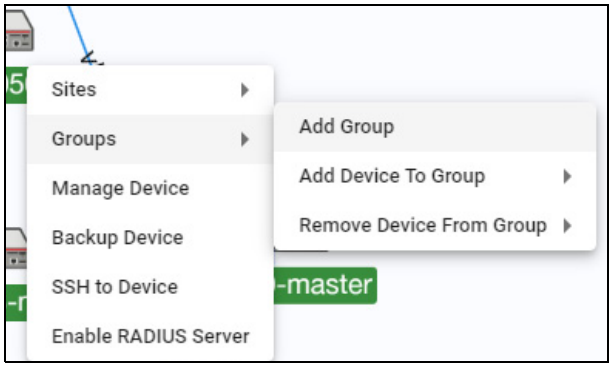
See the following sections for more information:

- "Groups" on page 65
- "Auto-Generating sites" on page 66
- "Manually creating a site" on page 69
- "Regex format separator support for auto-site generation" on page 71

Groups

Groups are collections of network devices chosen by a user. Groups may include devices from multiple sites and can easily be created on the Network Map. AMF areas are automatically converted into groups. When a new device is added to a group, assigned users automatically have access to the device. For more information on how to configure groups in the Asset Management menu, see "Creating Groups in the Asset Management menu" on page 168.

1. To create a group, click on the **Network Hierarchy** icon.
2. Then, click on the Groups tab in the newly opened sidebar.
3. Right click on the icon of a device you would like to add to a group to bring up the settings.
4. Mouse over the **Groups** tab, and select **Add Group**.

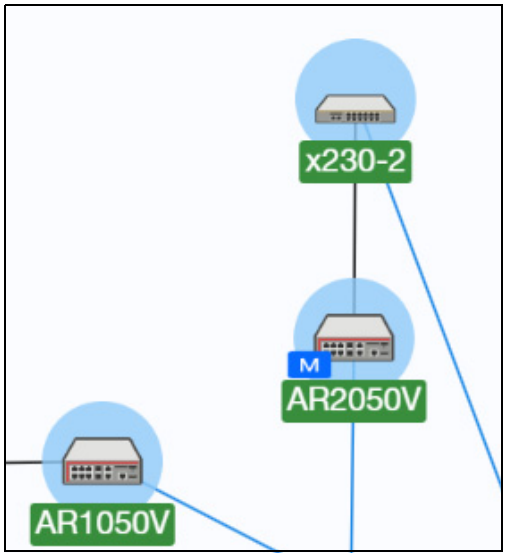


If you would like multiple devices to be grouped together, you can select multiple by either:

- holding **Ctrl** and clicking on multiple device icons before adding to the group, or

- clicking the multi-select button, and then selecting multiple devices

When Multiple devices are selected, they will appear with a blue circle around them, and appear in the **Selected Devices** left-hand menu.



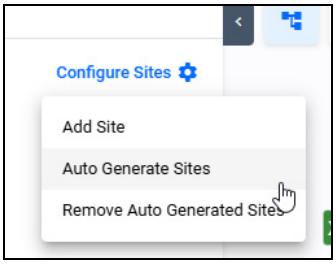
An **Add Group** window will appear, where you can name the group.

Auto-Generating sites

You can manually or automatically assign a device to a site. A site is a location, building, or floor where devices are stationed. Create sites on the network map by clicking the **Network Hierarchy** button and accessing the left-hand menu that appears.

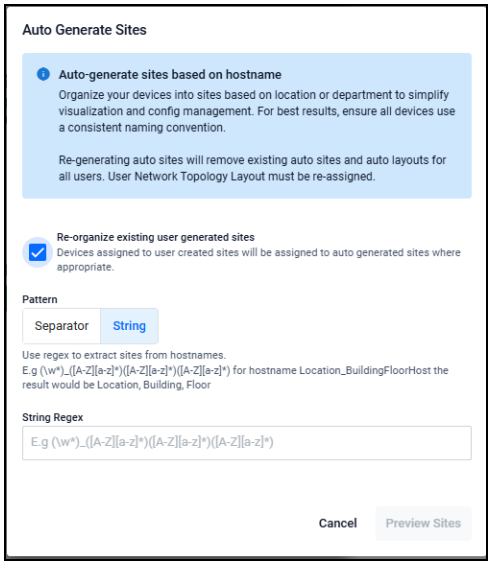
Vista Manager can create auto-generated sites. Note that auto-generated sites are read-only, and cannot be edited after they are generated.

1. To auto-generate a site setup, click **Auto Generate Sites** from the Sites & Groups tab on the Network Map.



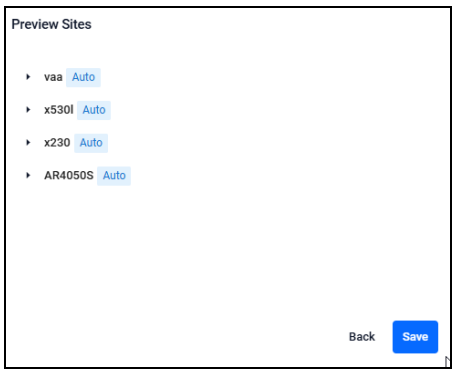
2. The Auto Generate Sites window will appear, where you can customize the regex pattern.

3. You can either enter a regex string, or choose to use an individual separator. For more information about regex strings, see "Regex format separator support for auto-site generation" on page 71.



- If a device fails to be auto-assigned, it will remain in its original manually created site if it existed prior.
- When a new device joins the network after you auto-generate a site, Vista Manager will try to classify the hostname with the existing sites hierarchy automatically. If no existing sites exist, Vista Manager will create new sites for it.
- If the hostname matches the parent site but not child sites, Vista Manger will create sites under the same parent site.

4. Click **Preview Sites** to get an example to confirm the generated setup.



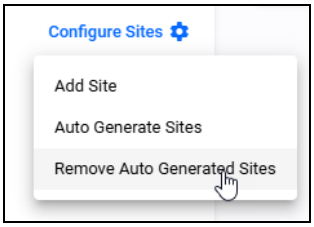
Note: Removing a site in the preview window only stops the automatic assignment. It does not remove the site from Vista Manager EX.

You can decide whether the existing manually created sites should be re-organized after the new auto-generated sites are confirmed.

- If you choose to re-organize the existing manually created sites, Vista Manager will try again to auto-assign a new generated site for all the managed devices. This includes the previously assigned devices.
- If you choose not to re-organize the existing manually created sites, the managed devices that do not belong to any manually created sites will attempt to auto-assign to the new auto-generated sites. The manually assigned devices will remain in the manually created sites.

Removing Auto Generated sites

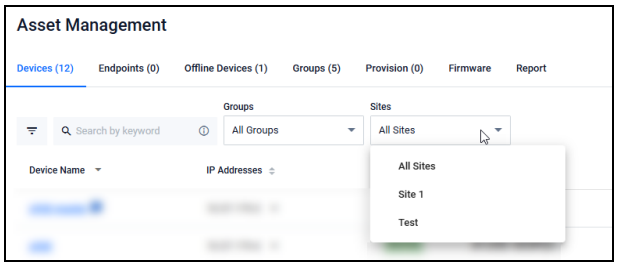
When you click the **Remove Auto Generated Sites** button, all Auto-generated sites and their corresponding layouts will be deleted. All devices assigned to Auto-generated sites will be reset.



Auto-generated sites also generate **Layouts** with the same names as the sites. This allows you to easily switch between site layouts. See "Changing the Network Map Layouts" on page 72 for more info about Layouts.

Filtering the sites in the Asset Management menu

You can filter by Sites in the **Asset Management** > **Devices** tab. This filter can be used in combination with the pre-existing Groups filter on the Devices tab.



Note: Guest and 802.1x nodes won't appear when filtering devices by a specific site even if they are connected to a device located in that site, because those devices do not explicitly belong to that site.

Take note of the following limitations:

- Automatic generation of sites supports up to 3 levels of network.
- Automatic generation of sites overwrites existing sites if they have the same name. Renaming or removing auto-generated sites stops the automatic assignment.
- When the sites are overwritten, the devices will be 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.

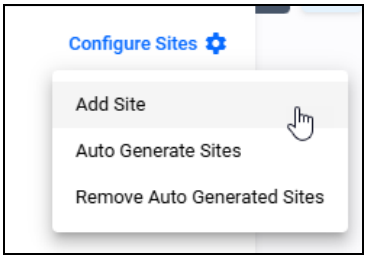
When a new device join a network after sites have been automatically generated, Vista Manager will try to classify the device's hostname using the existing hierarchy automatically. If no sites exist then Vista Manager will create a new site for it.

You can configure access to read/write permissions for specific sites for each user. For information about configuring permissions for sites see "Sites and Groups Permissions" on page 308.

Manually creating a site

To manually create a new site yourself, click on the **Network Hierarchy** icon to bring up the side-menu.

You can manually create sites via the Sites & Groups side panel by clicking the **Configure Sites** button and selecting the **Add Site** button.



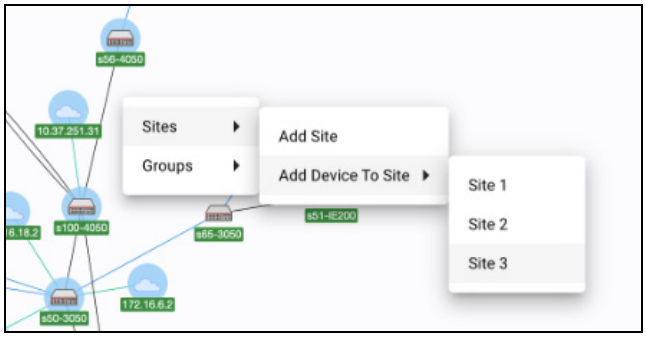
Similarly to automatically generated sites, once a site is created, an automatically generated layout with the same name will be created for each user who has access to this site.

This change applies to all layouts, including Auto-sites layouts, user-created layouts, and the entire network.

- For non-admin users, the layouts they are given will depend on which auto-generated sites they are given permission for. Any auto-generated site that the user has permission for will have a corresponding layout for that user.
- Each user has their own layouts based on the auto-generated sites. Layouts are not shared between users, so each user can make their own changes to a layout and it will not affect the layouts for other users.
- Likewise, if permission is removed from some auto-generated sites, the layouts for those sites will be removed. If a user saved their own copy of an auto-generated layout, that copy will not be affected.
- Layouts that were originally created from auto-generated sites will appear in a nested format.
- After running the Auto Site Generator again, the selected or default layout of all users may change.
- A non-admin user will only be able to see dot1x supplicants if the user has permission for a group and the group contains the dot1x supplicant.
- When sites are collapsed, a blue circle icon next to the site shows how many devices are in this collapsed site.

When migrating from an older release of Vista Manager any device that is a 802.1x supplicant and belongs to a site will be removed from the site during the database migration. It is very unlikely that a dot1x supplicant will have been explicitly added to a site. The device will now implicitly belong to whatever site the device is attached to.

To add a device to an existing site, right click on the device you would like to add to a site, then mouse over the sites tab. Mouse over **Add Device to Site**, and then select a site to add the device to.



You can also create a site from the Network Map by **right-clicking on device(s)** and selecting **Add Device(s) to New Site**. Note that a device cannot be assigned to multiple sites.

Regex format separator support for auto-site generation

You can select Regex as a **sites separator** for auto site generation. This feature allows you to define a custom separator pattern inside square brackets, where it will be read, and split into sites, child sites, and devices based on hostnames.

Vista Manager reads this data in a ***Site > Child Site > Device*** order.

For example, you can use an underscore inside square brackets as a Regex pattern for the following output:

Hostname format: CHCH_IT01SW01
Regex pattern: [_]

Results:

- One site named: CHCH
- One Device named: IT01SW01

Another example is:

Hostname format: CHCH_IT01-SW.01
Regex pattern: [_-.]

Results:

- One site named: CHCH,
- One child site named: IT01
- One child site nested in the IT01 site named: SW
- One device named: 01

Click Save after importing the regex string to store it.

If a site called Office has a child site named Building1, and a new device classified as “Office, Building2” joins, then Vista Manager will create a new child site for Building2 with the parent as Office.

Note: If the hostname fits any of the following examples it will be seen as an invalid hostname. Automatic site generation will not be performed on the below hostnames.

- starts with a separator (such as '_CHCH_Building'),
- ends with a separator (such as 'CHCH_Building_'),
- or has consecutive separators (such as 'CHCH__Building')

Regex Hostname matcher support for auto site generation

You can select Regex as a **site hostname matcher** for auto site generation as well. This feature allows you to define a custom regex string pattern to extract and create sites based on hostnames.

The following examples show example patterns:

Hostname format: CHCH_IT01SW01
Regex pattern: ([A-Za-z]+)_(\w{2})(\d{2})

Results:

- One site named: CHCH
- One child site named: IT01

Hostname format: aklvaa01, aklswi02
Regex pattern: (\w{3})(\w{3})(\d{2})

Results:

- One site named: akl
- One child site named: vaa
- One device named: 01
- A second child site named: swi
- A second device in that site named: 02

The input regex string will be stored after clicking **Save**.

Changing the Network Map Layouts

On the Network Map, **double click on a site** to switch to the corresponding Layout.

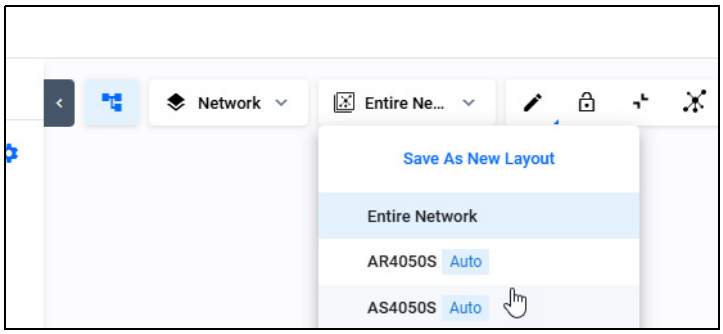
Click the top left button group of the integrated map to collapse all visible parent sites. Note that child sites will not be collapsed.

When viewing layouts for auto-generated sites, sites (including child sites) are expanded by default.

When expanding or collapsing sites, they will be saved like this automatically.

Note: The default layout for all users is the Entire Network. The Entire Network layout cannot be deleted. The Entire Network layout is read-only; it is not possible for the user to delete this layout.

Layouts of auto-generated sites and manually created sites have an **Auto** badge displayed next to their names in the layouts dropdown menu. Layouts are displayed in alphabetical order.



When you make changes to the Network Map, they will be automatically saved, including:

- Changing the position of devices/sites,
- Expanding/collapsing sites on the map,
- Changing the background image,
- and changing the zoom level of the map.

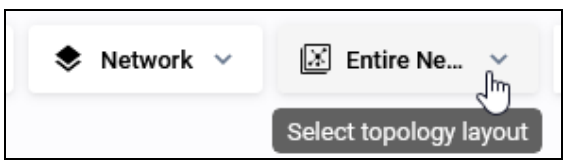
In the **User Management** menu, you can set default layouts to your admin user account, as well as other users.

- When an Admin user edits their details, the user can see all accessible layouts in the Network Topology Layout drop-down list. This includes the entire network, all Auto-Generated Layouts, all manually-created site layouts, and all user-created layouts.
- When an Admin user is editing another user's details or creating a new user, the Network Topology Layout drop-down list only includes layouts that are allowed to be shared between users.

Adding a new layout

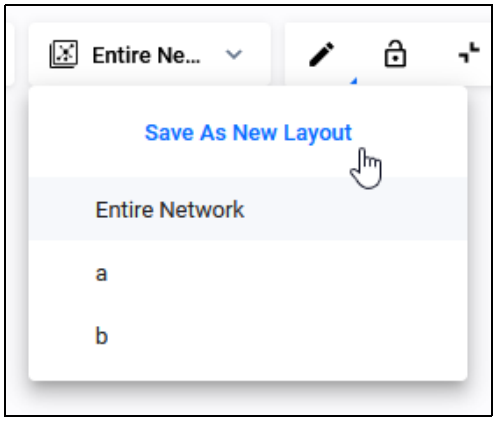
You can create new custom layouts by clicking and dragging devices around. You can save them as a new layout from this menu by clicking the 'Save as new layout' text.

1. Click on the **Select topology layout drop-down**.
   - If this is your first layout, the default will display as **Entire Network.**
   - Otherwise, it will be the name of the currently selected layout.

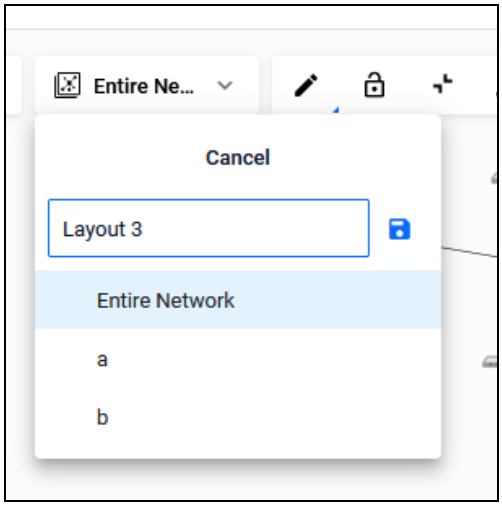


2. Click **Save as New Layout.**

   - You can duplicate an existing layout by saving the current layout with a new name.



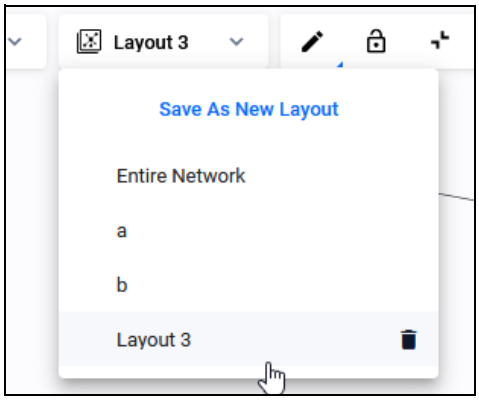
3. Enter a name for your new layout and click on the **save icon** to save the layout.



4. The new layout will become the currently selected layout. You can make any changes to the zoom level or layout of devices on the map.

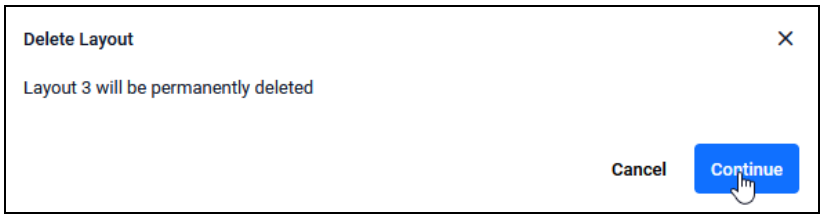
   - Changes will be saved to the new layout automatically.

5. Click the trash icon next to the layout you would like to delete to delete the layout.



   - Users can only delete map layouts that they created.
   - You cannot delete the Entire Network layout.

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

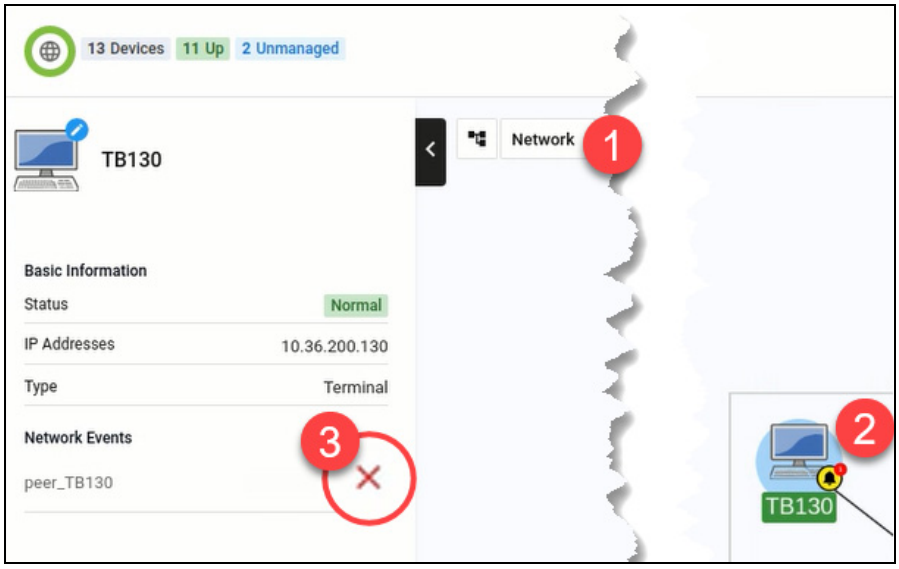


Note: Hidden devices are specific to the layout. You can hide devices on a per-layout basis, and they will be hidden for any user using that layout. For information on hiding devices see "Show/Hide devices" on page 103.

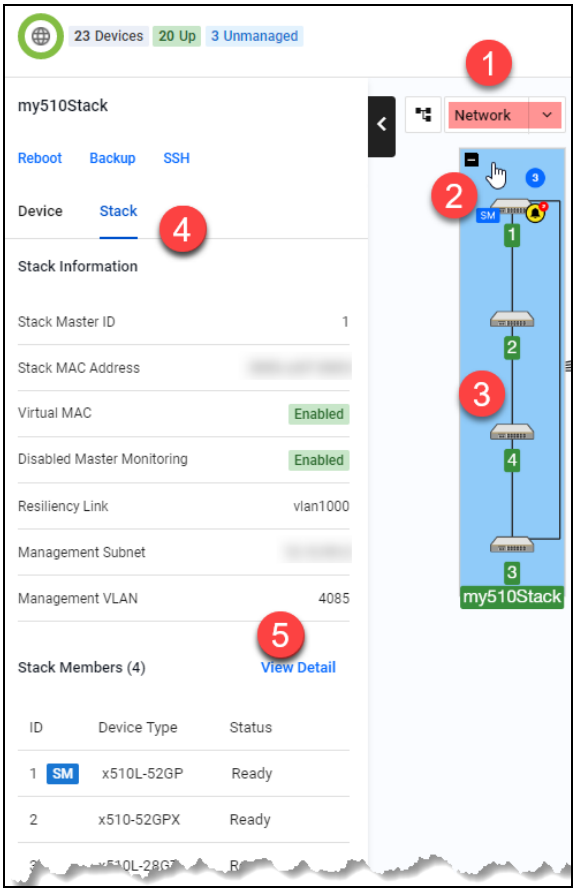
Syslog Rule alarms

On the Network map a bell icon will appear next to a device that has a syslog event that matches 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.

For information on setting up syslog rules and information on events, see "Events" on page 125.

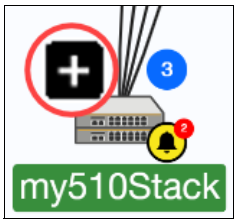


View Details of Stacked Devices



You can click on the **View Detail (5)** section of the stack member side-menu to monitor the state of stacked devices in your network.

Click the **+ icon by your stack** 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.



The Stack tab displays some basic stack-wide information such as:

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

Each stack member has an icon showing its stack member ID. Click on the stack on the map (blue highlighted area) to see its information. When a stack is expanded:

- All stack members and associated stacking links will be displayed.
- The stack master has an ‘SM’ badge indicating that it is the stack master.
- Click on each link to see which device type and interface is on each end of the link.

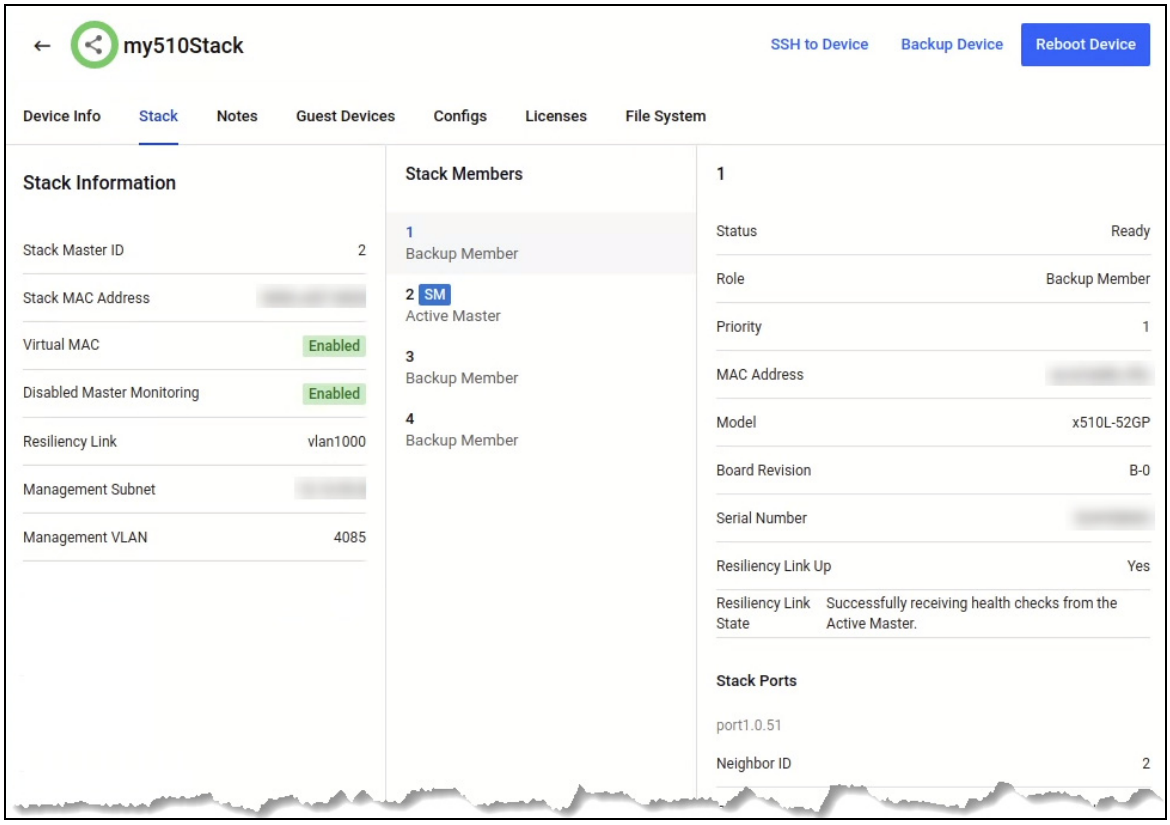
When a stack master leaves the stack, the stack master badge will update to show next to the new stack master.

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.

Note: If a stack member goes down, its position will move to the bottom of the stack to indicate its current down status. The hostname/member ID will stay green and not change to red. Individual stack members cannot be moved.

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



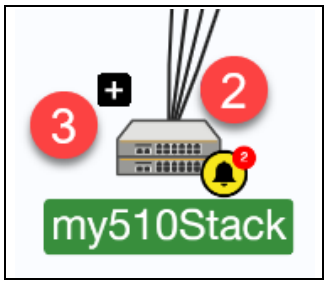
- **Stack Information:** Stack Master ID, stack MAC Address, virtual MAC, disabled master monitoring, resiliency link, management subnet, management VLAN
- **Stack Members:** Stack ID, status, role, priority, MAC address, product type, revision, serial number, resiliency links, state, stack ports

For more information about the device details page, see "Accessing device details" on page 148.

Active Fiber Monitoring with stacked devices

With enhanced information display possible for stacked devices, support has been added to display Active Fiber Monitoring Plus (AFM Plus) links. You can see links between members and fiber tamper alarms (red bell icons) when a link has been tampered with.

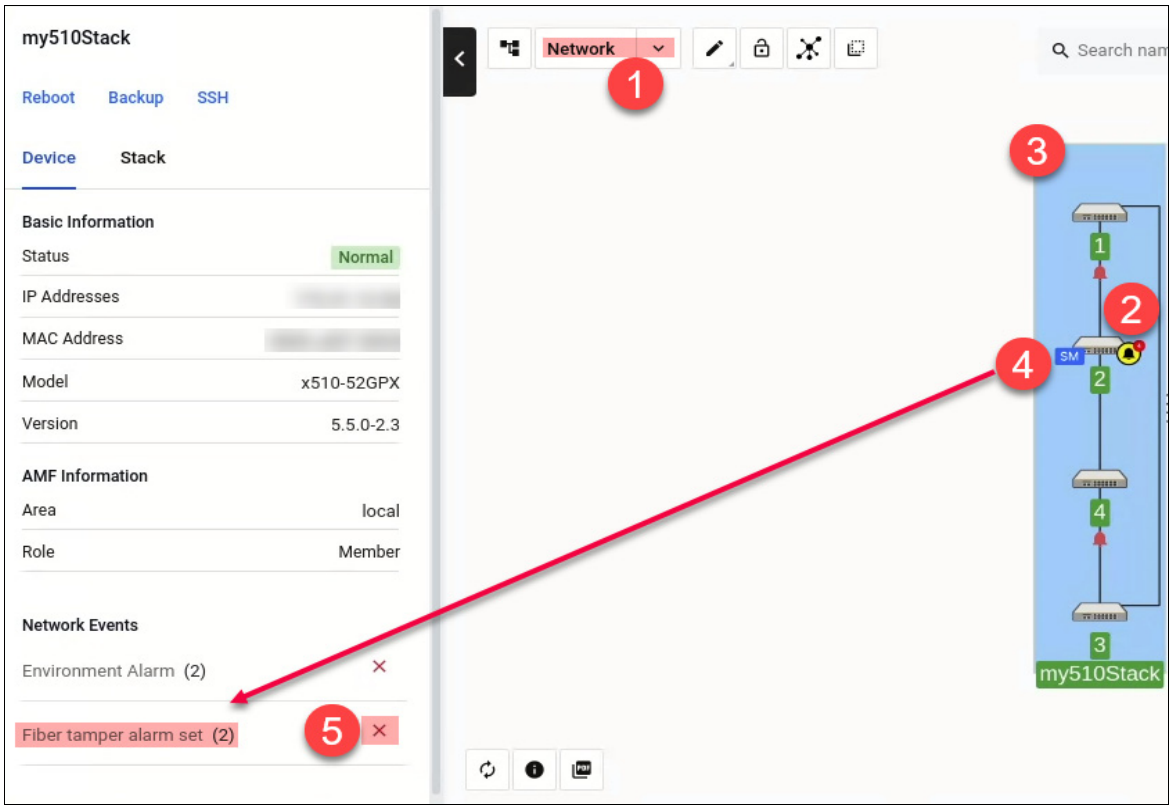
As an administrator, you can use this information to check on the physical links, dismiss the fiber tamper alarms and/or change AFM settings on specific links.



1.Identify a stack with an event bell icon.
This means there has been an event on the stack, for example, tampered links.

2.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.

3. 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.



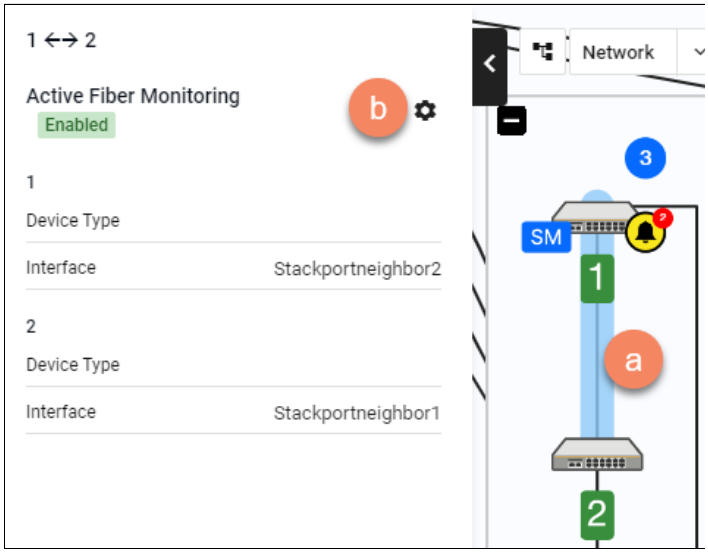
Note: Fiber tamper alarms will remain until you have dismissed them. This removes the red bell icon and reduces the event bell count on the device stack

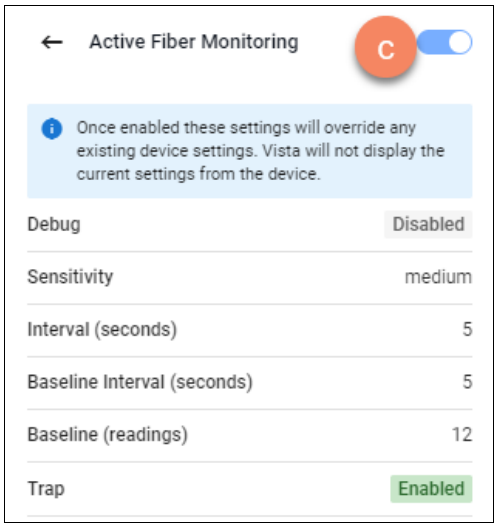
Enabling Active Fiber Monitoring on a stack

To change settings for AFM on a stack, expand the stack.

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

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





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.

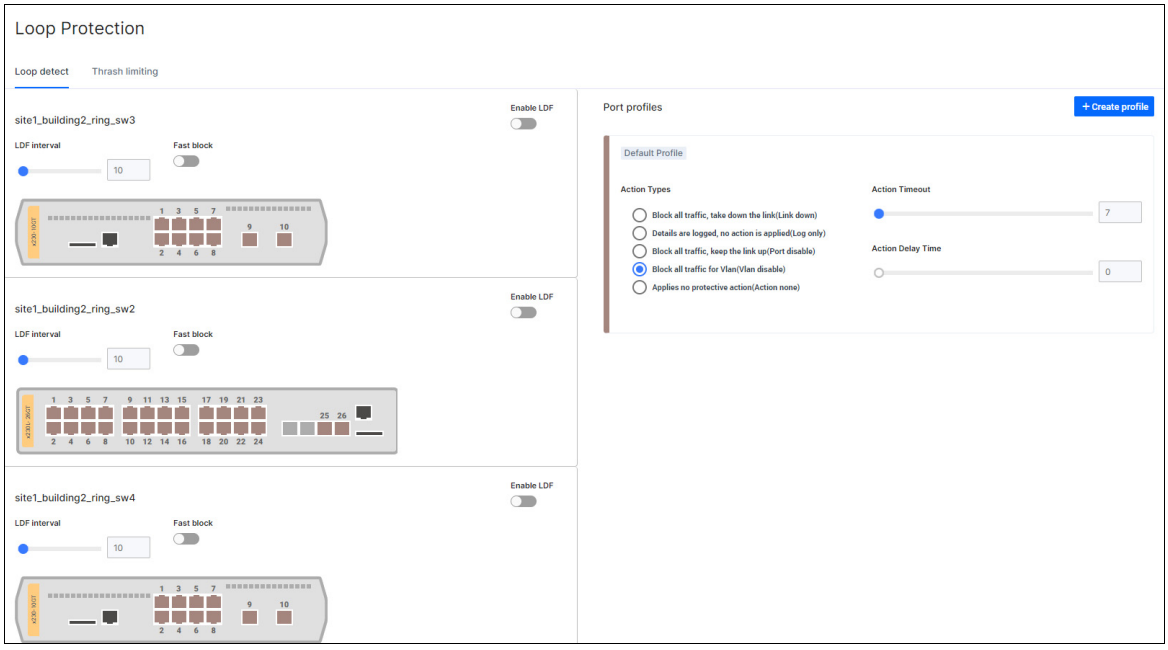
Dismissing Fiber tamper alarms

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**.

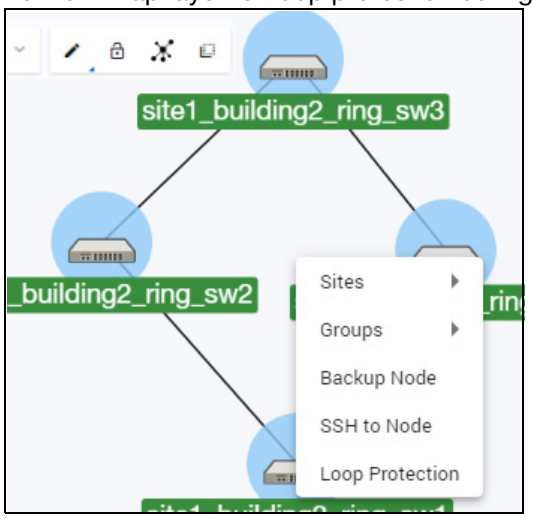
Loop protection

The loop protection feature helps prevent loops in your network. Network loops are also known as Layer 2 switching loops or bridge loops because they occur at Layer 2. Put simply, a loop occurs when a network is cabled in a way that allows traffic to get to a destination by multiple paths.



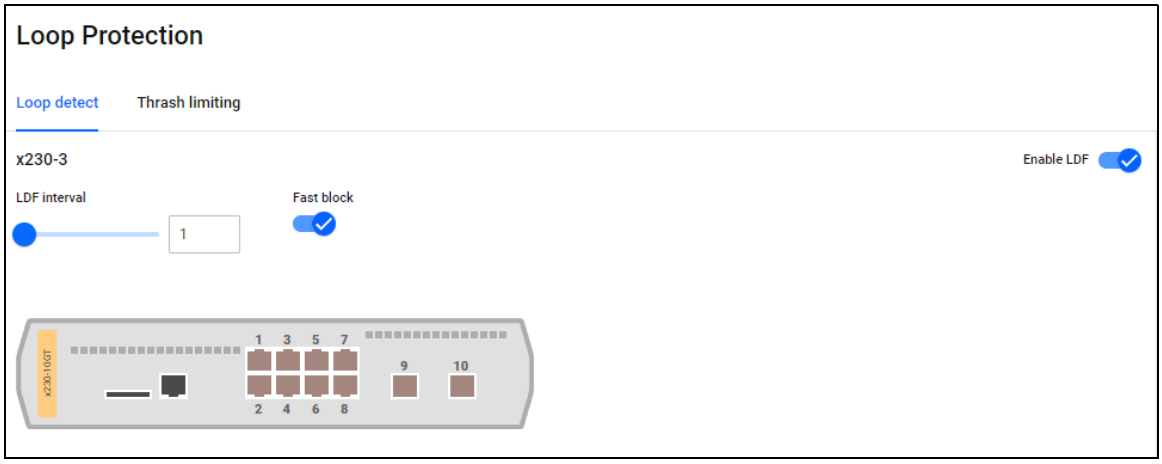
The loop protection feature helps you manage loop protection settings of your AlliedWare Plus devices in the Vista Manager GUI. You can use Vista Manager to manage both the loop detection and thrash limiting of your network. This feature is supported when devices are running firmware version AlliedWare Plus v5.5.0-0.1 or later.

Select a device, or select multiple devices with the multi-select button, then right click and select **Loop Protection** to open the menu. You can select one or multiple (up to 10) devices from the network map layer for loop protection configuration.

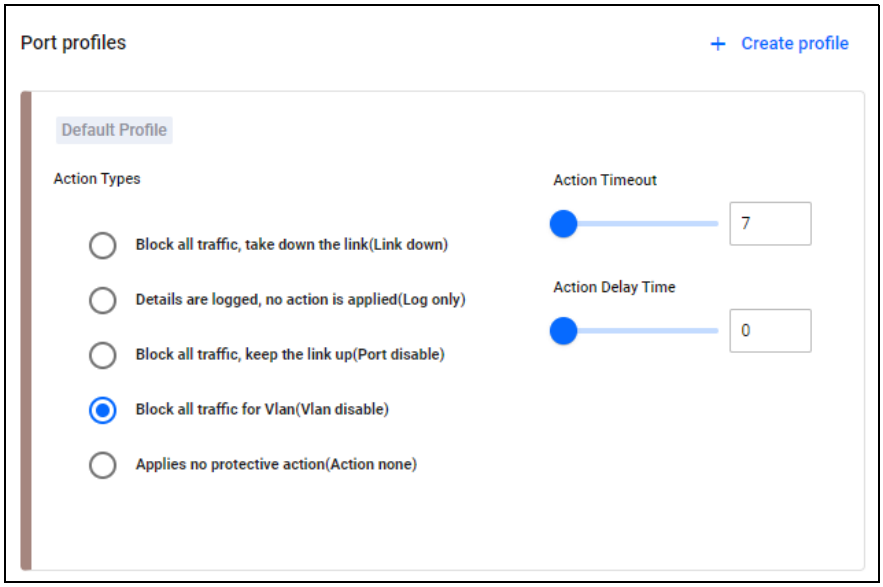


Loop Detection

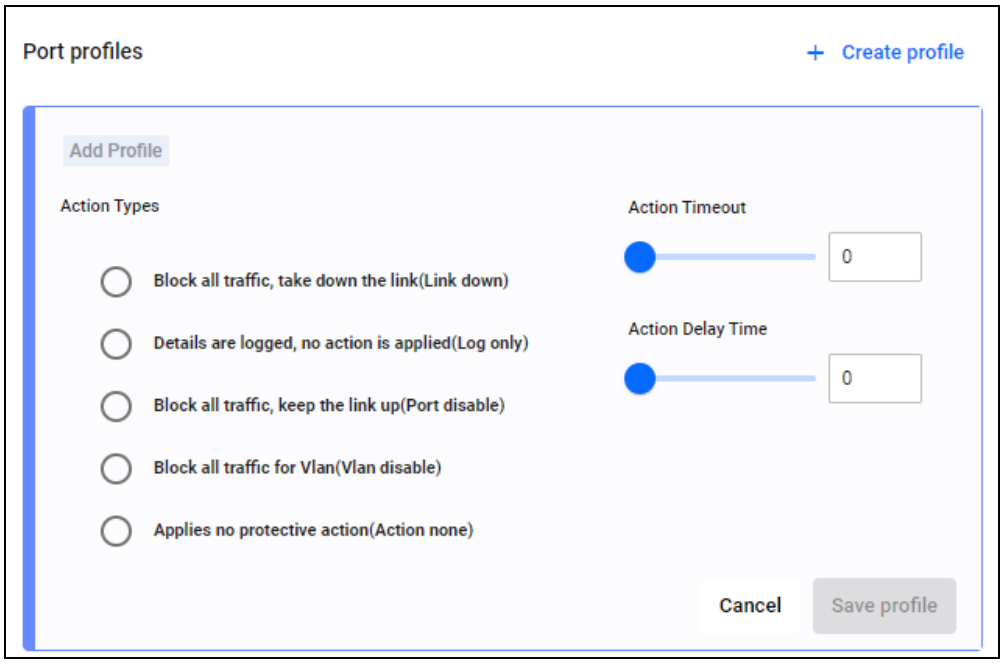
When you land on the Loop Protection page, the **Loop detect** tab will be selected. On the **Loop detect** tab you can configure loop detection for the selected devices. The **Enable LDF** button lets you enable or disable loop-detect frames (LDF) for each device. The LDF interval slider lets you set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



For loop detection port profiles, you can choose the action type, the action timeout, and the action delay time for the profile. 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.

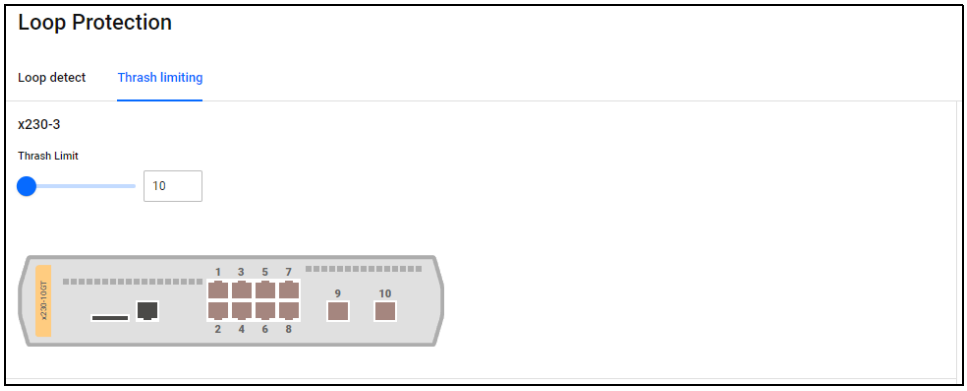


You can select multiple ports across one or multiple devices, and apply the profile to all of them at the same time. Click on Save profile to save the changes.

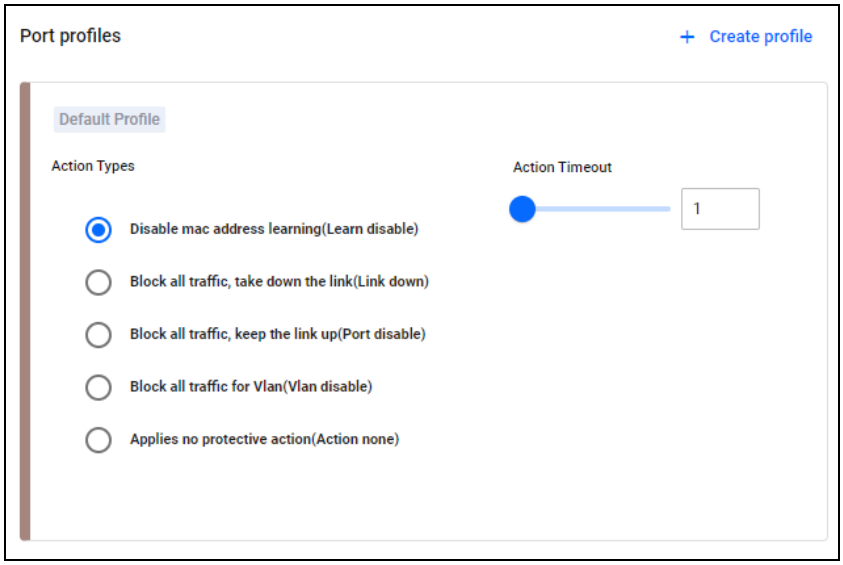
Thrash Limiting

Thrash limiting, also known as rapid MAC movement, detects the rapid changes in MAC address table entries that a loop causes, and takes action to deal with the loop. It is highly user-configurable—from the rate that indicates a loop to the action for the switch to take.

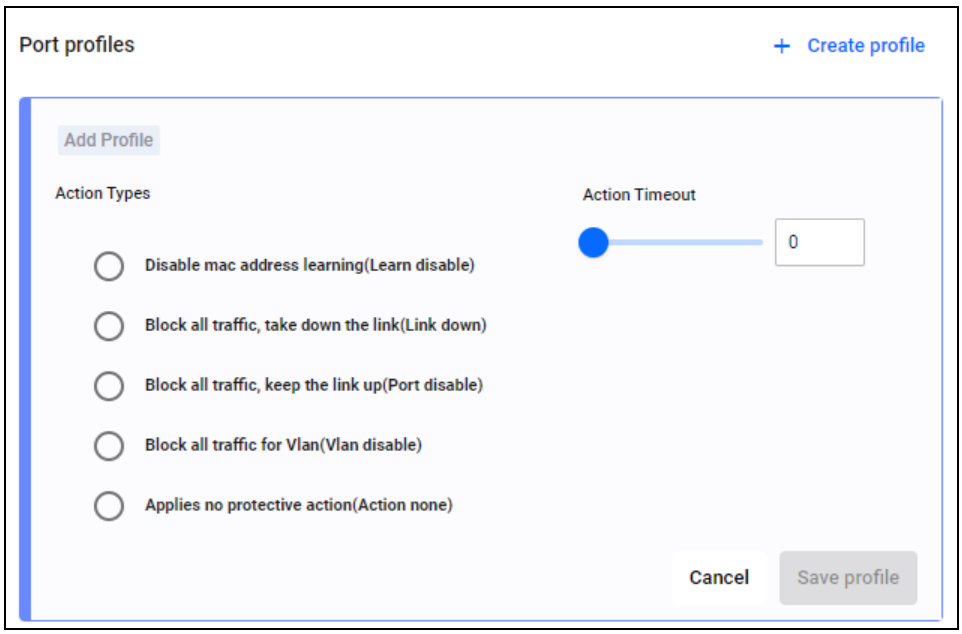
On the Thrash Limiting tab, you can configure thrash limiting for the selected devices. The Thrash Limit slider lets you set the thrash limit.



For thrash limiting port profiles, you can choose the action type and action timeout. You can then assign the profile to device ports. By default, the settings of the Default Profile apply to all ports on the device.



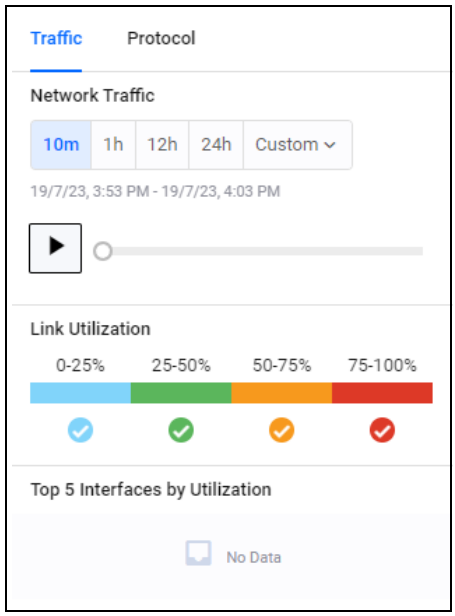
To create a new profile, click on the **+ Create profile** button.



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.

Traffic map Layer

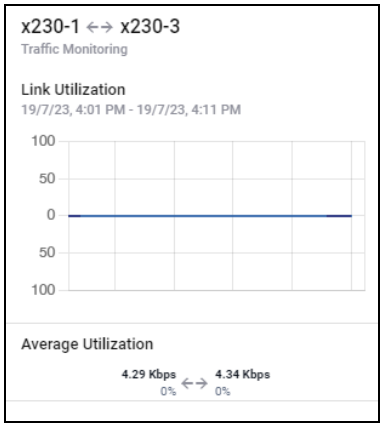
When selecting the Traffic map layer, the map switches modes and displays the traffic menu on the left-hand side. The links between devices will change to colored arrows based on the link utilization key, that indicate the utilization percentage of that link.



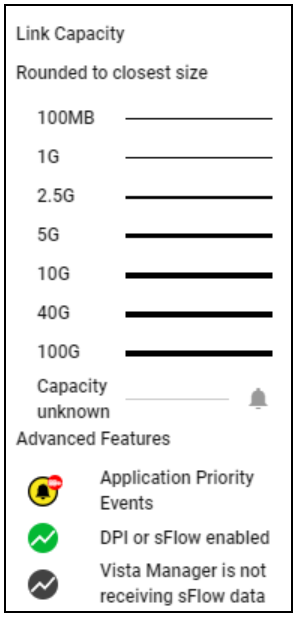
As a user, you are:

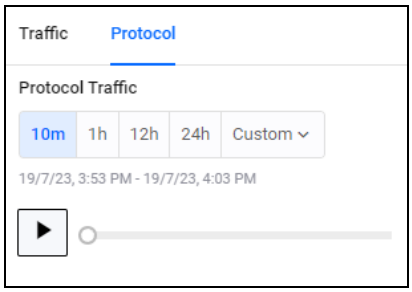
- able to create a rule which generates an action on a link that no longer has high utilization
- notified when any links have a high utilization (consistently oversubscribed)
- able to create a rule which generates an action on any link having high utilization over a period of time (consistently oversubscribed)
- able to 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

Link utilization is color coded so you can view which areas of your network carry different levels of traffic. If you click on a device, you can monitor the traffic going to and from that device. If you click on a link on the map, then you can monitor the traffic between the two devices.



The ‘i’ icon now shows the **Link Capacity** when clicked. This shows in the links between devices, as well as the meaning for icons that may appear beside devices.



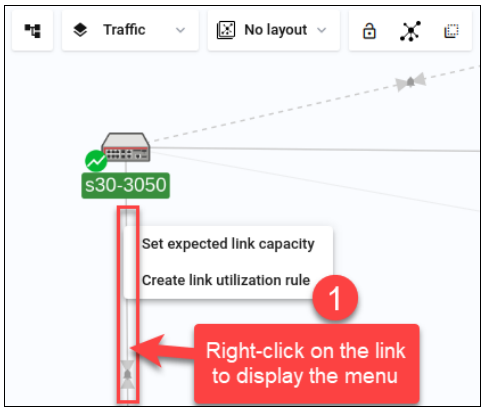


The protocol tab displays the protocol traffic. You can select a time or a custom date to view network traffic. You can monitor any link by clicking, to show bi-directional traffic on all aggregated ports over the last 24 hours. You can replay network traffic from up to 24 hours by clicking the play button on the left-hand menu.

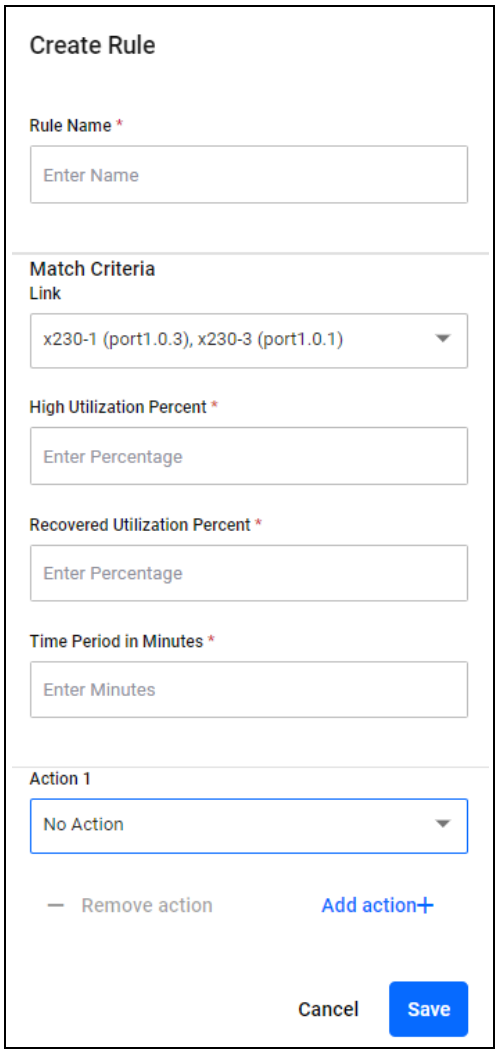
Custom link monitoring

You can view custom link information from the Traffic map layer. However, in order to view link utilization information, you must first configure the interfaces through the Edit map layer. For information about how to create a custom link see "Edit map layer" on page 102.

Creating link utilization rules



If you would like to create a link utilization rule, you can do so by right-clicking on the link you want to monitor, then selecting **Create link utilization rule**.



On the left, the **Create Rule** panel will appear. Here you can create a rule to monitor link utilization on the Traffic map and see related information.

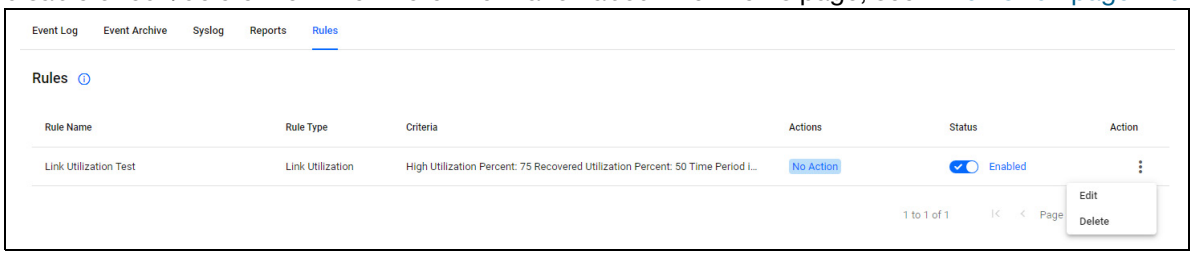
Click on the **Save** button to save your rule.

Click on the tunnel link to view its link utilization information. The side panel pops out showing the link utilization and its related information.

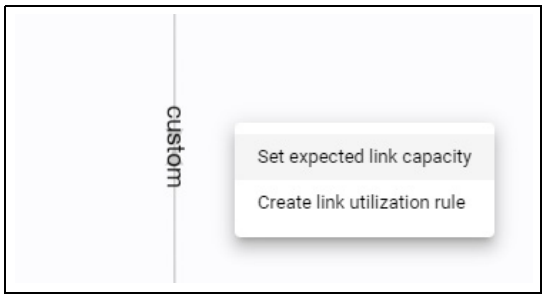
Note: There are some limitations to take note of:

- 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.

You can see all created rules on the **Events** page. Select Rules to see all created rules and enable/disable or edit/delete them. For more information about the Events page, see "Events" on page 125.

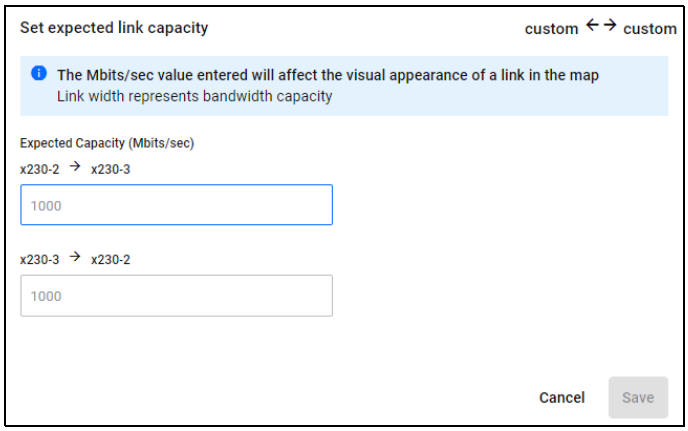


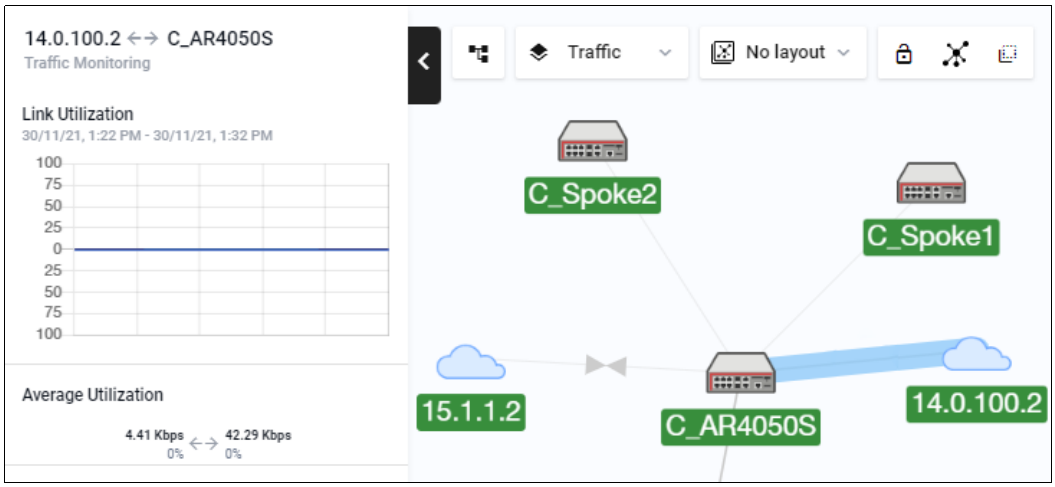
Set expected link capacity



You can set the expected capacity for a custom link you are monitoring on the Traffic map layer. To set the capacity, right-click on a custom link and click **Set expected link capacity**.

This will open the **Set expected link capacity** dialogue box, where you can input the expected capacity for your custom link.





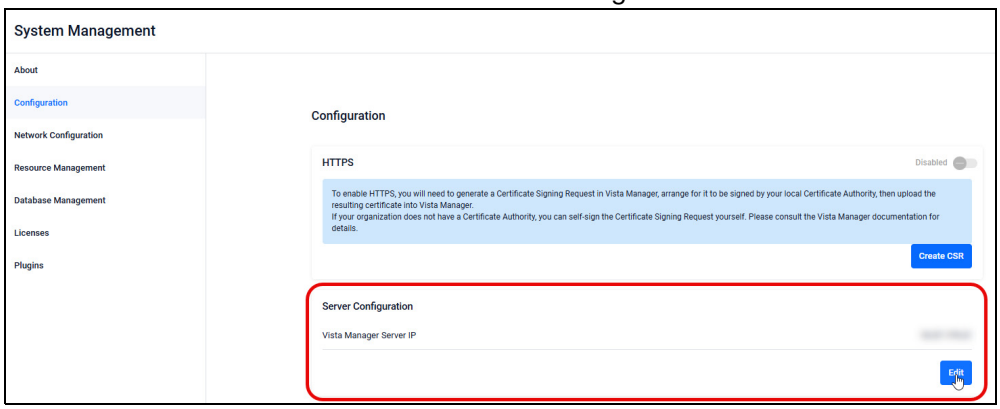
Advanced Traffic Monitoring with sFlow

You can monitor network traffic using Vista Manager's sFlow (sampled flow) feature on the Traffic map layer. After configuring sFlow on your network devices, you can use the Advanced Traffic Monitoring section to view information about network traffic, protocols, and applications.When sFlow is active, a green icon will appear next to the device you have decided to monitor.

With sFlow configured, the **Advanced Traffic Monitoring** section will appear at the bottom of the sidebar when you select a device. When you first click on a device without sFlow configured, there will be no data.

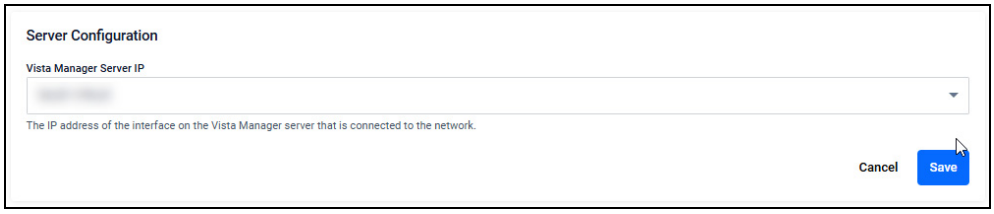
From version 3.13.1 onwards, support has been added to change the IP Address of the sFlow server.

This IP is used by devices with sFlow enabled for its Collector IP, and for SMTP when sending license expiration email alerts. Note that If this Server IP is changed, you will need to re-configure sFlow on the AlliedWare Plus devices that are configured to use it.



To change the IP Address for sFlow, go to **System Management** > **Configuration**.

Under **Server Configuration**, click **Edit** to change the Vista Manager IP address. Vista Manager will display a list of IPv4 addresses that you can select from.



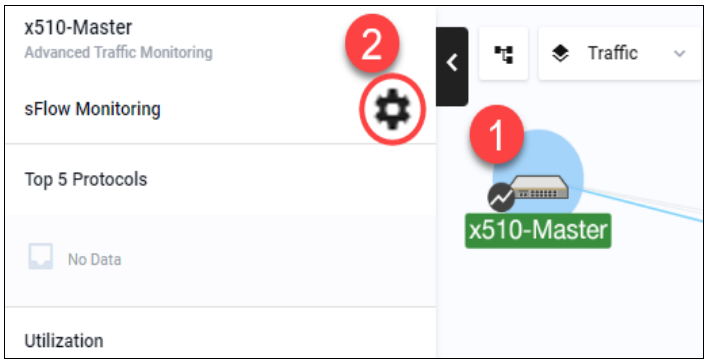
The default is set to the first public IPv4 address in the list.

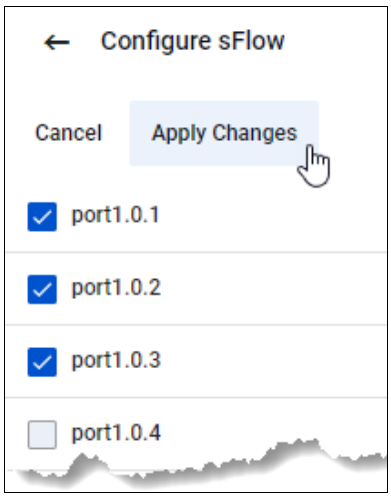
Configuring devices for sFlow using Vista Manager requires the device to be running Alliedware Plus version 5.4.8-2 or later. Devices running older releases are still compatible with this feature; however, the sFlow configuration will have to be done manually through the CLI. To see how to configure a device for sFlow using the CLI, see "Configuring sFlow through the CLI" on page 93.

To configure a device with sFlow:

Step 1. **Select the device from your map to configure**

Step 2. **Click on the settings cogwheel on the newly opened information panel to configure it.**





The side panel will show a list of the ports on the device. Select a port via the check-box to enable or disable sFlow on the port.

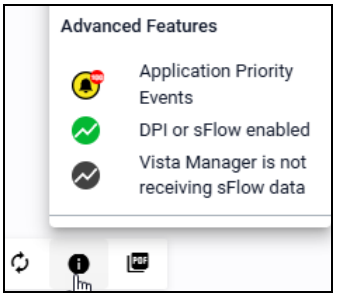
Click **Apply Changes** to save.

The side panel will then show monitoring output from the selected switch, including the protocols,

If you would like to change the server IP for sFlow and SMTP, see "Advanced Traffic Monitoring with sFlow" on page 89.

Enabling DPI for advanced traffic monitoring

Routers do not support sFlow by themselves. However, by enabling DPI (deep packet inspection) on a router, you can carry out features of traffic monitoring. DPI Enabled devices have a green icon next to them.



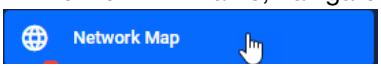
DPI traffic statistics

From version 3.13.1 onwards, you can select multiple devices when viewing DPI traffic.

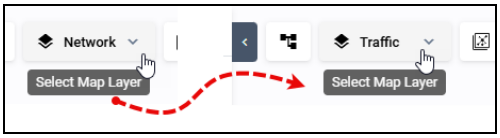
This means that you can click on multiple DPI-enabled devices to display an aggregated view of traffic statistics across the selected devices.

Statistics and visuals of applications from the selected devices are shown on the left side-panel. DPI Enabled devices have a green icon next to them.

1. To view DPI traffic, navigate to the **Network Map**.

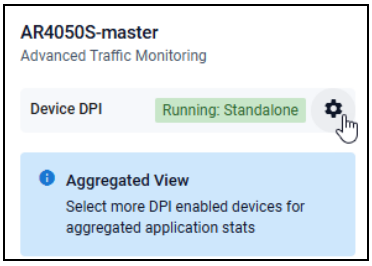


2. Click the dropdown to turn the Network Map into the Traffic Map.

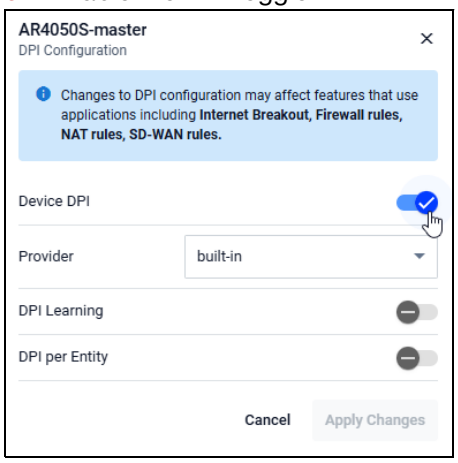


3. To enable DPI on a device, click on the device to bring up its information on the side panel.

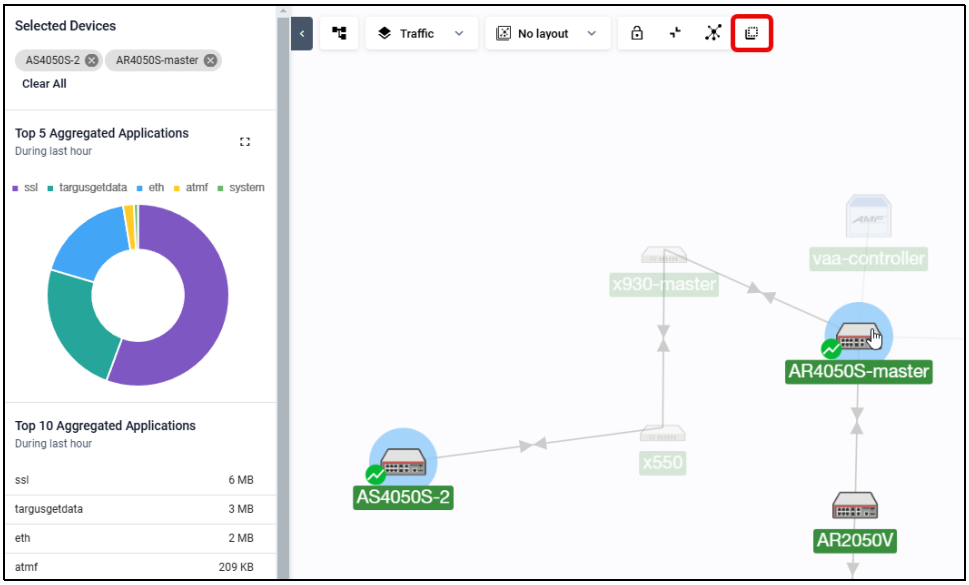
4. Click the **Cog** icon to open the DPI settings.



5. Enable the DPI toggle.



6. Click **Apply Changes**.



Once enabled, the DPI application information and DPI icon will display on the Network map.

To select multiple devices, **Ctrl + Click** or use the **Multi Select Devices button** to select multiple devices to include in them in the chart on the left panel.

The side panel will show the protocols being used by the router in a chart, along with other charts. You can click on the diagrams in the side panel to open the associated chart widget.

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

Configuring sFlow through the CLI

Configuring devices for sFlow using Vista Manager requires the device to be running Alliedware Plus. Devices running releases older than version 5.4.8-2 are still compatible with sFlow; 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. You can find the IP address by 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
```

VLAN map layer

The VLAN map layer shows all VLANs in the network on the left side-bar, which are color coded by a strip on the left side of the name. When a VLAN on the sidebar is clicked, devices that are part of that VLAN are highlighted on the map and displayed with a background that corresponds to the color on the list.

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 and delete ports to VLANs
- set VLAN ports as tagged or untagged

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

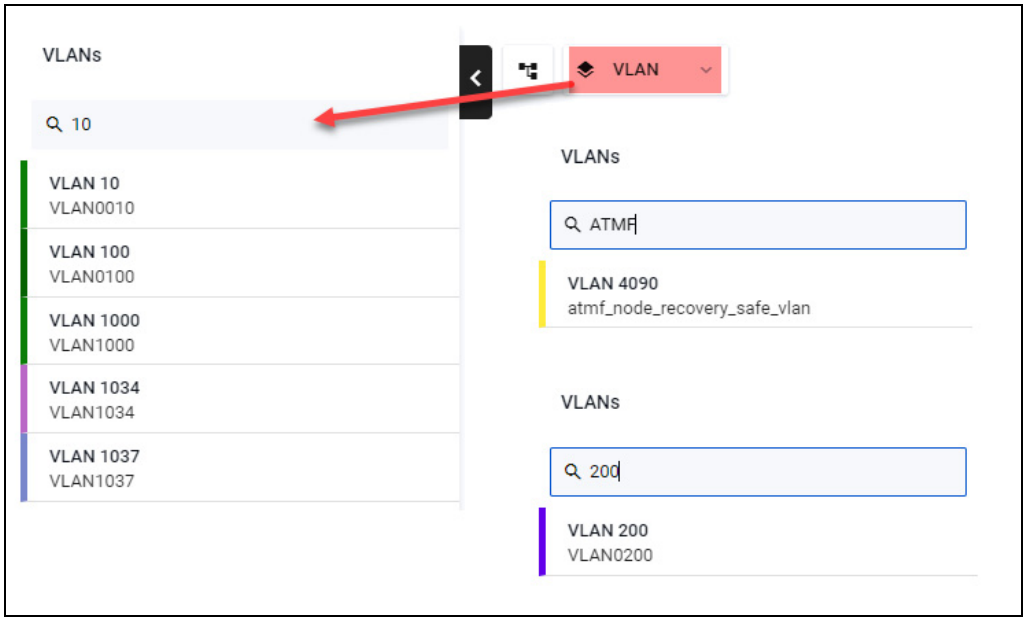
VLAN search

When searching by VLAN ID, the filter performs an exact match to narrow down search results and ensure higher accuracy.

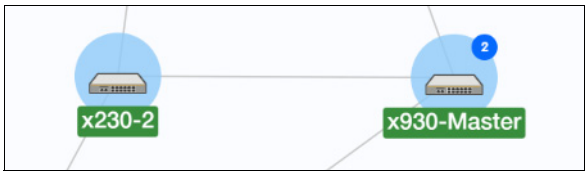
When searching for VLAN names, the filter is not case-sensitive and performs partial matching only.

For example, in the screenshot below, 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 typed. Other VLANs containing 10 in their names will appear after, such as VLAN 100, 1000, 1034, etc.

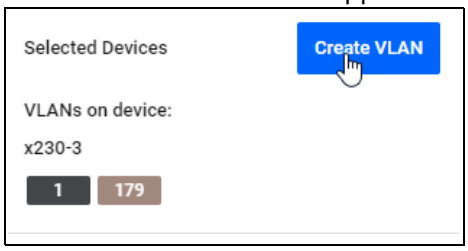


Create VLAN



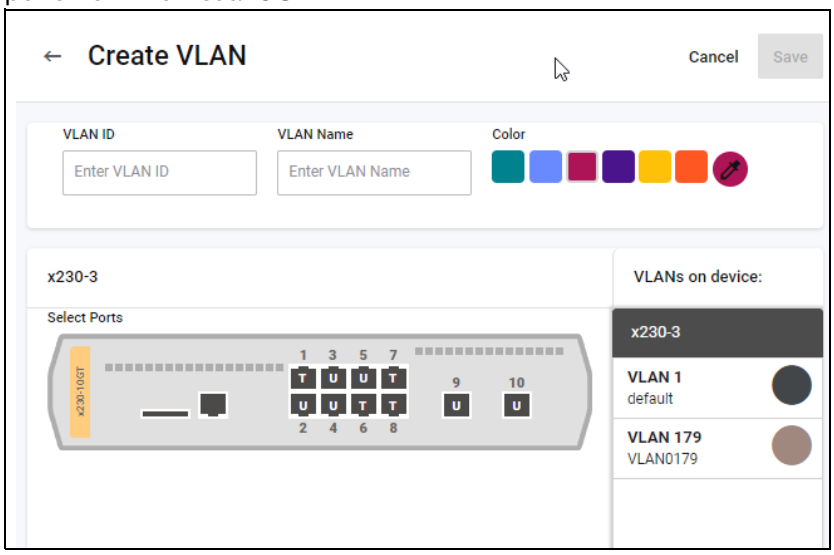
To create a VLAN, select the device or devices you want to add the VLAN to. Click to select one device, or click the multi-select button to select more devices.

A **Create VLAN** button will appear on the left side menu, which you can use to create a new VLAN.



Clicking **Create VLAN** brings up the Create VLAN page.

You can customize the color, ID and name of the VLAN which appears on the map, as well as select ports from the visual GUI.



Once a VLAN is created, it will display on the VLAN list back on the map.

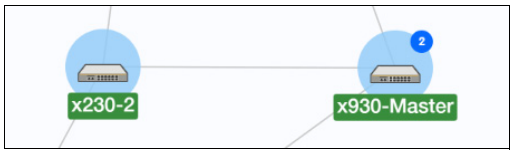
Creating a Native VLAN configuration

When a port has a native VLAN, any packets received on the switchport without a VLAN tag are placed into that native VLAN. Packets then leaving a switchport on the native VLAN will not be tagged. You can assign different native VLANs to different switchports on a device. Note that only one native VLAN can exist per switchport.

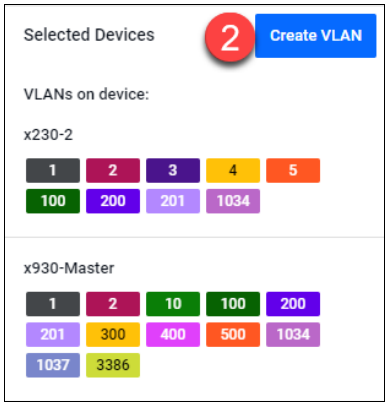
Note: Native VLANs only apply to switchports in trunk mode.

The following procedure first uses the VLAN map to put the switchport into trunk mode, then sets the correct native VLAN:

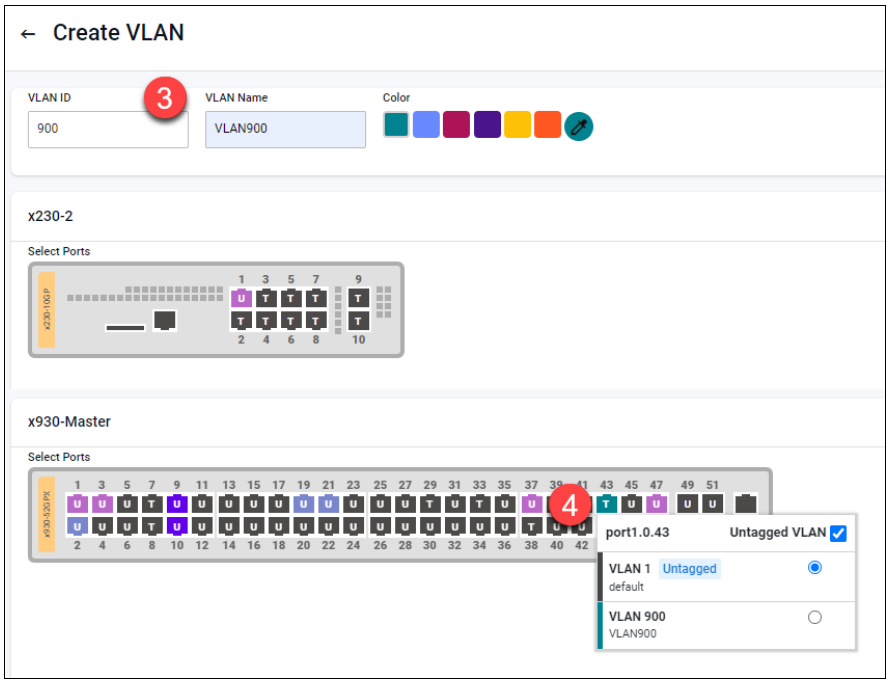
1. Select the device or devices you want to add the VLAN to. Click to select one device, or use the multi-select button to select more devices.



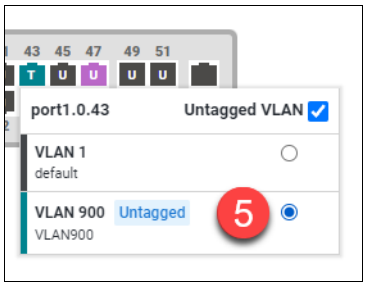
2. Click **Create VLAN** to create a new VLAN.



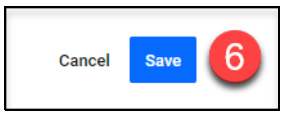
3. Enter the VLAN ID and name, and select a display color for it.
4. Click on the switchport you want to add the VLAN to, until it changes to the VLAN's color and shows a **T** (for "trunk").



5. 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.

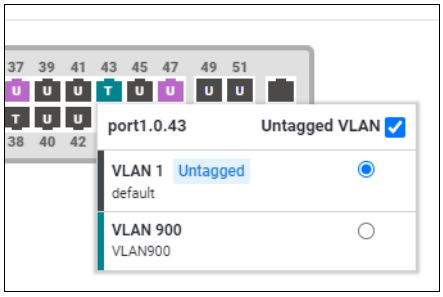


6. Click **Save** to save the configuration.



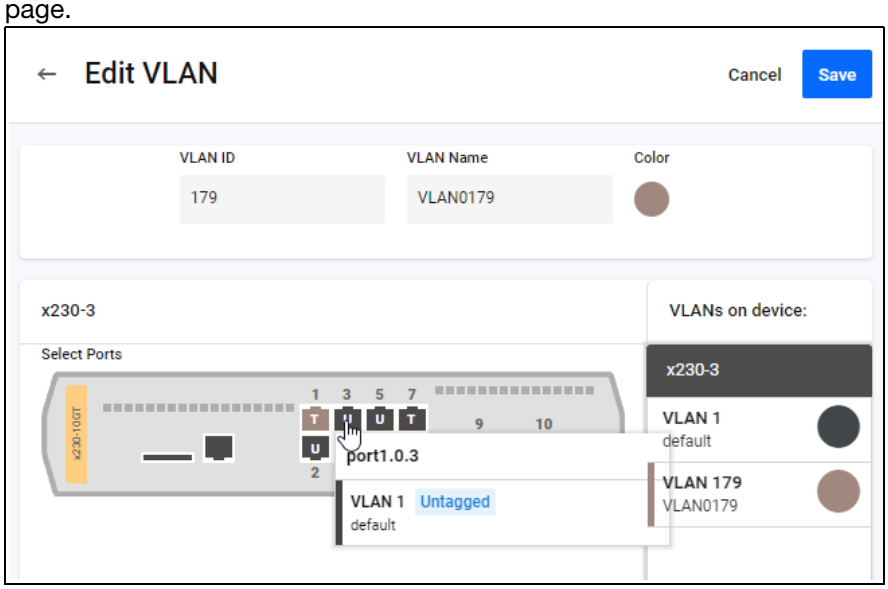
VLAN 1 port reconfiguration

If a port is assigned to VLAN 1 in Access mode, you can reassign a different VLAN without having to remove VLAN 1 first. 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.



Edit VLAN

Clicking on the pencil icon on the right of an already created VLAN brings you to the edit VLAN page.

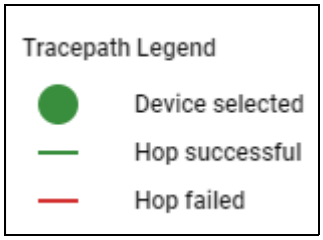


On the edit VLAN page, you can edit the ports added to the VLAN selected. Ethernet Protection Switching Ring (EPSR) ports are disabled on the VLAN editing page. You can easily identify EPSR ports when editing VLANs, and avoid misconfiguration.

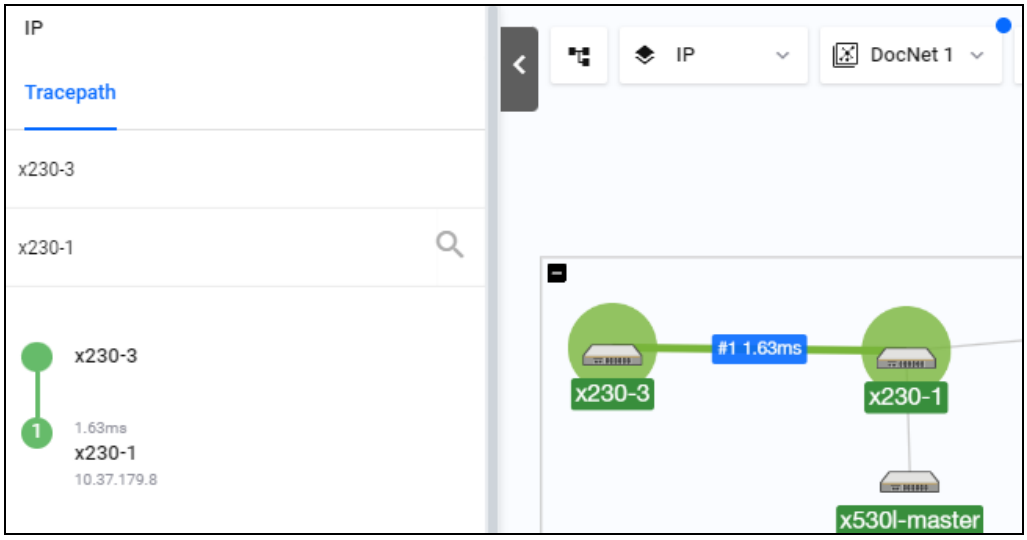
IP map layer

The IP map layer shows the hops that data packets take between two selected devices. The devices you select, as well as the path between, are marked in green. From the IP map layer, you can access the **Tracepath** and **Walk path** features on the side menu.

The information icon changes to show the Tracepath or Walk path legend, depending on what you have selected in the side menu.

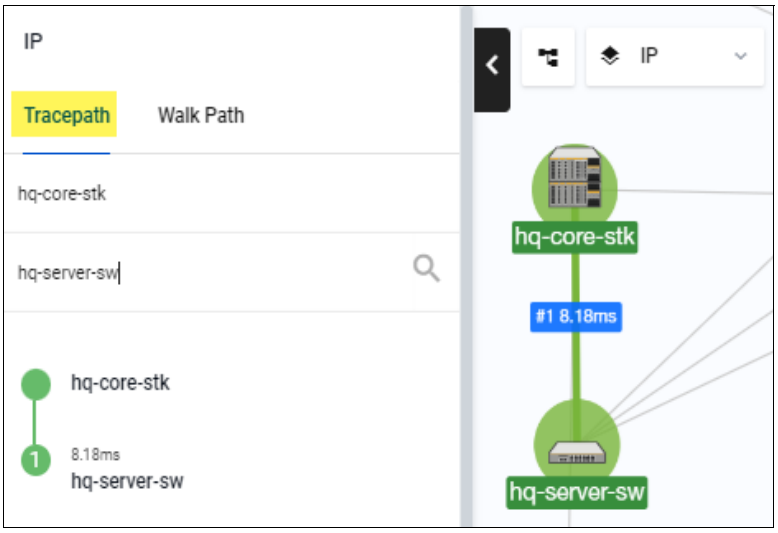


You can manually enter the source and destination from the search list on the left, or click on the devices on the map to select them.



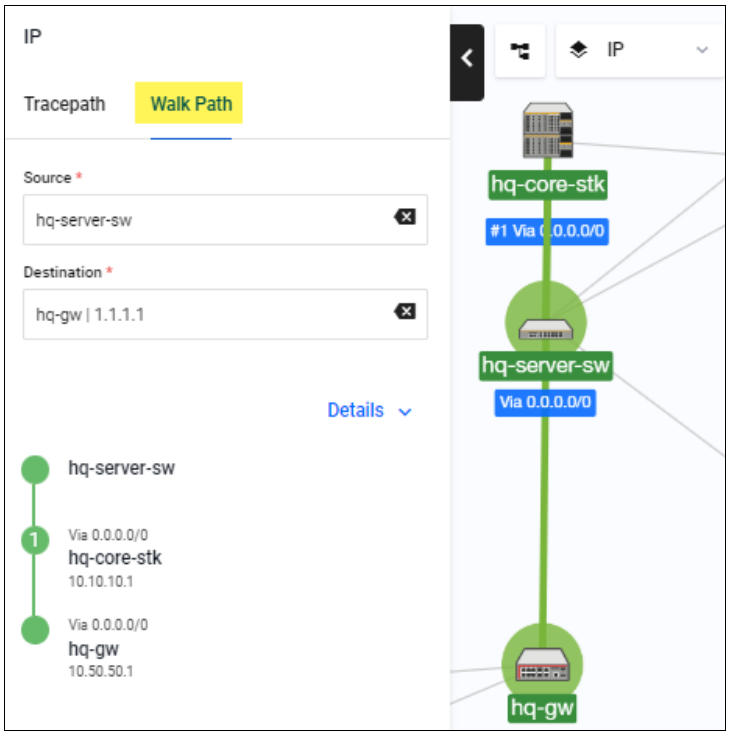
Tracepath

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 round trip time (RTT) information.



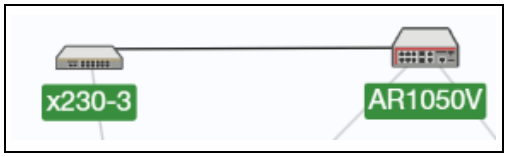
Walk path

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.

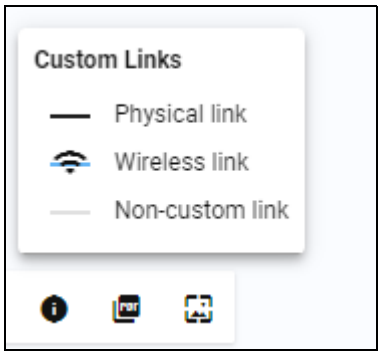


Edit map layer

On the Edit map layer, you can edit the layout of the devices on the network map and create custom links.



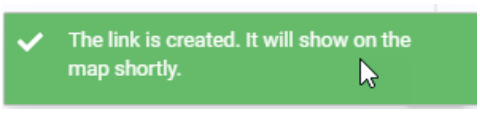
The information icon changes to display the custom links legend:



The **Upload Background Image** button is visible on the edit layer. You can apply a background image to the map of your network such as a floor map or other image.

Creating custom links

You can create custom links between devices on the Edit map layer. In order to create a link between devices, select the first device you would like to create the link on, and then select the second device to connect the link to. The link will appear in a few seconds after Vista Manager processes the change. To see information on how to manage the traffic of custom links, see "Traffic map Layer" on page 85.

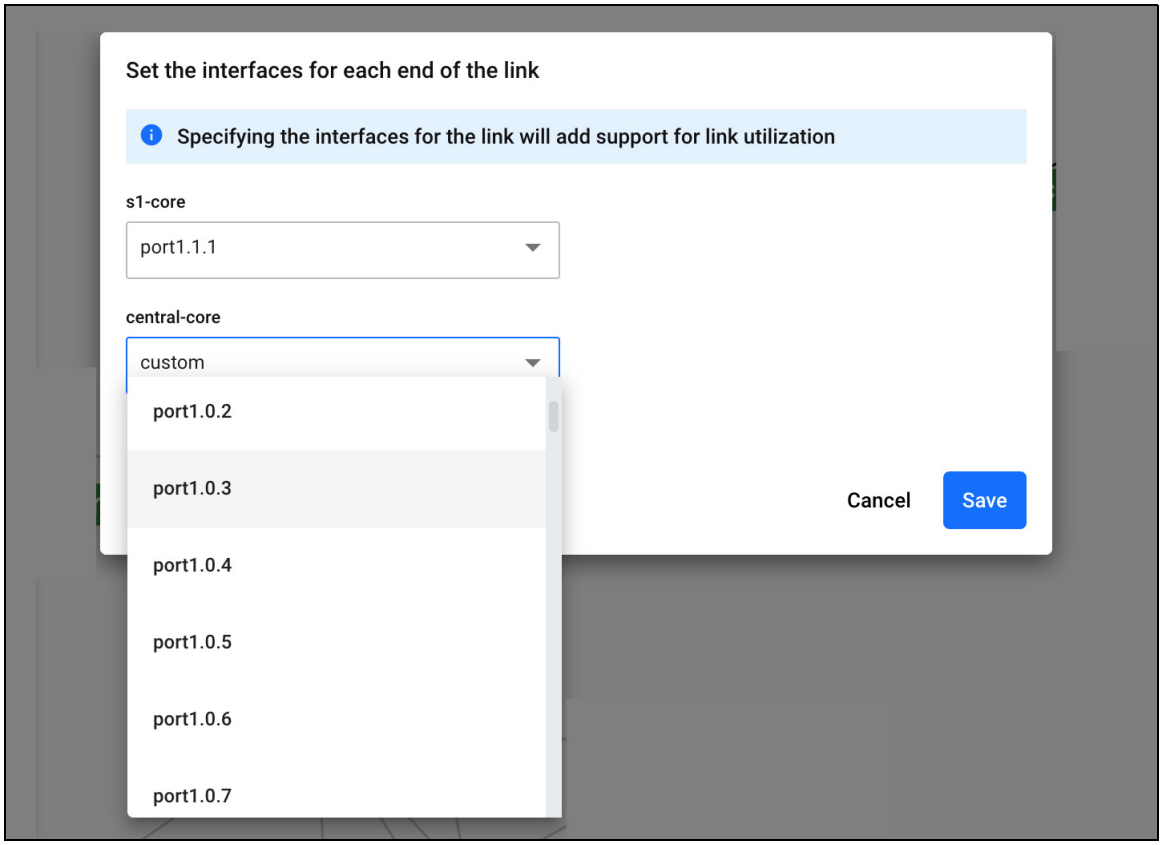


When a link is created, a notification will appear in the bottom left of the map which indicates that Vista Manager is creating the link.

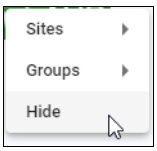
You can set or unset a custom link as a wireless link, and set link interfaces by right clicking on the link.

Setting custom link interfaces

When you right click on a custom link, you can select **Set link interfaces** to bring up a menu where you are able to set the interfaces for each end of the custom link.

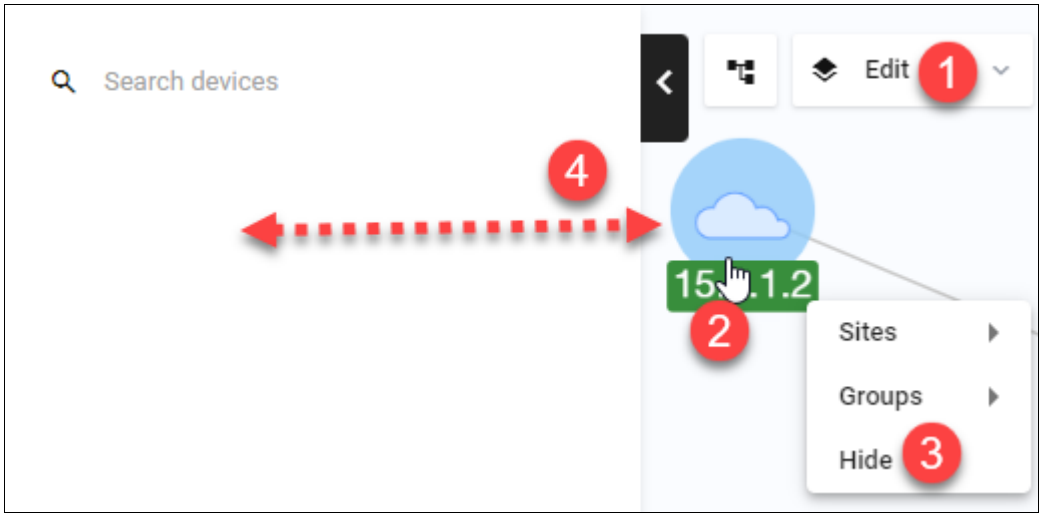


Show/Hide devices



From the Edit map layer, you can hide devices, and they will remain hidden on any layer of the map. You can hide devices on the map by right-clicking the device you would like to hide, and selecting **Hide.**

Hidden devices will appear on the left-hand menu and you can show them again on the map by dragging them out of this menu and back onto the map.



Importing a background image

You can import a background image to a map screen on the Edit map layer by clicking on the **Upload Background Image** button. This is useful to show the physical location of devices that may be on a building level or floor map.

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.

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 again.

Health Monitoring

You can use the Health Monitoring menu 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.

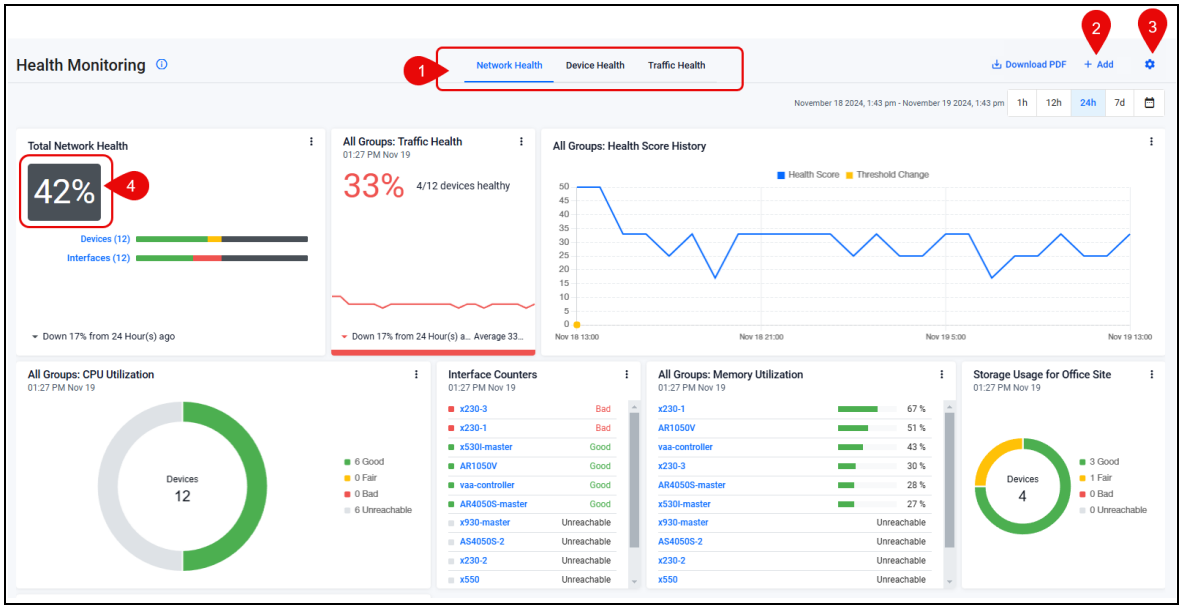
There are three key indicators (tabs):

- **Network Health**: the default tab - shows your entire network's health
- **Device Health**: shows utilization statistics of devices in your network (CPU, memory, storage, temperature).
- **Traffic Health**: shows the health of the traffic flow of your network (including interface counter metrics, when toggled).

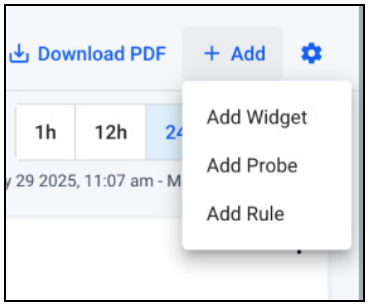
Checking the network health

To check your network health and customize the dashboard, from the Network Health tab.

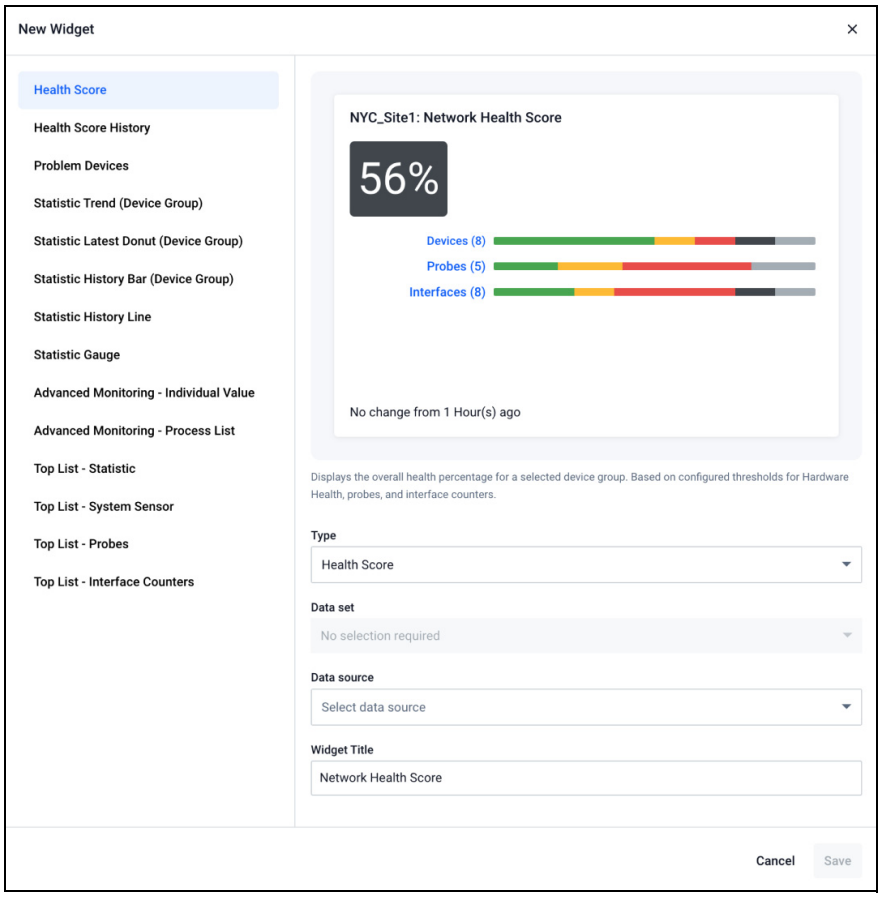
1. Make sure the Network Health tab is selected



2. Optionally, add widgets, probes, or rules by clicking the **+ Add** button in the top right of the Health Monitoring page.



When creating a widget, you can also add a custom name to display as the title of the widget.

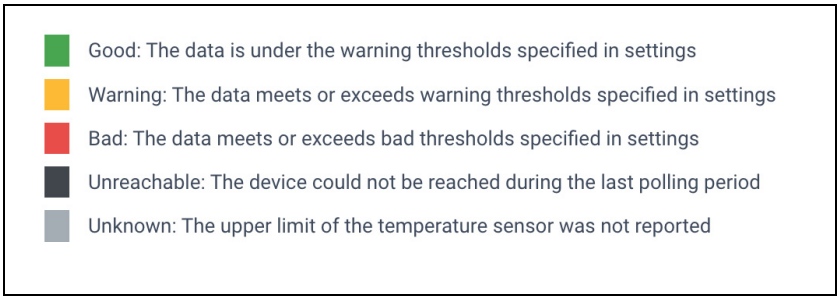


3. Once you've created the widget, use the **Settings** icon in the top right of the Health Monitoring page to configure the threshold values for the states (i.e. good, fair, bad) of each metric. These thresholds apply to the entire network and are used to determine the health status of devices and interfaces.

4. Check the **Total Network Health** score (located on the top left widget by default), which 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.

Health Monitoring Categories

The health monitoring widget for the monitored item is color-coded to indicate its health status. The color key as of version 3.14.0 is as follows:

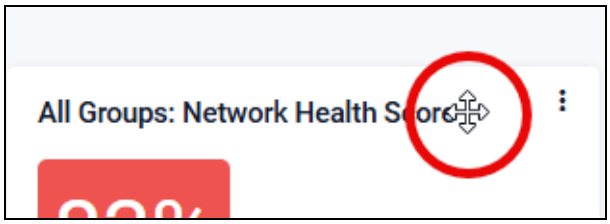


Categories include ‘Good', 'Warning' (previously 'Fair'), 'Bad', and 'Unreachable’.

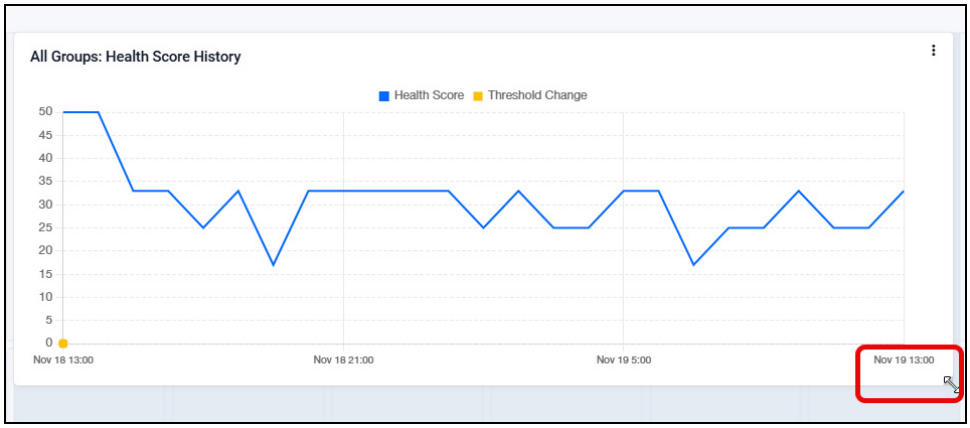
When there is no high limit on a sensor, that sensor will be classed as 'Unknown', and it will not count towards a Health Score rating.

Temperature sensors include an ID number at the end of their name.
For example: ‘Temp: System 8’ would indicate that sensor has an ID of 8. When multiple sensors share the same name on a device, this ID helps you match each sensor in Vista Manager to its corresponding sensor on the device.

From version 3.14.0 onwards, when you create a new widget from the Health Monitoring menu, a preview of the widget will be displayed. To move a widget, hover over the widget heading and click and drag the widget to the desired location.

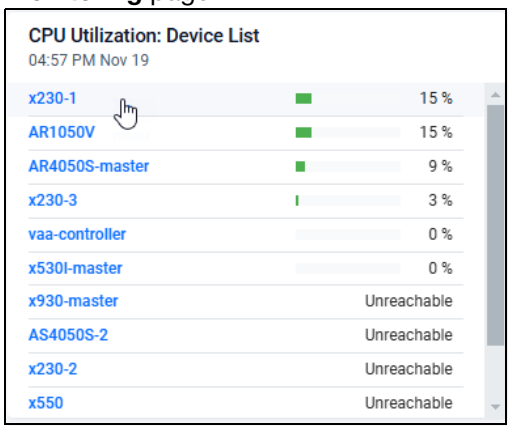


You can also resize widgets, such as the Health Score History graph, for a bigger or smaller view.




To delete a widget, click the Action button (the 3 dots) in the corner of the widget.

To see a device's live CPU statistics, click on a device from the **Device list** on the **Health Monitoring** page.



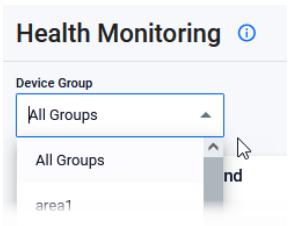
- CPU usage data matches data shown in the CLI command **show cpu**
- CPU charts update in real-time.

CPU charts include:

- CPU load history per second (over the last 60 seconds)
- CPU load history per minute (over the last 60 minutes)
- CPU load per 30 minutes (the last 60 load values over 30 hours)

Scroll to the bottom of the Device's Health Monitoring page and you will see the Live CPU graphs.

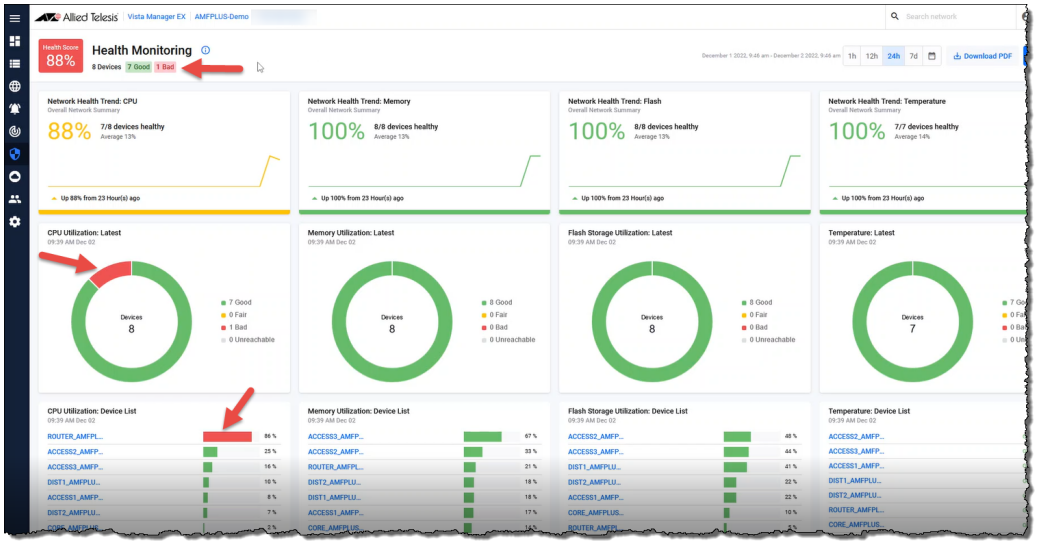
Checking a Device's Health



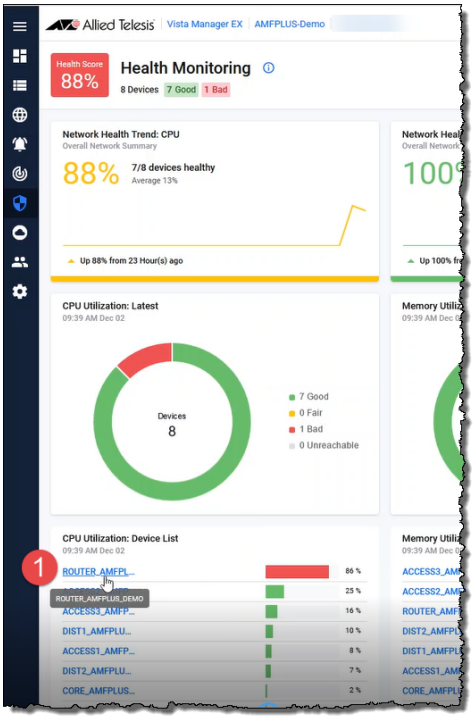
Use the **Device Group** selector on the Device Health and Traffic Health tabs to display a specific group. The default is All Groups. For information about creating groups in the **Asset Management** menu, see "Groups" on page 168.

Note that this example uses screenshots from a previous version of Vista Manager. The process looks different in current versions, but still retains most of the same step by step procedure.

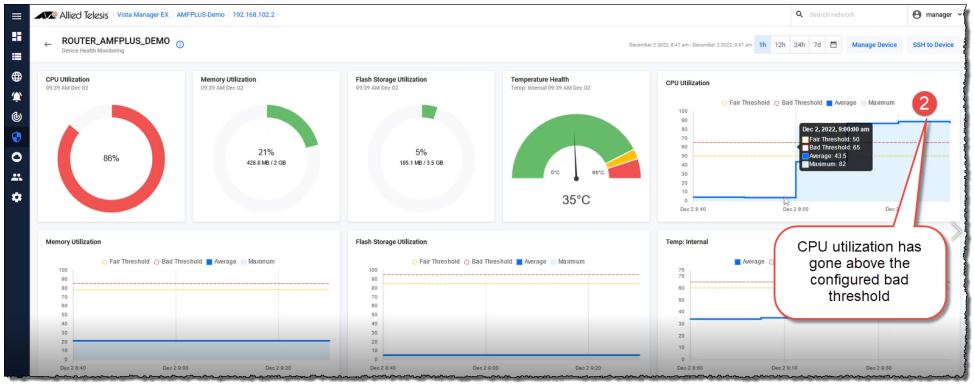
In the example below, you can see a Health Score of 88%. There are 8 devices in this network, but there's a CPU issue with one of them. The bad device is highlighted in red.



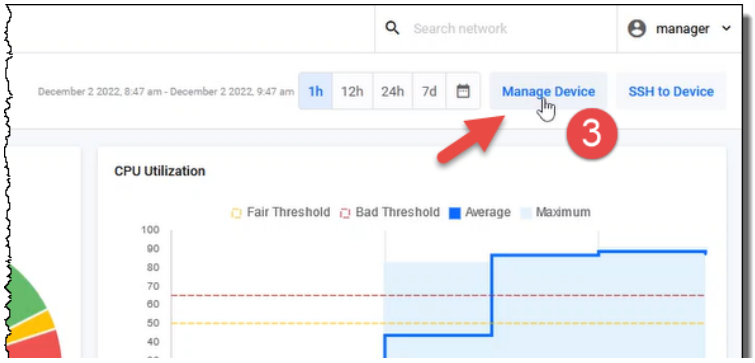
1. Click on the 'bad' device name to investigate further.



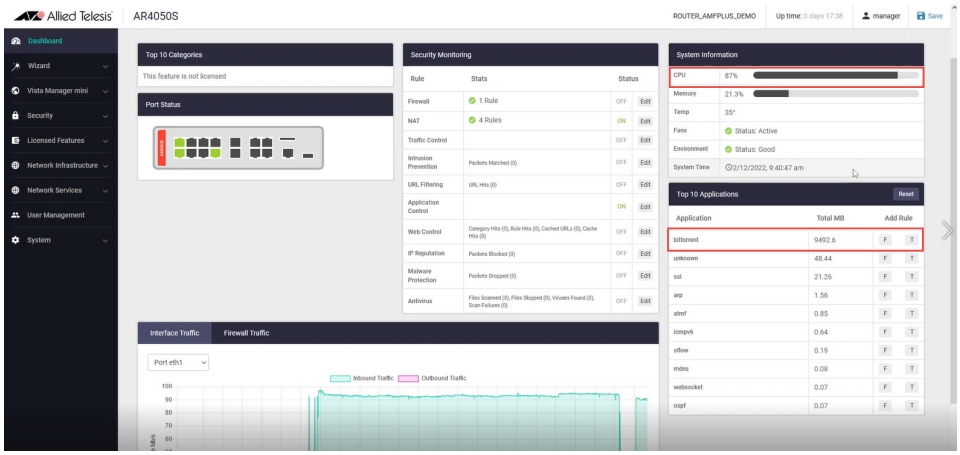
2. Drilling down confirms that around 9am CPU utilization rose above the configured band threshold.



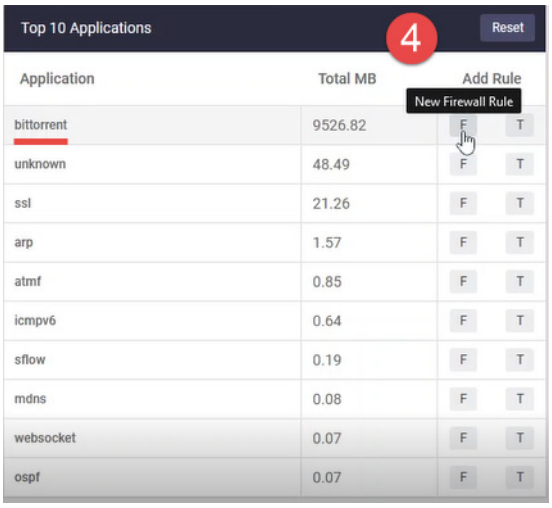
3. To further diagnose the issue, click on **Manage Device** to open the Device GUI.



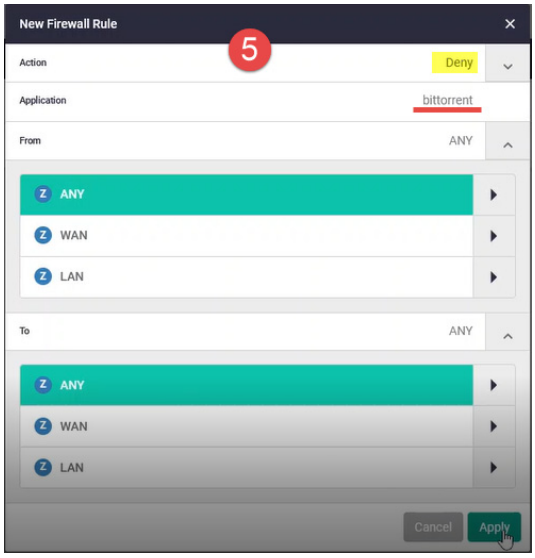
From the Device GUI of the AR4050S device, the system information section indicates a very high CPU usage, and the Applications section shows bittorrent traffic increasing quite rapidly. This is likely to be the cause of the high CPU utilization.



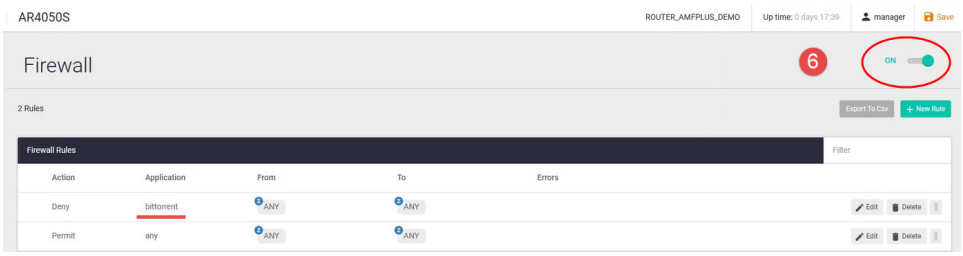
4. At this point you may decide to disallow the bittorrent traffic by adding a firewall rule.



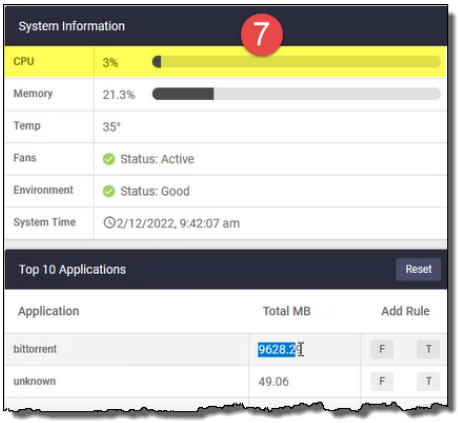
5. Configure the firewall rules.



6. Turn on the firewall.



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



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.

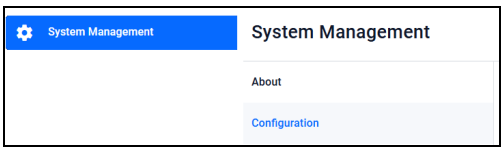
Note: You can export a PDF of the selected tab from the Health Monitoring page by clicking the **Download PDF** button. The PDF scales to match what you see in Vista Manager when you zoom in or out in your browser window.

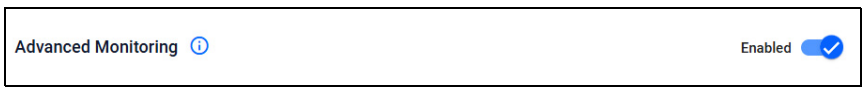
How to add a Windows Server to Vista Manager

From version 3.13.1 onwards, you can view Windows Server Monitoring charts and metric data from the Health Monitoring page. This means you can monitor Windows Server information in Vista Manager.

Step 1. Enable Advanced Monitoring from System Management.

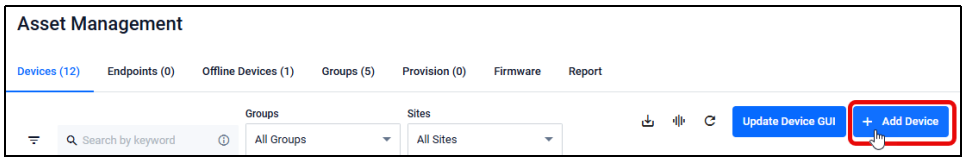
Go to **System Management** > **Configuration** and enable the Advanced Monitoring feature.



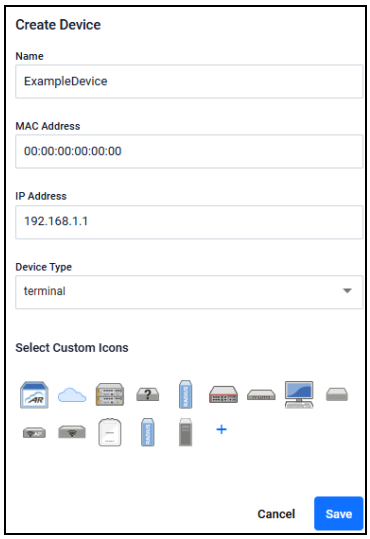


Next add the windows server as a device in the Asset Management menu. Note that you do not have to perform this if it has already been discovered from another source.

Step 2. Go to the **Asset Management** page and click **+ Add Device**



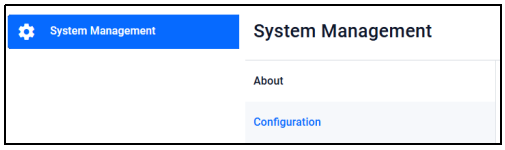
Enter the Name, MAC Address, IP Address, Device Type, and optionally a custom icon.



Click **Save**.

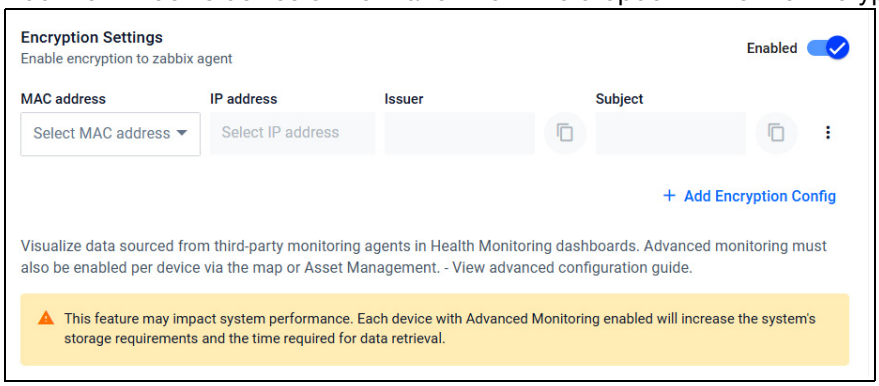
Step 3. **(Optional)** Enable Encryption settings and enter the zabbix agent information.

Go back to the **System Management** > **Configuration** page.

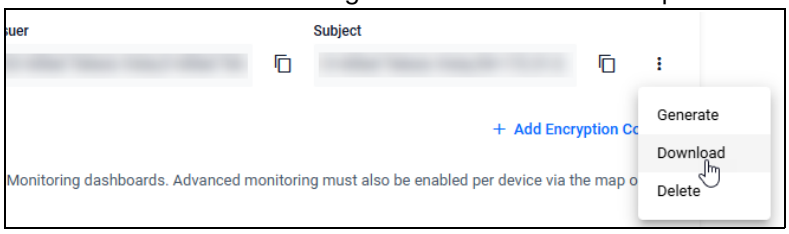


Scroll down to **Optional Features**, and toggle the Advanced Monitoring Encryption Settings toggle. Using the information from the previous step, select this device from the dropdown for encryption.

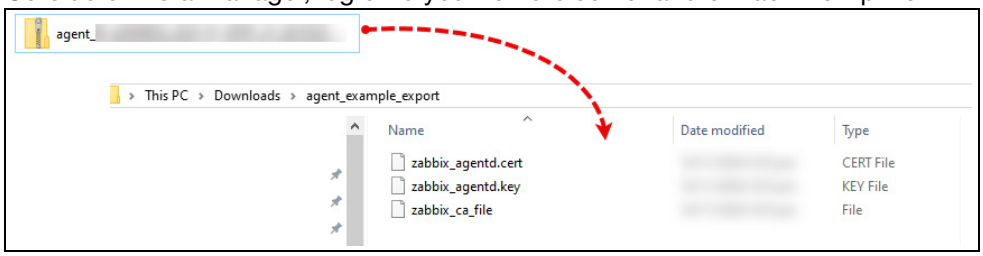
Add the Windows device's information from the dropdown into the Encryption Settings fields.



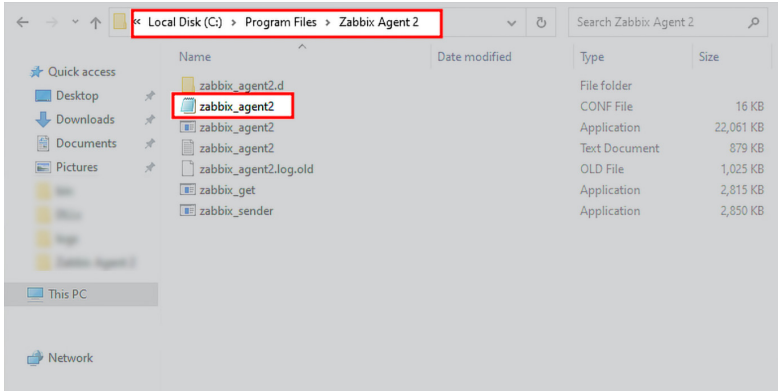
- You can optionally click the Action button and select Generate to get the Issuer and Subject information.
- Click the Action button again to download a local zip file of the configuration.



Outside of Vista Manager, log onto your remote server and extract the zip file.



Navigate to your Zabbix Agent 2 installation folder and open the Zabbix_Agent2.CONF file in a text editor of your choice.



The default path for the installation folder is ***C:\Program Files\Zabbix Agent 2***

Follow the documentation from the Official Zabbix Agent 2 Documentation to see how to edit the configuration file.

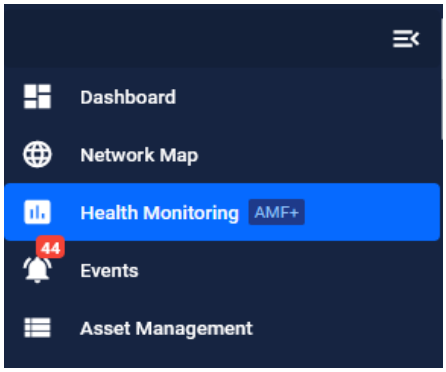
Step 4. **Restart the Zabbix_agent2 service** from Task Manager on your remote server to apply the updated configuration.

Step 5. In Vista Manager, refresh the Network Map topology by clicking the **Refresh button**.

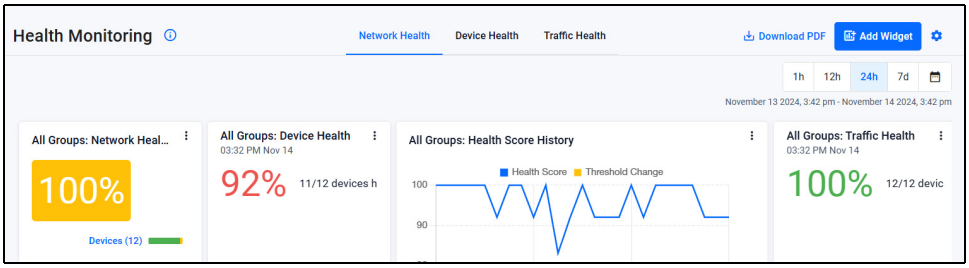
The Windows Server will appear as a device on the Network Map.

How to add the widget to the Health Monitoring Page

Step 1. Click on **Health Monitoring** from the **side menu.**

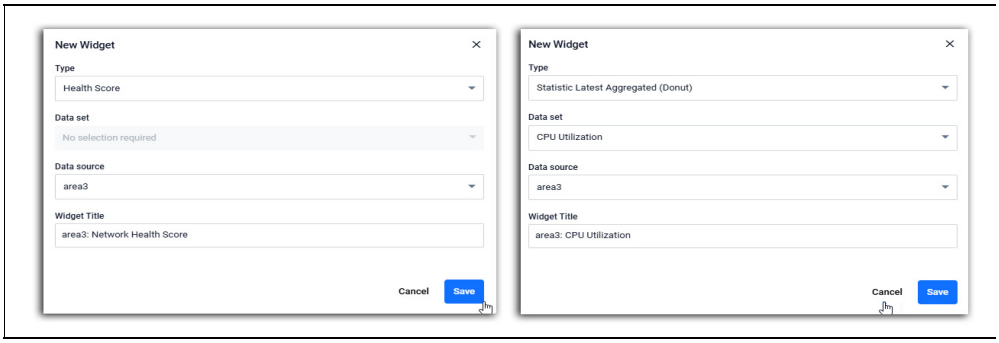


This opens the Health Monitoring page:



Add Widget

Step 2. Click **Add Widget** to add a widget, and click on the **Type**.



For the windows server specifically, you can select from:

- Advanced Monitoring - Individual Value (CPU, RAM)
- or Advanced Monitoring - Process List (CPU, RAM)

Step 3. Select the **Windows Server** as the **Data Source.**

Step 4. **Wait a moment** for polling and the data will appear on the **Network Health dashboard**.

Creating Link Monitoring Probes

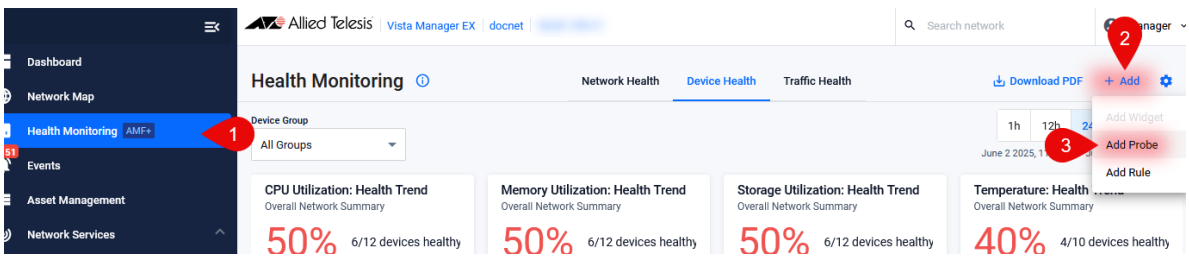
The Health Monitoring feature allows you to create Link Monitoring (Linkmon) Probes and will report statistics (latency, jitter and packet loss) on these probes, representing the health of the traffic.

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

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

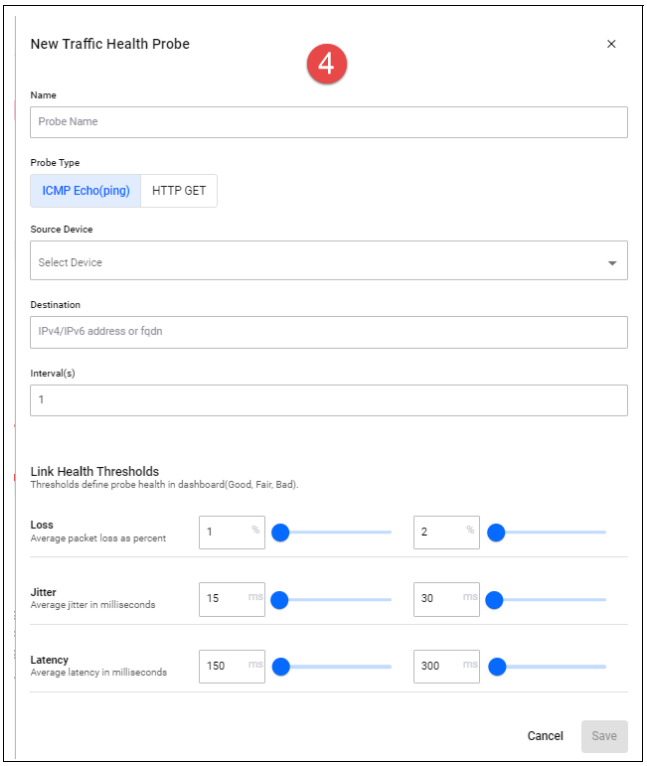
To use this feature:

1. Go to **Health Monitoring**
2. Click +Add and select Add Probe
3. The sidebar will open.



4. The **Add Traffic Health Probe** side-window opens.

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



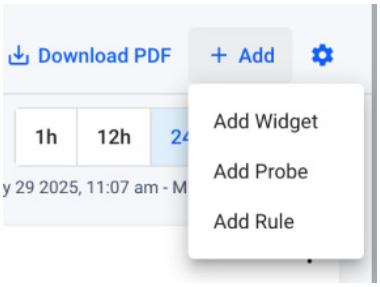
Adding Health Monitoring Rules

From version 3.12.0 onwards, you can create custom rules for Health Monitoring from the Health Monitoring Dashboard. This feature allows you to set up actions, such as email notifications or alarms, when Health Trend widgets from the Health Monitoring dashboard go red (or bad).

Note that you must enable Health Monitoring Polling for all rules to work.

For rules that use Interface Counters as a metric, you must enable both Health Monitoring Polling, and Interface Counters.

Click **+ Add** and select Add Rule to add a new custom rule.



You can then input a name, select a metric, and select an action. You can add an additional action by clicking **Add action +** below the first Action (with a maximum of 2 total actions).

An action or event will be triggered if:

- The metric you specified has its Health Trend change from good to bad,
- or, if a device within that metric becomes bad from fair or good, and if it has not already been triggered for a given period of the metric being red.

When a metric goes green again, then devices fitting that metric have the ability to be triggered once the metric goes red again.

If you do not select an action, then no notification will be sent even if the conditions are met.

Metrics that you can select from are:

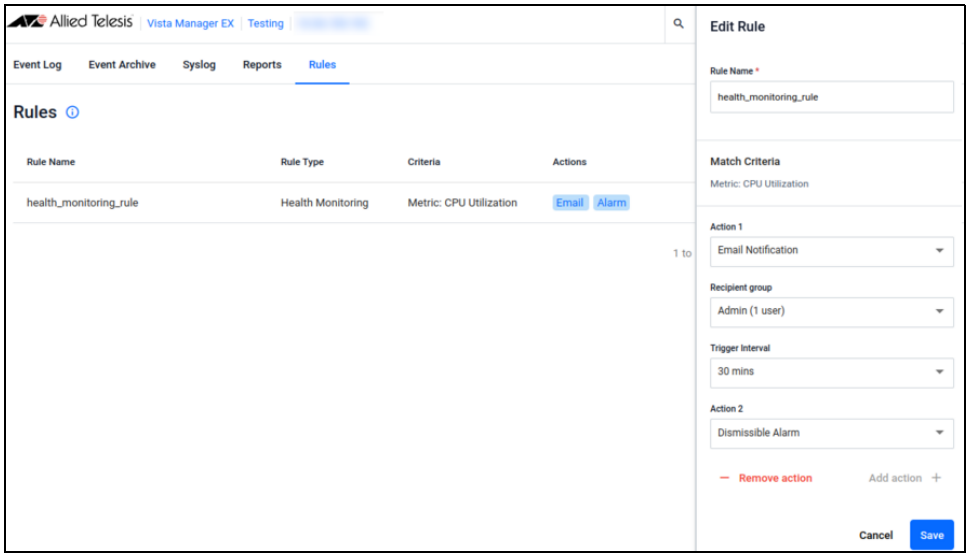
- CPU Utilization
- Memory Utilization
- Storage Utilization
- Temperature
- Traffic Health
- Interface Counters - Note that this must be enabled first in the Settings

The **Actions** you can set from include:

- Email Notification
- Dismissable Alarm
- No Action

You can dismiss the alarms manually.

Created rules are displayed on the **Event** page in Vista Manager EX, and you can edit existing rules from the **Rules** tab on the Events page.

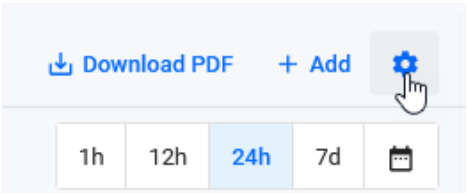


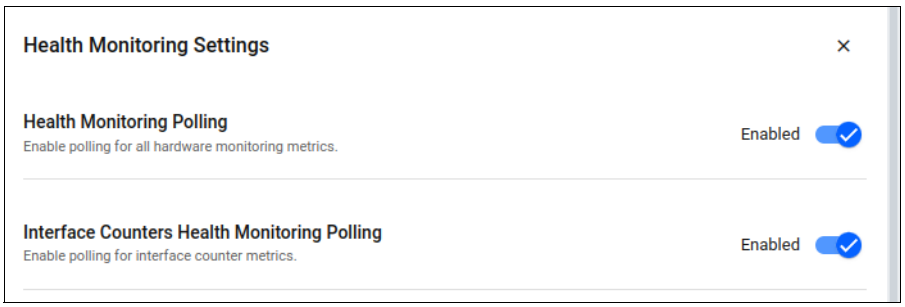
You cannot edit the Metric Criteria section from this page, so if you require a new metric to be tracked then create another rule.

Health Monitoring Polling and Interface Counters Polling

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

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

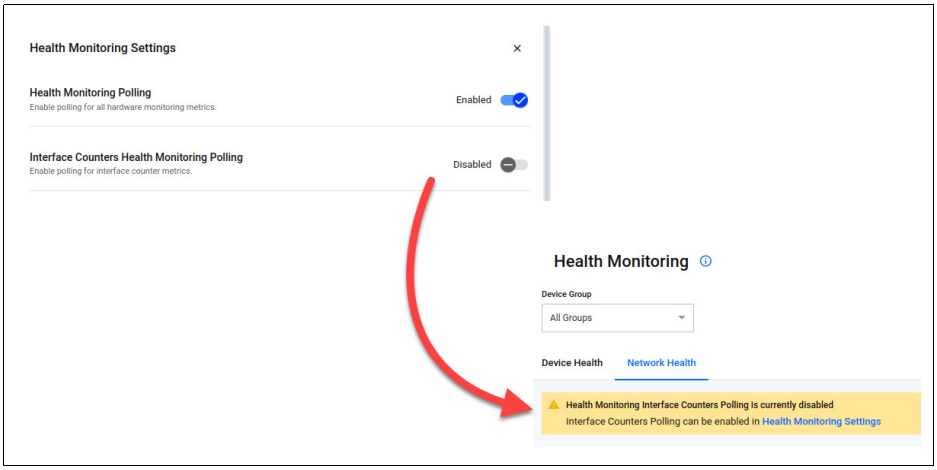




You must first enable Health Monitoring Polling before you can enable Interface Counters Health Monitoring Polling.

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

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



The Interface Counters dashboard includes the following widgets:

- Health Trend
- Latest
- Device List
- History

Use the Interface Counters dashboard to easily monitor:

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

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

Monitoring third-party devices

From version 3.10.3 onwards, the Health Monitoring page incorporates information on third-party devices (i.e., non-AMF devices). Prior to this, only network devices belonging to AMF were subject to monitoring. Using the SNMP Plugin, the Health Monitoring dashboard displays the latest stats for all devices with an IP address.

The SNMP plugin collects detailed information and statistics from network devices, and utilizes a Standard MIB compiler to generate charts based on MIB values. See Table 2 on page 121 for the supported MIB information.

If the SNMP device can provide such information, the Health Monitoring dashboard will display CPU, RAM, Storage, and Temperature statistics.

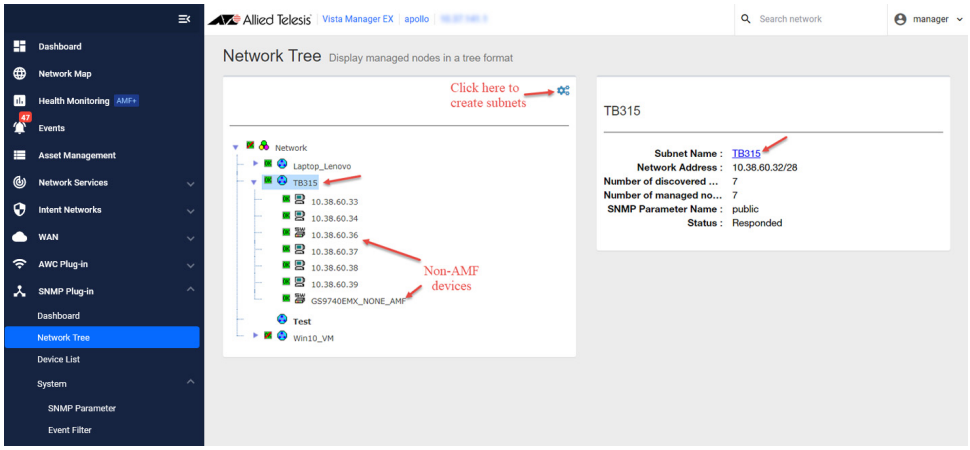
Table 2: Supported MIB information

VENDOR NAME	SNMP AGENT	MEMORY SIZE	STORAGE SIZE	CPU LOAD	SENSOR
Standard MIB	SNMP Service (Windows) Net-SNMP package (Linux)	HOST-RESOURCE-MIB::hrStorageTable (hrStotageType=hrStorageRam)	HOST-RESOURCE-MIB::hrStorageTable (hrStorageType=hrStorageFixedDisk or hrStorageRamDisk)	HOST-RESOURCE-MIB::hrProcessorLoad	ENTITY-SENSOR-MIB::entPhySensorTableENTITY-MIB::entPhysicalTable

Activating Health Monitoring statistics for non-AMF devices

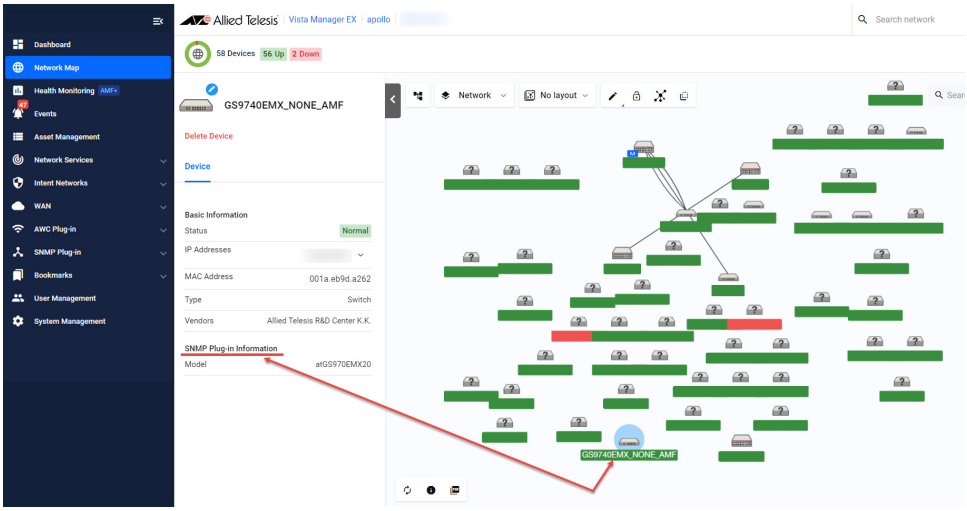
First you need to add the SNMP Plugin, then add and configure an SNMP network.

1. To add the SNMP plugin:
   - Go to **System Management** > **Plugins**
   - Click **+ Add Plugin**
   - Enter the Server URL - https://<i***p-address***>:6443/NetManager
   - Verify the connection and **Save**.
   - For more details on registering plugins, see "Registering/Installing plugins" on page 26
2. To add an SNMP network.
   - Go to **SNMP Plugin** > **Network Tree**
   - Create a subnet.
   - After a few minutes the SNMP Plugin automatically discovers available devices under the specified subnet.
   - After auto discovery is complete, a list of devices is shown on the Network Tree.



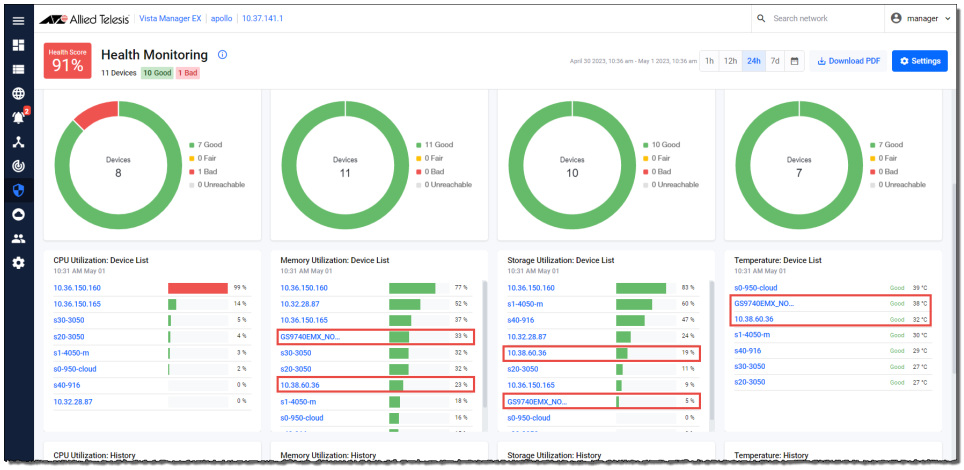
3. Check the Network Map to find the devices that were discovered by the SNMP plugin.
   - Go to **Network Map**

- Click on a device to see its SNMP Plugin information.



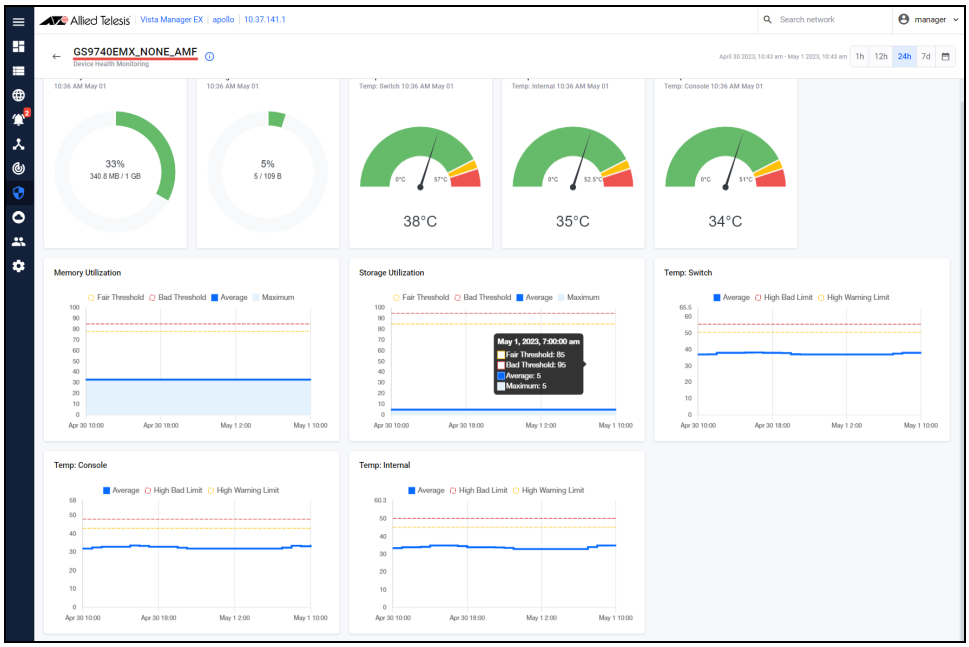
4. To obtain the latest statistics for third-party or non-AMF devices discovered by the SNMP plugin, check the Health Monitoring dashboard or the Device Specific dashboard.

   - Go to **Health Monitoring**
   - The Health Monitoring page includes all valid third-party or non-AMF devices in the summary charts.



- Click on a specific device to see its details.

- For example, the image below shows the details for ‘GS970EMX_NONE_AMF.

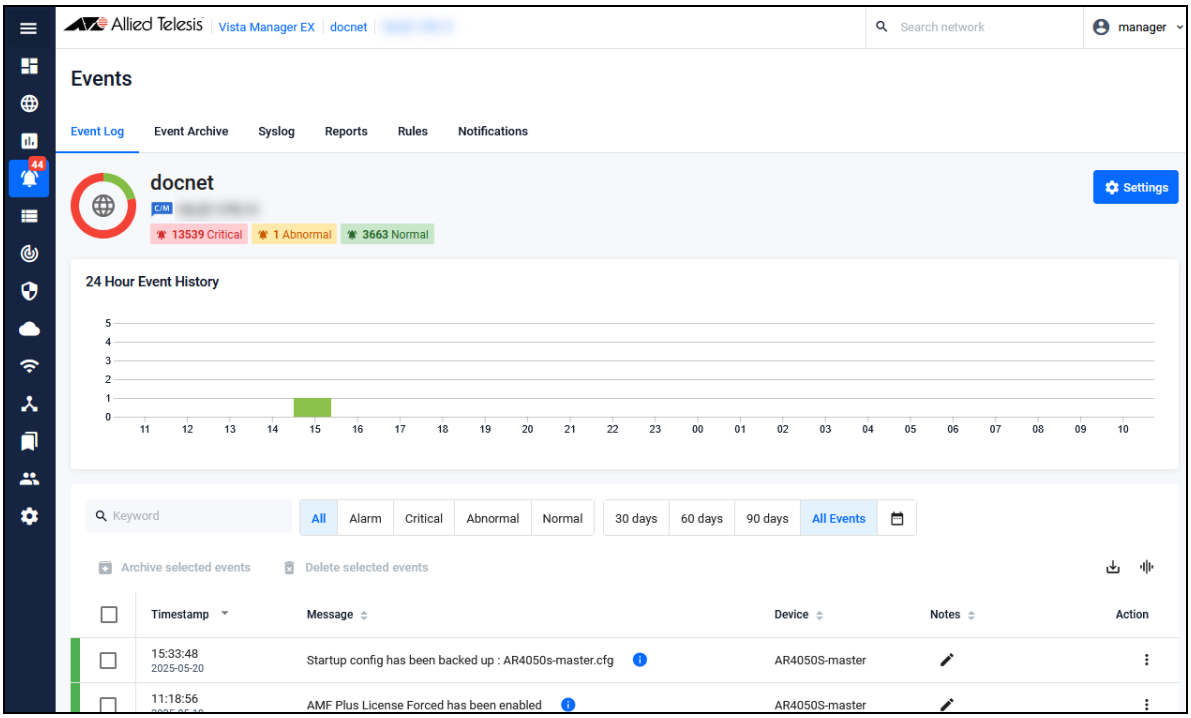


Please note that you can only find third-party devices on the Health Monitoring dashboard if the correct MIB is supported on the third party device.

Events

Event Log

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



The event log shows you the history of events in your network, and currently uncleared events. Critical events have a red background, abnormal events are yellow, and normal events are green. As an administrator, you can manage events in your network.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. The graph at the top of the image shows the event history of your network over a 24 hour period.

As a user, you can view and search through all event logs.

Vista Manager Event severity levels

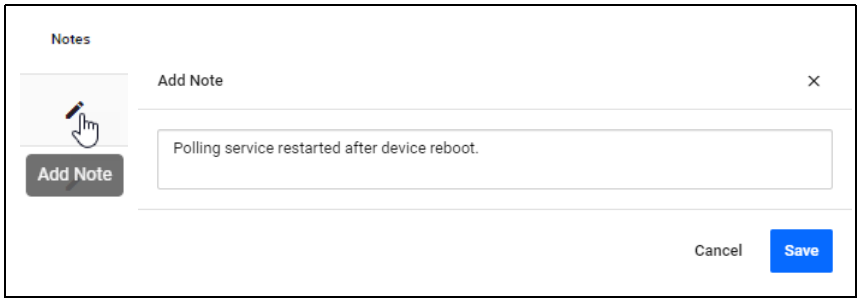
Events in Vista Manager are categorized by the following severity levels. The alert level depends on how important an event is:

- 0 EMERGENCY
- 1 ALERT
- 2 CRITICAL
- 3 ERROR
- 4 WARNING
- 5 NOTICE
- 6 INFORMATION
- 7 DEBUG

EMERGENCY and ALERT level events create an alarm on the Network map (if device-related), and also appear as a count in the Endpoints table until the alarm is dismissed.

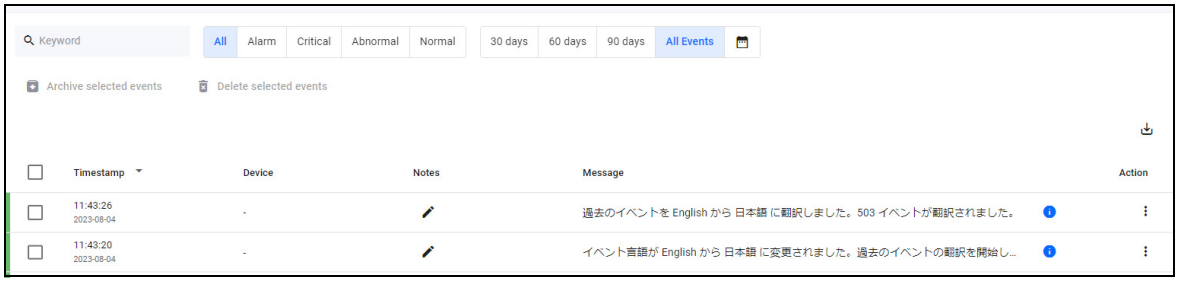
Adding notes to events

Click on the **pencil 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.



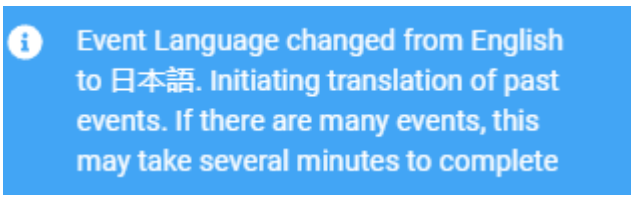
Event language

When you change the event language, the general UI will retain the main language, however event messages will be translated into the new language you have set. By upgrading to Vista Manager EX version 3.7.0 and later, you can translate events into Japanese (日本語).



Navigate to the Language tab of the System Management page's About section to change the language of events.

You are able to search for terms in Japanese, and the search function will search for key words matching that language. This language support functionality is only applicable to the Event Log, SD-WAN table of events, and Event Rules. Plugin events will not be translated.



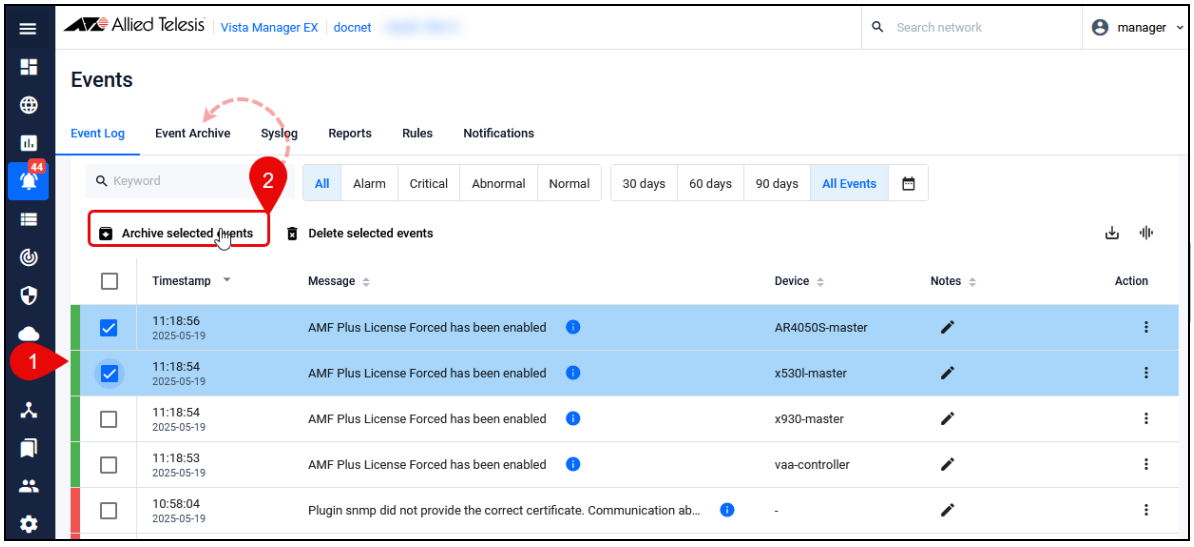
Changing the event language initiates the background process of translating past events. Once past events have been translated, event rule messages will then be translated to the new language.

An event log is also created and added to the list when the translation completes.

Note that this feature has been designed to support more languages in the future.

Event Archive

As an administrator, you can archive events on the Event Log section of the Events tab in Vista Manager. Archiving an event moves the log entry to the Event Archive tab and decreases the alarm icon's event count on the side bar.



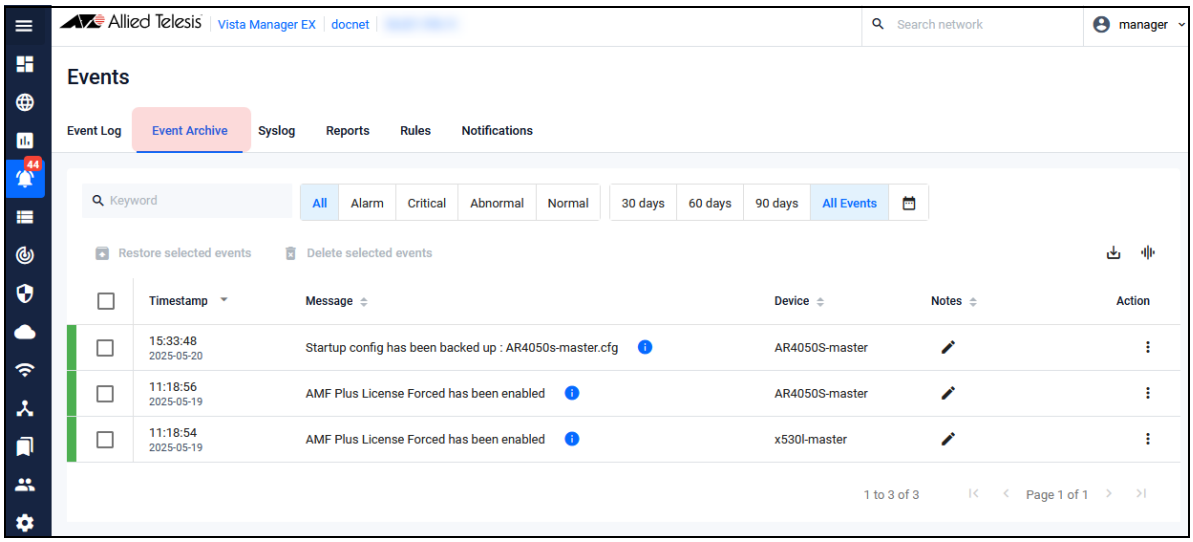
You can also:

- 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.

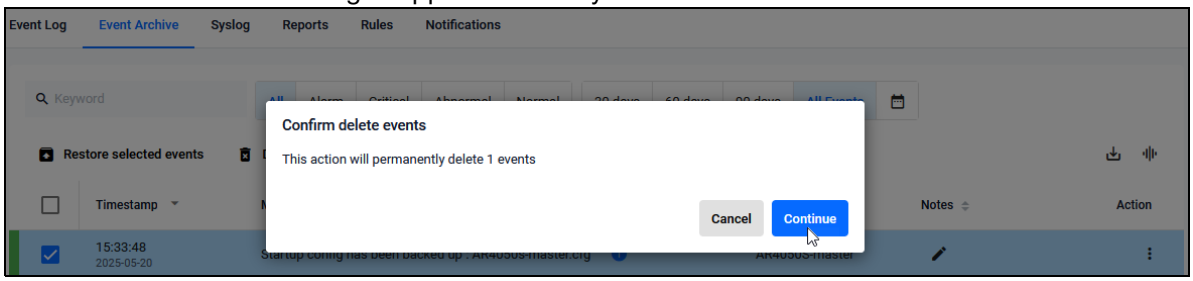
Archiving event notifications

To archive old or cleared events, select the events by checking the box on the left-hand side, and then click the **Archive selected events** button. You can also select all 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 restore archived logs back to the Event Log, or permanently delete them from the Event Archive. A confirmation dialogue appears when try to delete events.

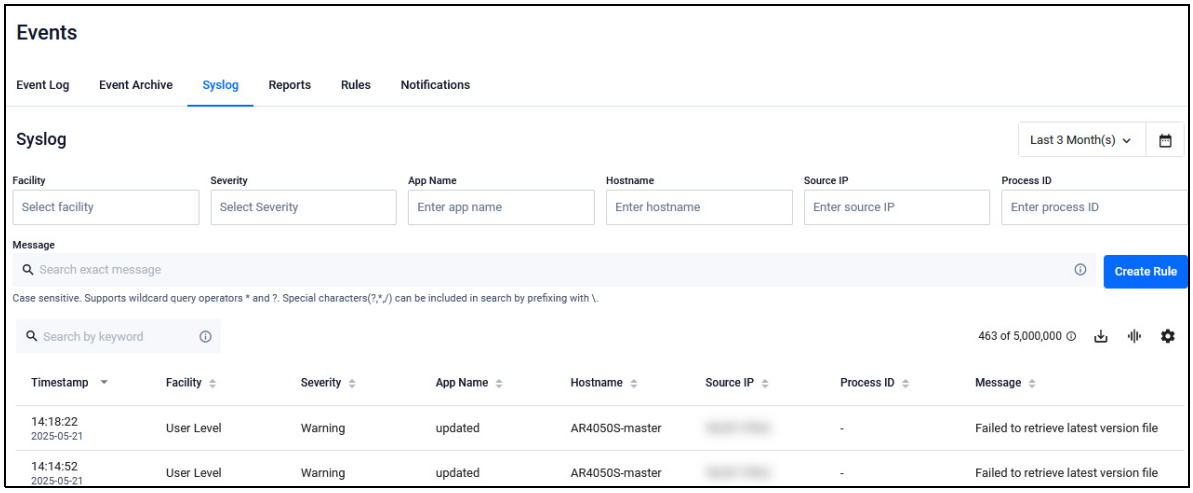


A server log message is displayed after a successful restore or delete operation.

Syslog

The Syslog tab shows syslog messages from the network or for a specific device on the network. Messages older than the default or configured length of time are automatically deleted.

As an administrator, you can configure how long Vista Manager stores syslog messages.The syslog storage is limited to 5 million entries, and the default configuration is 365 days.



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

Setting up Syslog messages in Vista Manager

To set up Syslog messages from a device to Vista Manager, you must configure the following commands in the device's CLI, as an administrator.

In this example, we send logs with the severity level of 'Notice' or above to the Syslog tab.

```
awplus# configure terminal
awplus(config)#log date-format iso
awplus(config)#log host <ipv4-addr>
awplus(config)#log host <ipv4-addr> level notices
```

Use `<ipv4-addr>` or `<ipv6-addr>` for the IP address of the remote syslog server. In this case, we use Vista Manager's IP address.

There are some limitations to take note of:

- As syslog messages are based on UDP protocol, this functionality may be unreliable.
- 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.

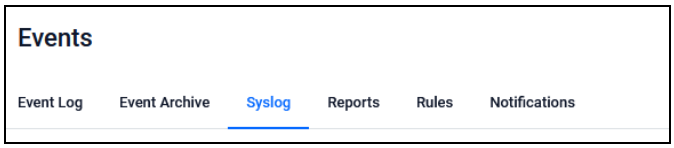
Syslog forwarding

As an admin user, you can relay syslog messages to an external server. This functionality forwards all received syslog messages to a specified syslog server, regardless of any rules configured. Note that only one external syslog server is supported.

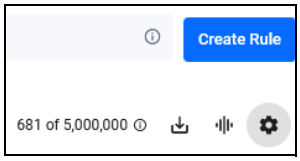
Note: The source address of a syslog cannot be retained to its external server.

To add a relay server address and enable syslog forwarding:

1. Navigate to the **Syslog** tab page from the Events menu.



2. Click on the Syslog settings gear icon. This will open the **Syslog settings** window.



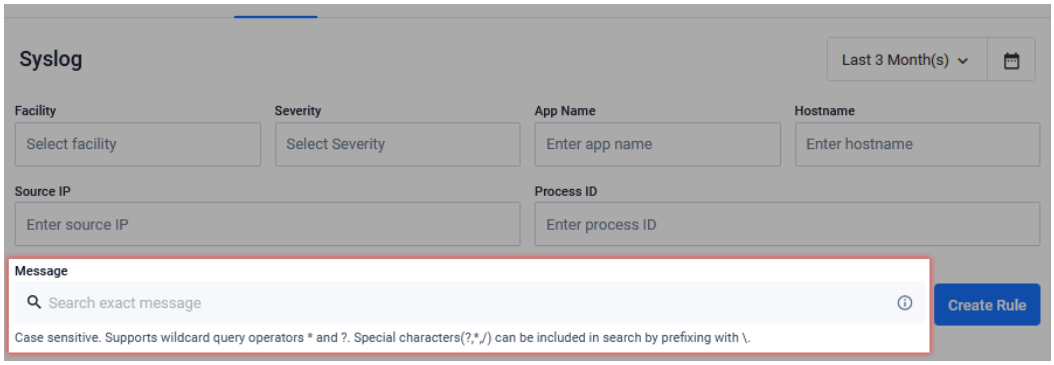
3. Check the **Relay syslogs to external server** checkbox to enable the Relay server address text field.

4. Enter the relay server address and port number.

5. Click **Save**.

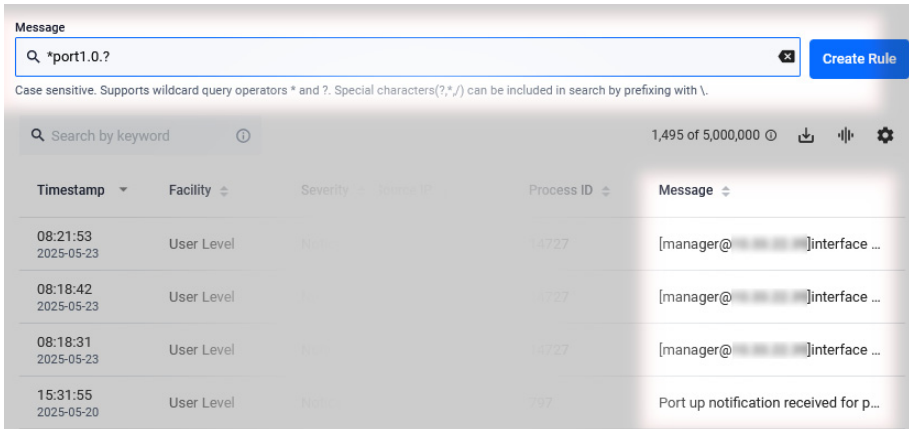
Syslog message filtering using wildcard characters

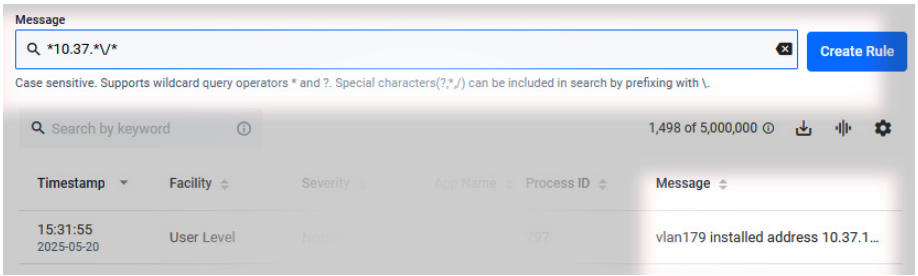
You can filter syslog events by whole or partial message content, by using multiple wildcards.



Details of supported wildcard query operators and special characters are as follows:

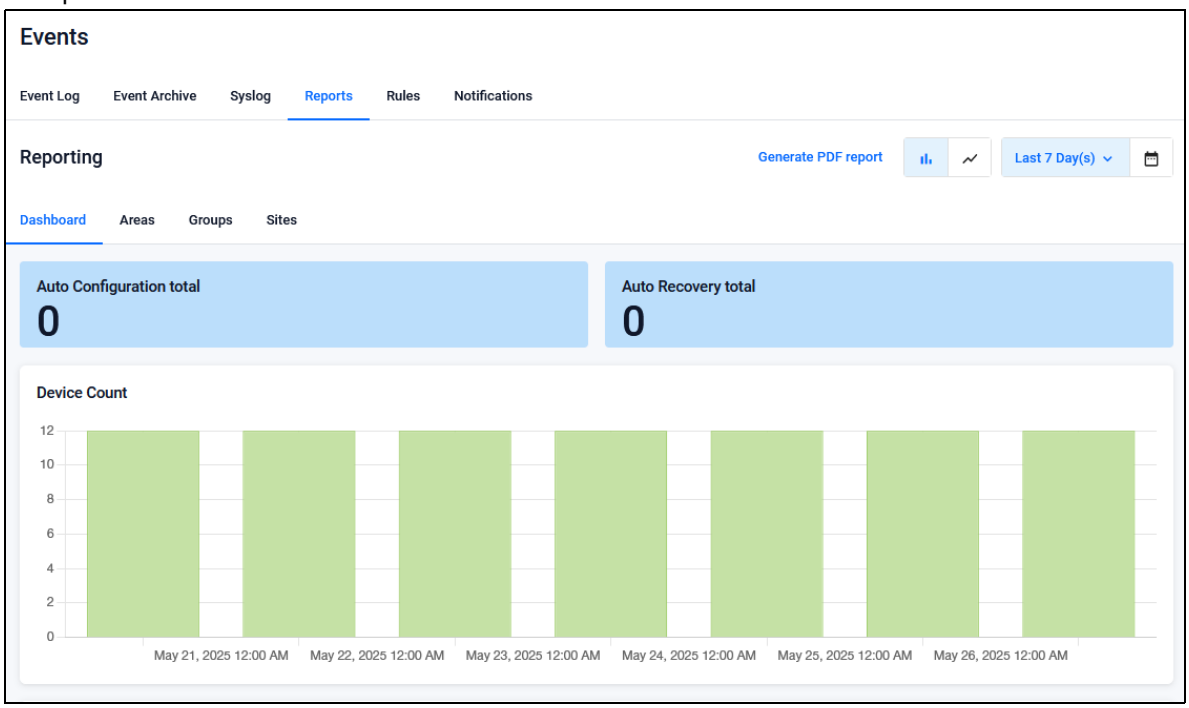
- A question mark (**?**) is used for a single character.
- An asterisk (*****) is used for multiple characters.
- A backslash (****) is used to escape any special characters (**?**, *, **/**) after it.
- When a backslash is expected to be part of the message to be matched on, escape it with an additional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



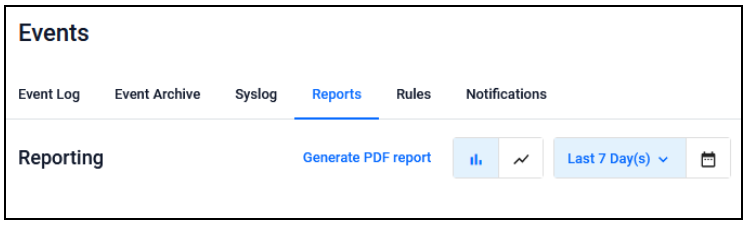


Reports

From the **Reports** tab, you can generate reports that provide detailed statistics of actions performed by the AMF networks. Reports are presented in easy-to-understand charts and tables. You are able to export these charts and tables to a PDF.

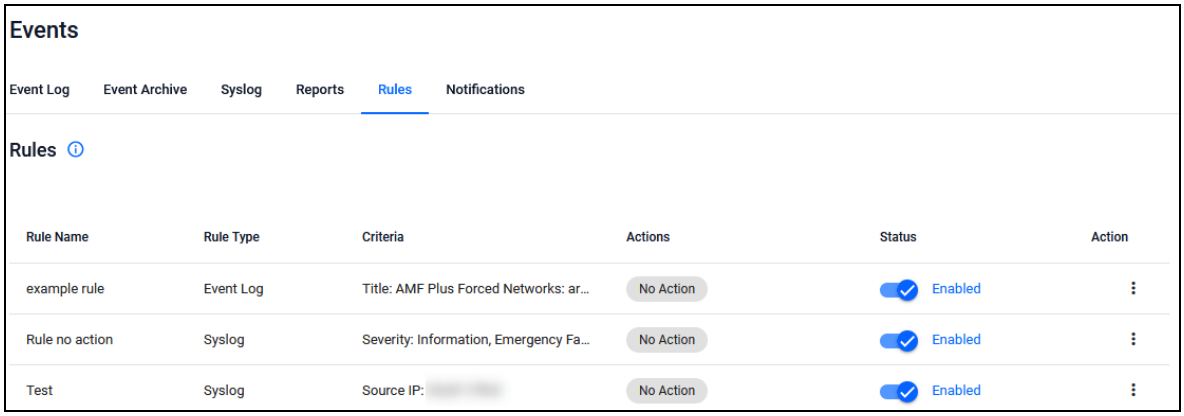


- Data for reports is compiled daily at midnight UTC time.
- You can specify a range between 7 days to 6 years for the reports tab to display, and can see how the size of your network has changed over time.
- You can click on the graph buttons to change the graph type, and click the Areas, Groups, or Sites tabs for specific statistical reports about your network.
- As an administrator, you will be able to justify why and when you have to renew your AMF subscription license.



Rules

The **Rules** tab shows the assortment of rules you have deployed. These include Event log rules, Syslog Rules, and Link Utilization rules.



- Event Rules - Created from the event action menu in the event log table.
- Syslog Rules - Created from the syslog filter panel. Syslog Rules accept a combination of column filters and message to generate match criteria.
- Link Utilization Rules - Created from the traffic map layer by right-clicking a link that supports utilization and selecting **Create link utilization rule**.

To read more about the differentiation in rules, click the information icon by the Rules tab.

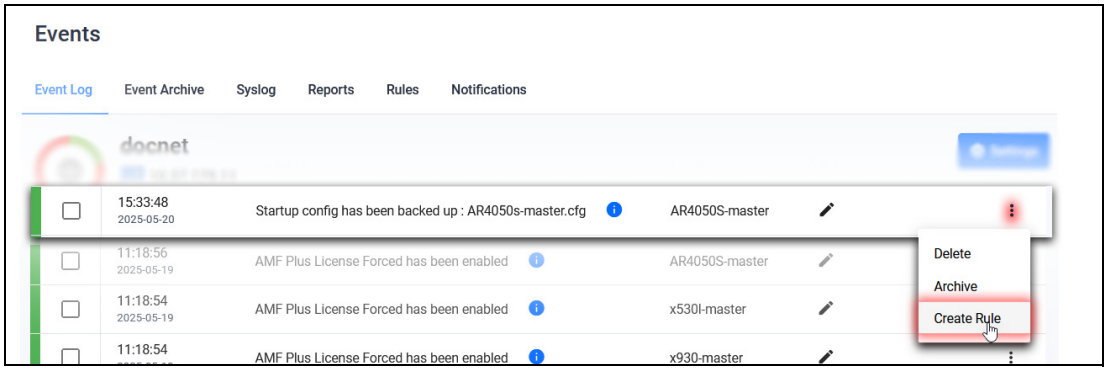
How to create Event log rules

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

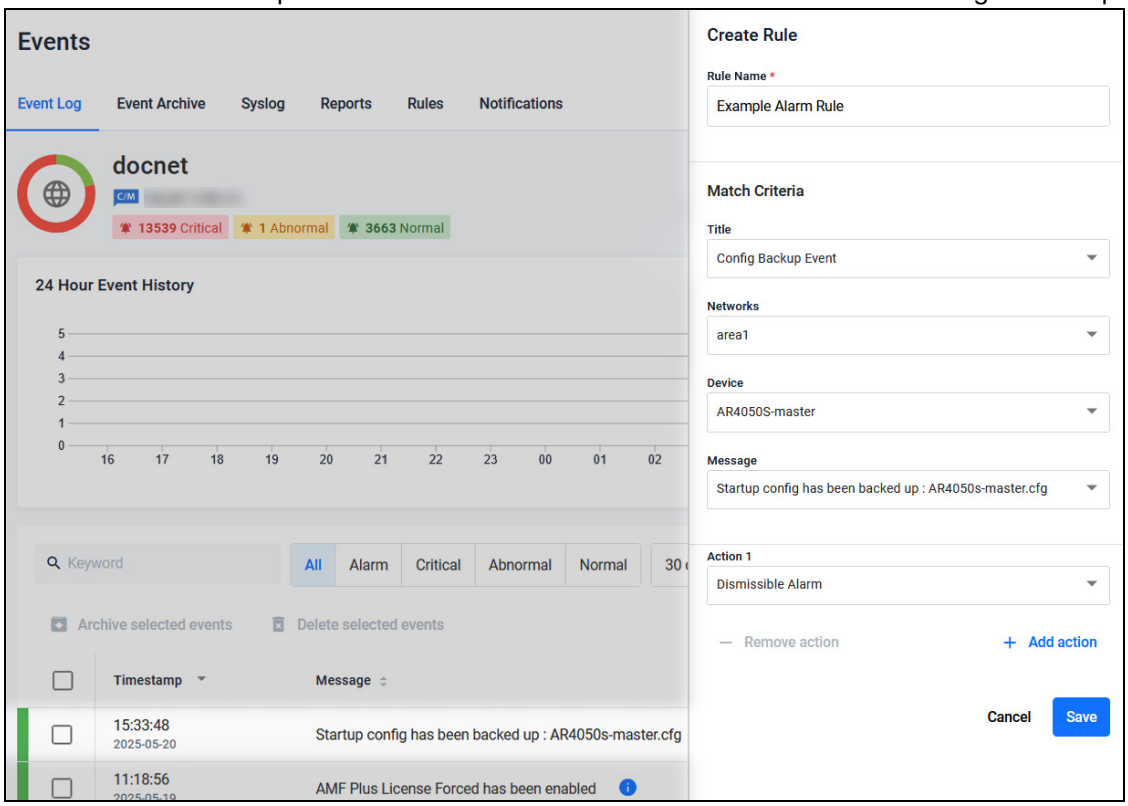
Note: We recommend using the **title field** instead of the message field when creating event rules so you can receive broader search results when searching for events.

To create an event log rule:

1. From the left-hand menu, navigate to **Events.**
2. From the **Event Log** tab, scroll down and 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**.



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



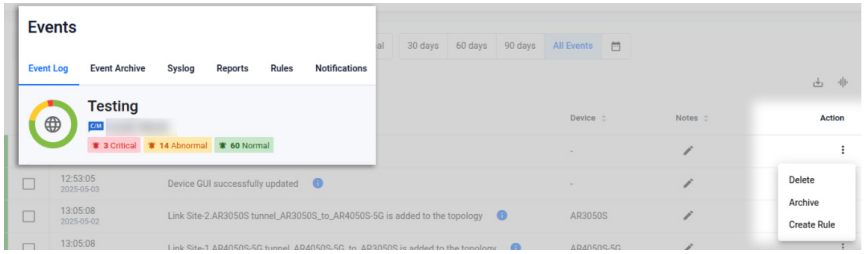
- Enter a rule name.
- Select **any** criteria to match on anything.
- Select an **Action**: Email Notification, Dismissible Alarm, or No Action.

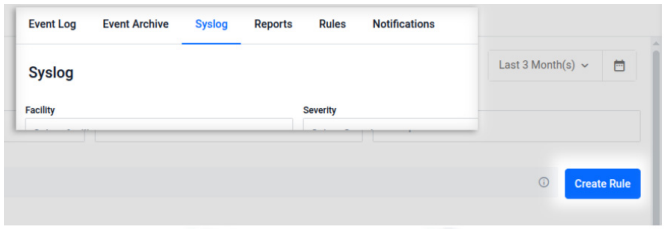
6. Click **Save**. You can use the **Rules** tab to view, edit, or delete existing rules.

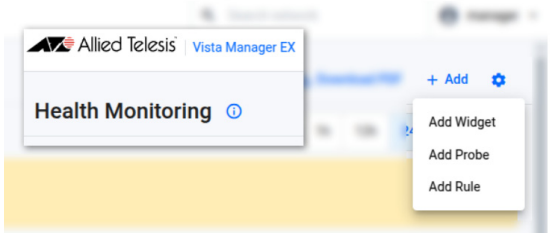
An SMTP server is required for email notifications to be sent. You can configure users' email addresses in the **User Management** window.

You can create rules from the Events > Syslog page, main Event Log page, or from the Health Monitoring page. To create a new rule on the:

- Events page - click the three dots next to an event log entry.
- Syslog page - click the Create Rule button.
- Health Monitoring page - click the + Add button and add a new Rule.



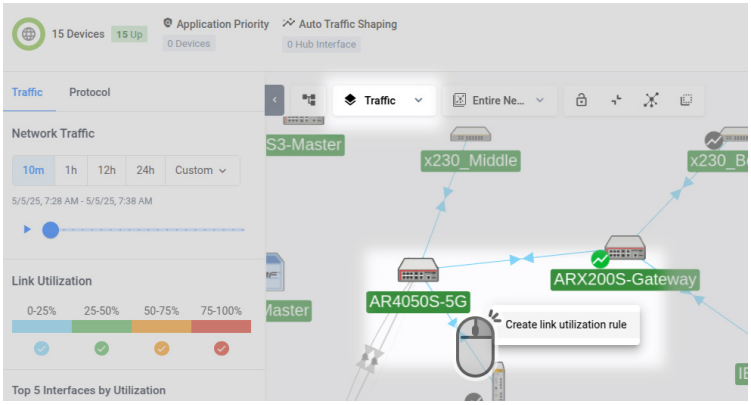




You can place an alarm on an event rule to identify it as a critical event.

- 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.

You can also create a link utilization rule from the Traffic layer of the Network map by right clicking a blue link.



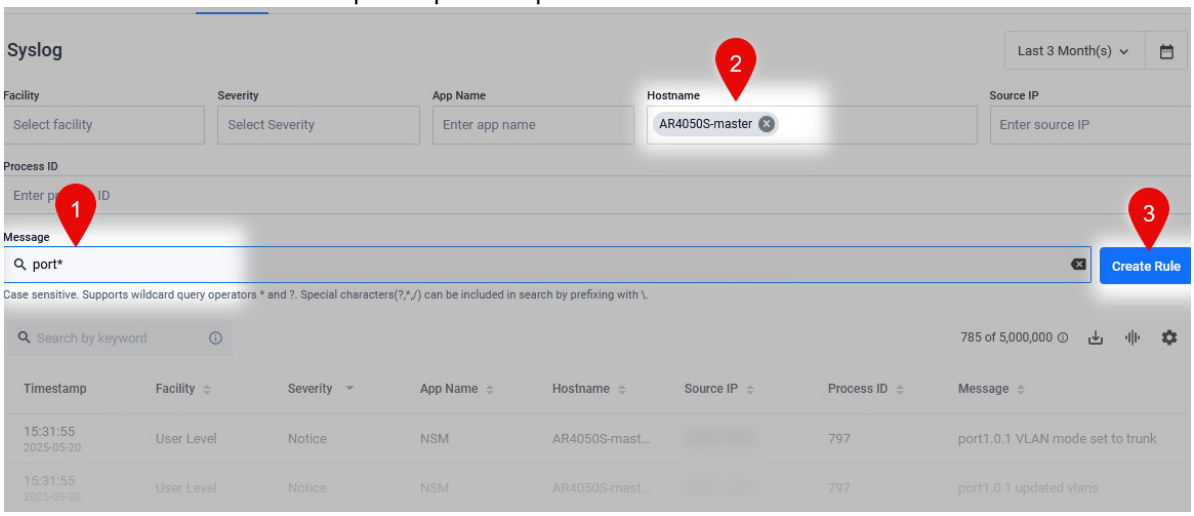
How to create Syslog rules

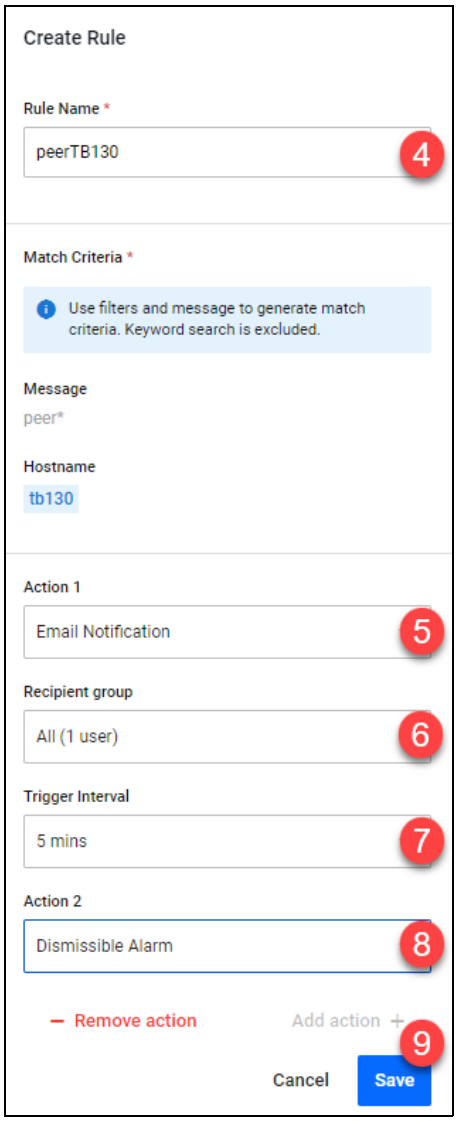
Syslog rules work similarly as the existing event rules. Any received syslog that matches a rule will trigger the action associated with the rule. Create a syslog rule based on the syslog message filter from the syslog tab page. When creating a single rule, configure up to two of the following actions:

- email notification
- dismissible alarm
- no action

To create a syslog rule:

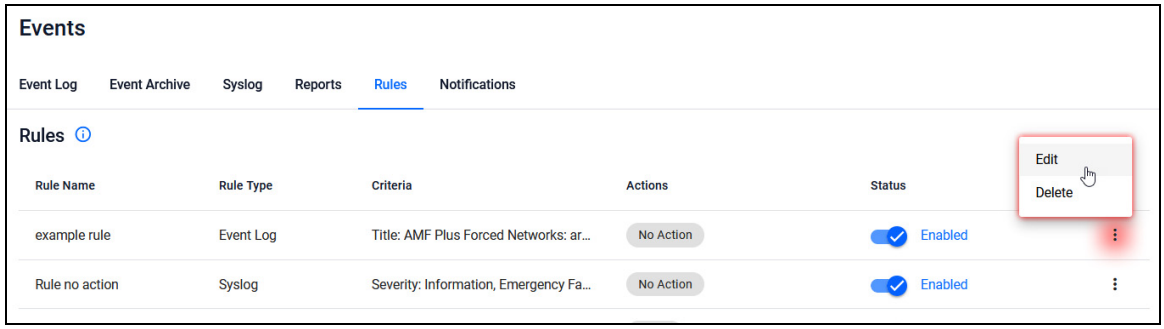
1. Use the syslog message filtering to search for messages of your choice.
2. Next, select a hostname.
3. Click **Create Rule**. This opens up a side panel.





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**.

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



How to create Link Utilization rules

You can configure link utilization rules from the Traffic map. For more information on how to configure this, see "Creating link utilization rules" on page 87.

Setting up third-party notifications

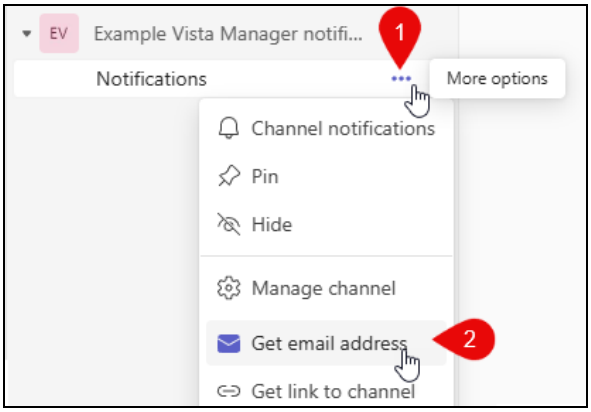
From version 3.14.0 onwards, you can configure Vista Manager to send you notifications about your network to third-party communication applications including Microsoft Teams and Slack, with the introduction of recipient groups.

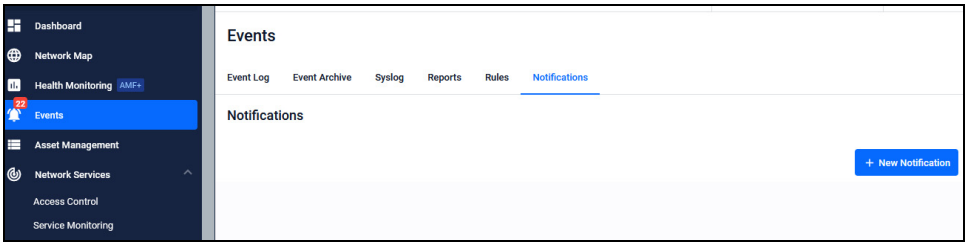
You can select a recipient group from the recipient group section of the event rules drop down. You can create a recipient group with a name and a set of email addresses from the Events > Notification page.

A recipient group is treated as a user that has permissions for all events. It is up to the admin creating the event rule to decide which notifications the group receives.

To get an email for a Teams channel:

1. Click the three dots next to the channel you wish to send notifications to.
2. Click **Get email address**. Teams will generate an email address.
3. Copy the email address in the middle of the generated string between the <>

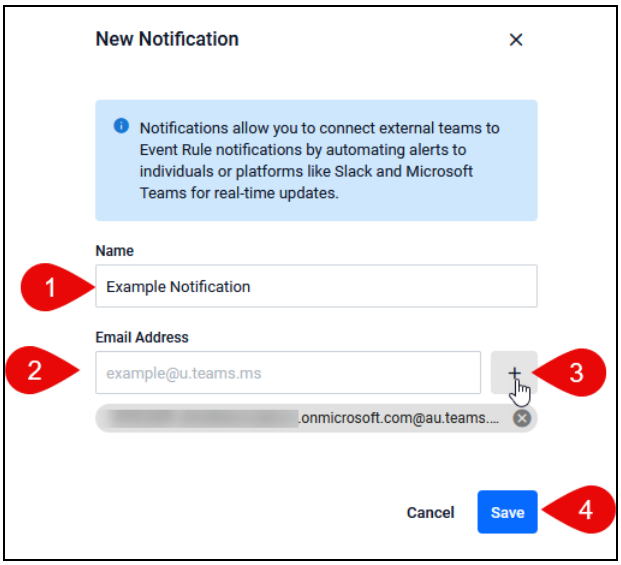




The Notifications tab on the Events page has been added to support sending notifications from Vista Manager to other applications. Click the **+ New Notification** button to add a new entry.

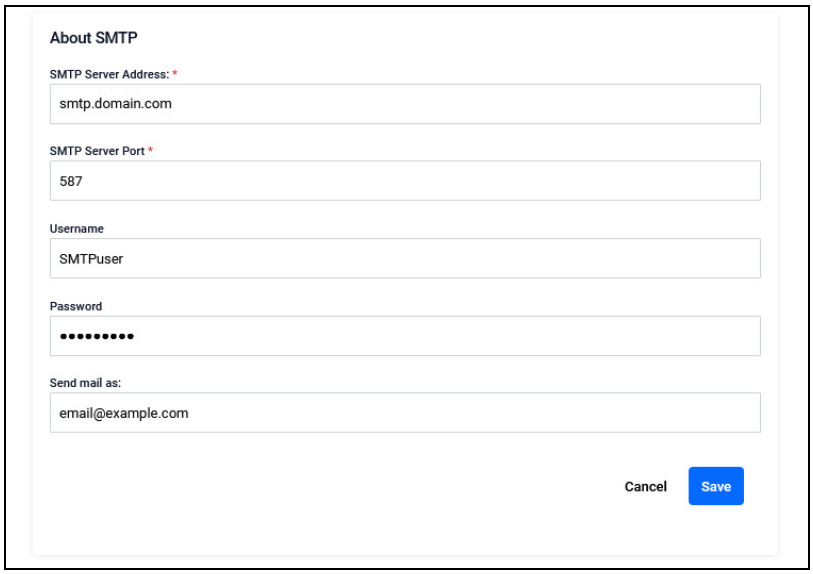
1. Enter a name.
2. Enter the email address from the communication channel.
3. Click the + button to confirm and add the email address.
4. Click save.

The new notification entry will be added to the Notifications page.

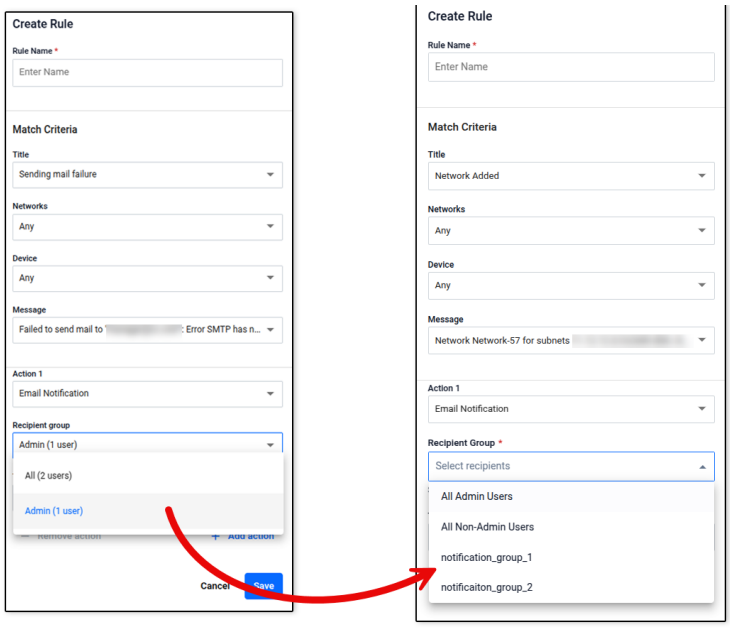


You must also set up SMTP Server settings to get notifications. The SMTP config handles encrypted SMTPS on port 465 and port 587. An SMTP Auth User and Password is required for the SMTP Server to forward information.

To change the SMTP settings, navigate to System Management > About and scroll down to the About SMTP section and click the ‘Edit details’ button.



In version 3.14.0 onwards, the recipient group option has been extended. When you create a rule, you can choose to send notifications to specific notification groups.



AMF Security (AMF-Sec) support

The 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.

You can 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.”**

AMF-Sec Alarms

Vista Manager EX will convert specific actions that match AMF-Sec syslog messages into alarms (high severity event logs) and display them on the map. These specific blacklist and whitelist 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 you associate one AMF-Sec syslog message with multiple devices, then 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 plugin. 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 plugin 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**.

Auto-dismissed Alarms

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.

AMF-Sec 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 Trap Events

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

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

Asset Management

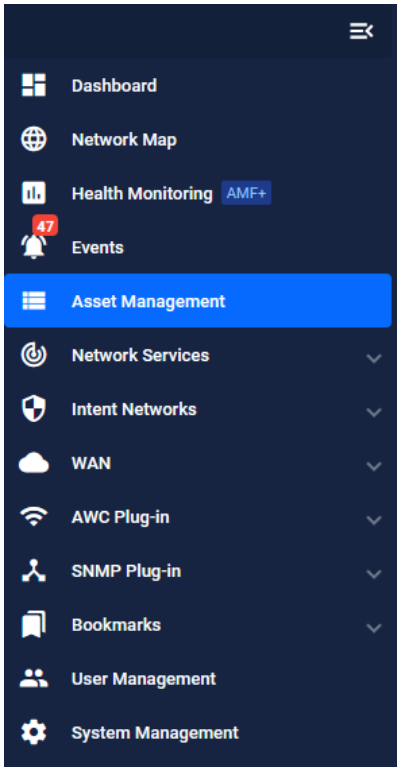
You can use the Asset Management screen to manage the assets in your network. It is made up of several components. You can view devices and groups from this screen.

- **Device discovery** - devices on the network are discovered via AMF and plugins.
- **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, including those that have connected to the network and subsequently left in the last 1.5 years.
- display the assets on the network 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.

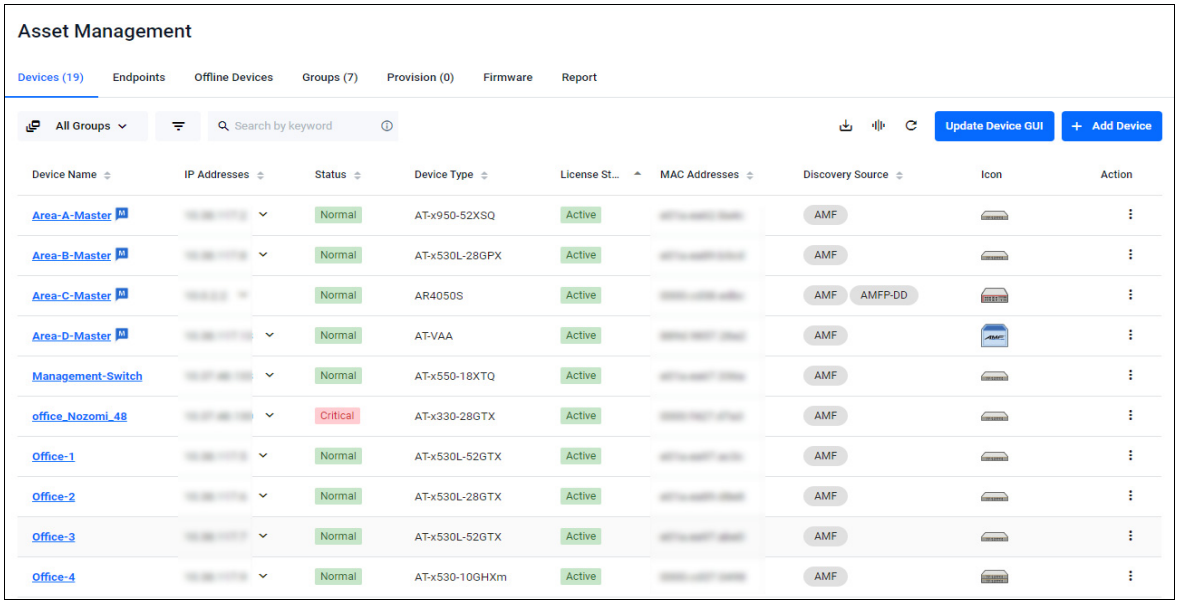
Asset Management is accessed from the sidebar menu.



Devices

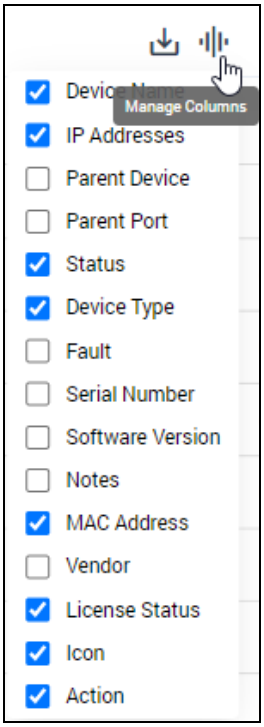
Device list

The **Asset Management** screen shows you the devices in your network, including their details. It also allows you to search for particular devices. You can re-order any of these columns by clicking and dragging the column title. The changes are saved and reset after login/logout.



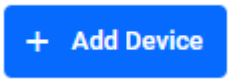
- Click on the **Export as CSV** icon at the top right corner to download a CSV file list of assets.

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

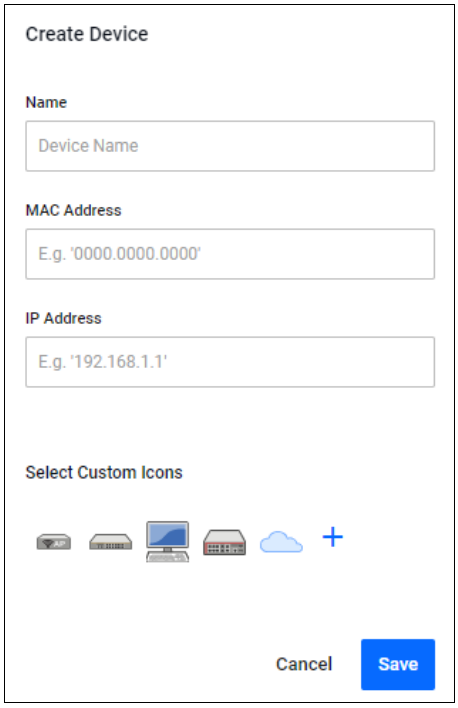


Updating the device list

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

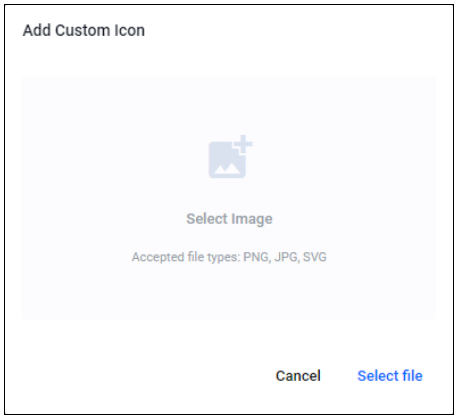


When you add a new device, you will be prompted to name the device, as well as specify the MAC address and IP address. You can also select an icon to represent the device.

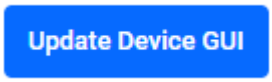


Click on the '**+**' button, to upload a custom icon for the device. The custom icon dialog supports PNG, JPG, and SVG image files.

Note: Only administrators have the permission to upload and change custom icons. An AMF device cannot have its default icon changed.



- You can update a device's GUI by clicking the **Update Device GUI** button.



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

Vista Manager uses address resolution protocol (ARP) to discover any new devices, and return a list to you. A message appears indicating the number of new devices found. Detected devices that fall into a user defined inventory group inherit the assigned custom icon.

Note: Discover devices will only discover IPv4 neighbours.

Any detected devices will not automatically appear on the map or show link information and will require you to add devices and links to the map manually once they have been discovered. See "Edit map layer" on page 102 for more information on how to display the devices on the map and create links.

STOAT Device Discovery

STOAT (Standardized Topology Organizer and Transport) is a feature that is responsible for discovering devices and network topology. AMF Plus Device Discovery supports STOAT as a topology data source. Devices and links discovered by STOAT will be added to Vista Manager EX's database, allowing them to be displayed on the Network Map and included in the Asset Management table.

It organizes device and topology information into a standardized format. Devices that are a part of the STOAT process are configured as collectors or sources using LLDP protocol.

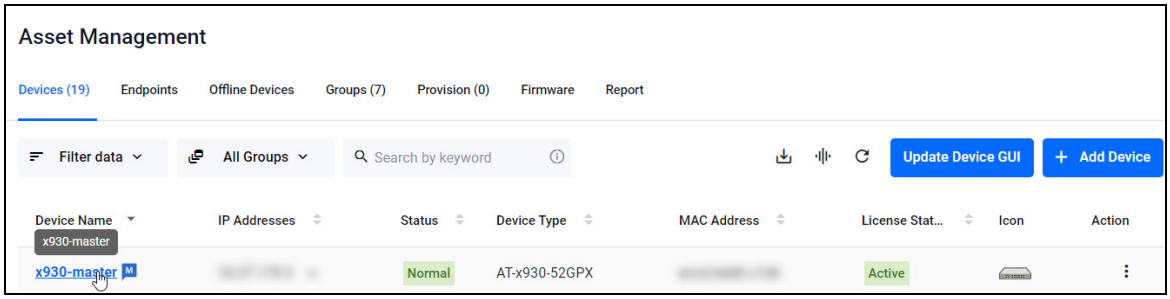
The following titles are referred to during the STOAT process:

- **Device** - a network node that has no STOAT role but is LLDP capable.
- **Source** - compiles data about itself and the nodes it can discover with LLPD and streams it to the collector.
- **Collector** - collects and stores data about itself and discovered devices.

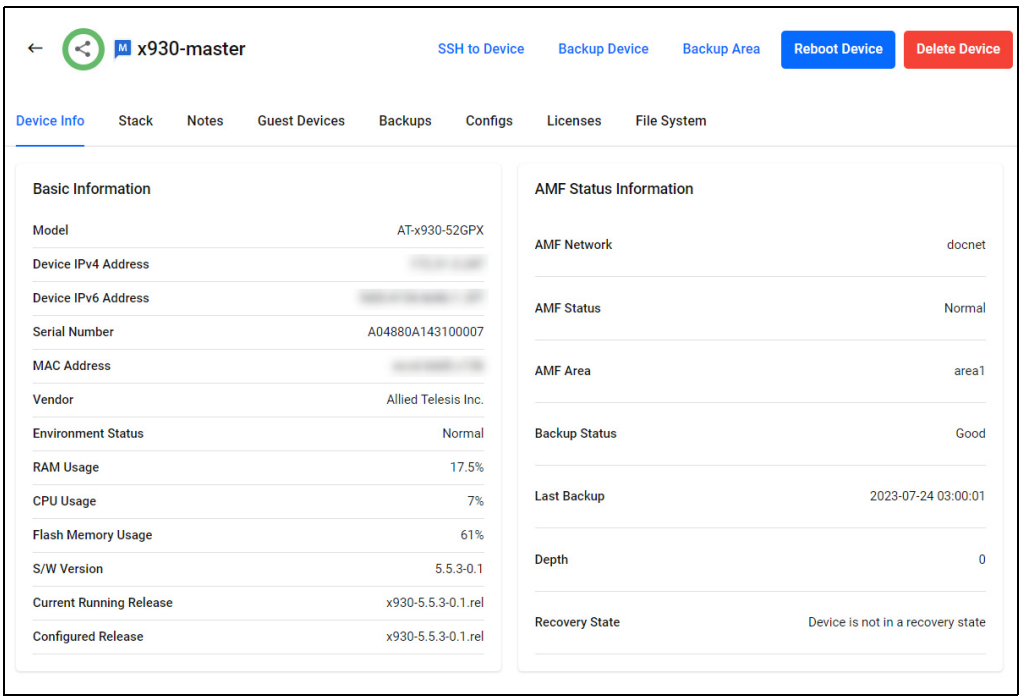
For more information about how to configure STOAT devices, see the Device Discovery using STOAT Feature Overview Guide.

Accessing device details

You can click on the device name to access the device's information page.

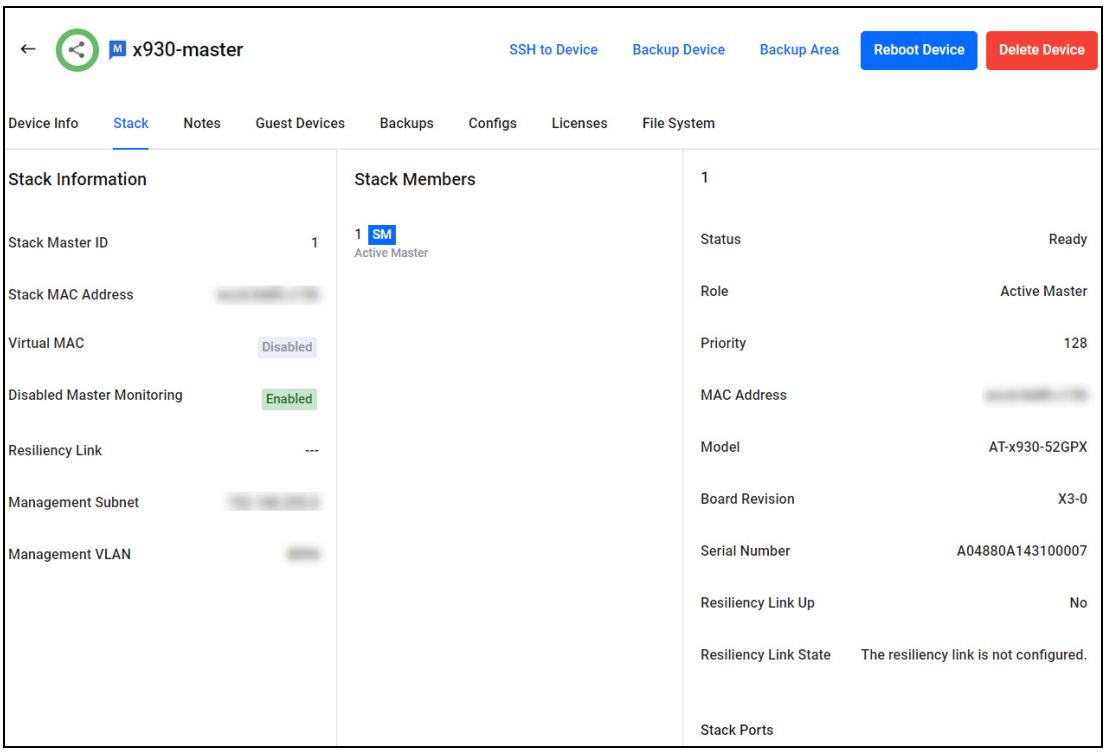


This will bring up the **Device Info** page for the specific device you have selected. You can see information and configure a variety of settings relating to your device from this page.



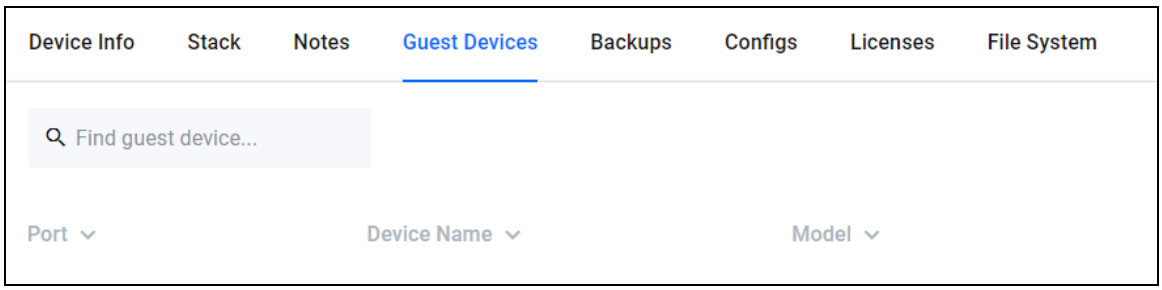
Stack Information

The Stack tab shows stack information for the device.



Guest Devices

Guest Devices that are connected to your device are shown here.



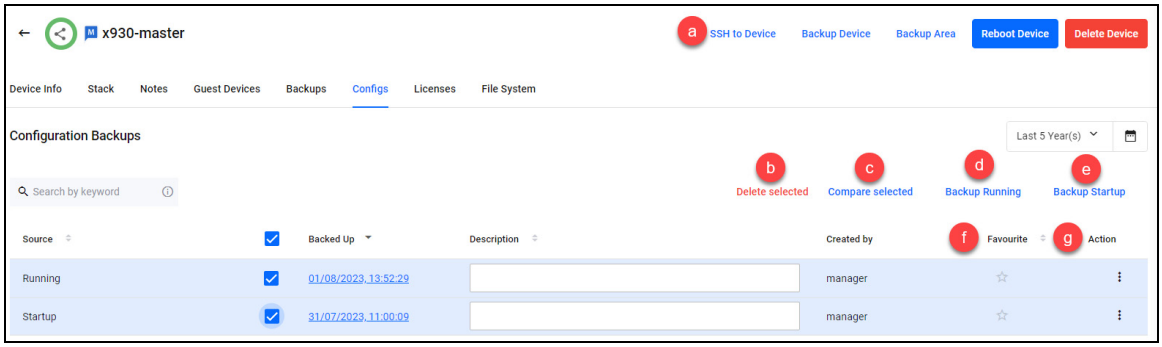
Backups

The Backups tab is shown when you select an AMF Plus Master or Controller device. This section specifically controls the AMF backups. Note that using Vista Manager, you cannot initiate a backup from a member node, this is only for AMF Master or Controller devices.

For more information about AMF Plus, "Using AMF Plus Features" on page 218, as well as the AMF Plus Feature Overview and Configuration Guide.

Configs

Clicking on **Configs** leads you to the Configuration Backups menu. In this menu, you can back up both running and startup configurations.



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

You can:

a. SSH to a device

b. delete a selected configuration

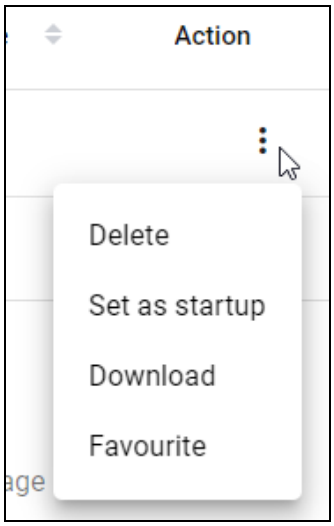
c. compare two selected configuration files

d. back-up a running configuration file

e. back-up a startup configuration file

f. set favorite configuration files

g. perform actions from the Action menu



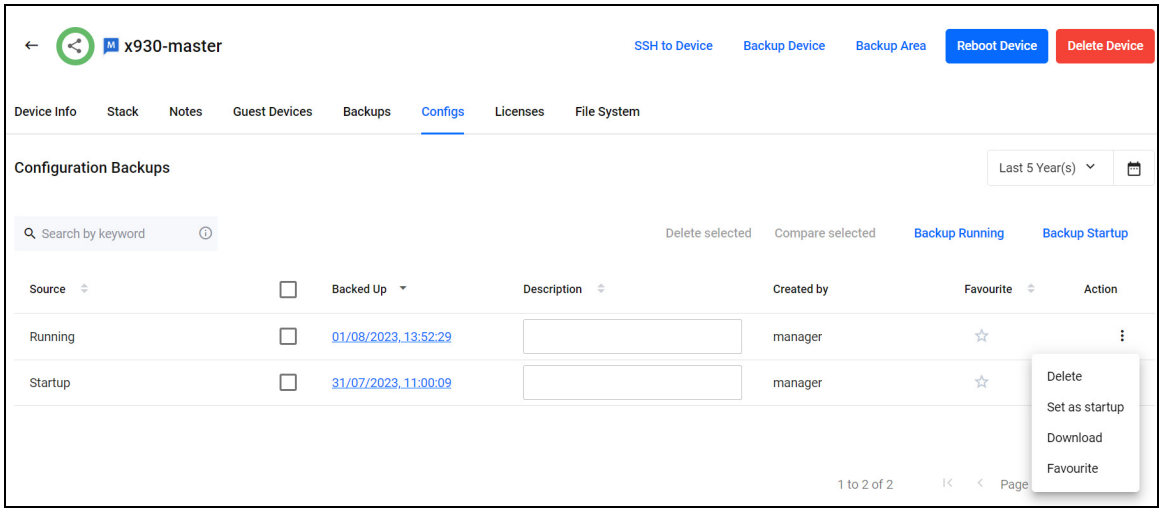
You can perform specific actions on one file from the Action menu:

- delete a configuration
- set a configuration as start-up
- download a configuration
- favourite a configuration

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

How to backup a device configuration and set at startup

Backing up your configurations is an important procedure that helps to prevent issues in your network. This is helpful if you would like to go back to a previous configuration.



On the **Configs** tab of the device you wish to update, click the **Backup Configuration** button.

1. A notification on successful backup will appear.
2. Type a brief description in the Description textbox. Click outside the textbox to save.
3. You can click on the Action drop-down to set a config backup that you wish to set as startup.

A reboot is 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.

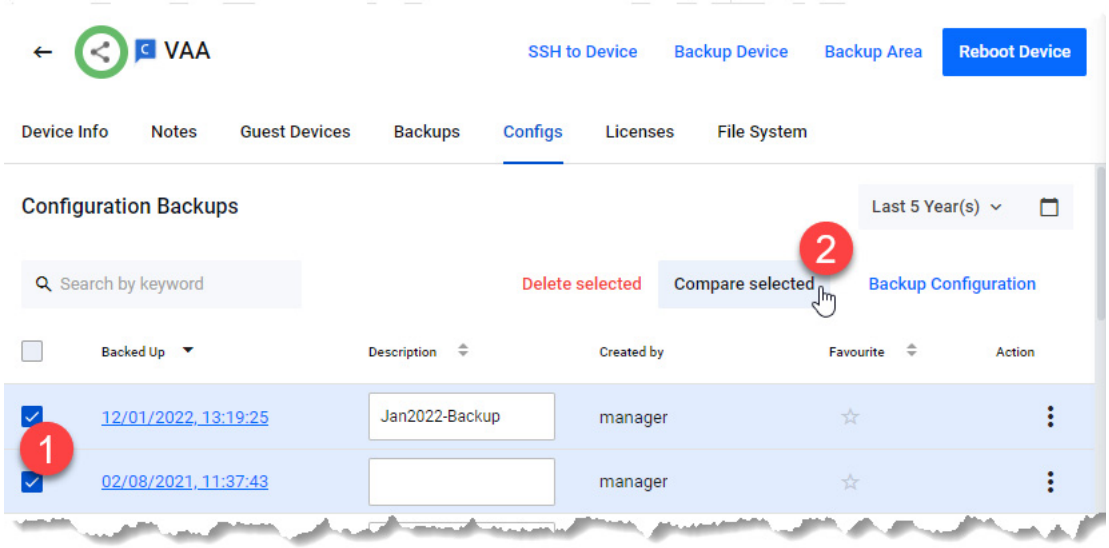
Restoring a config overwrites the contents of the current startup-config only. The original file-name and location of the backup config will not be used during the restore.

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

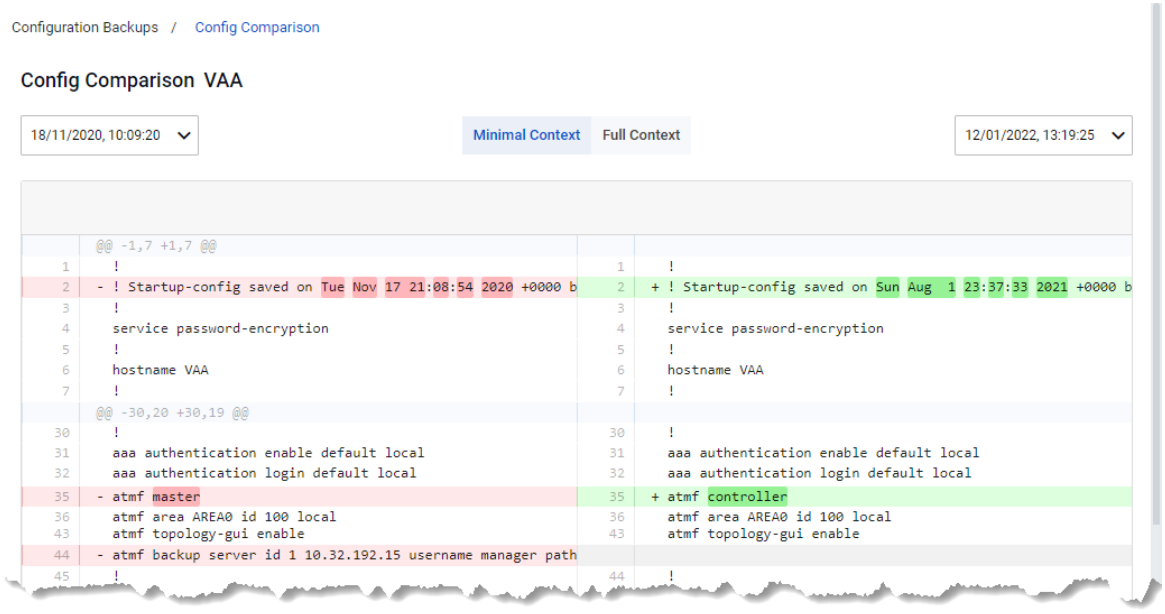
Comparing configuration files

You are able to compare device configuration files if you wish through the device's configs tab. This helps you make a more informed decision about the changes being written to your device. You can also compare running config and start-up config. To do this:

1. If you want to compare the current running config with another config file, make a backup of the current running config.
2. Click on the check box on the left-hand side of each configuration file you wish to compare. Select up to two files.
3. Click on the **Compare selected** button.

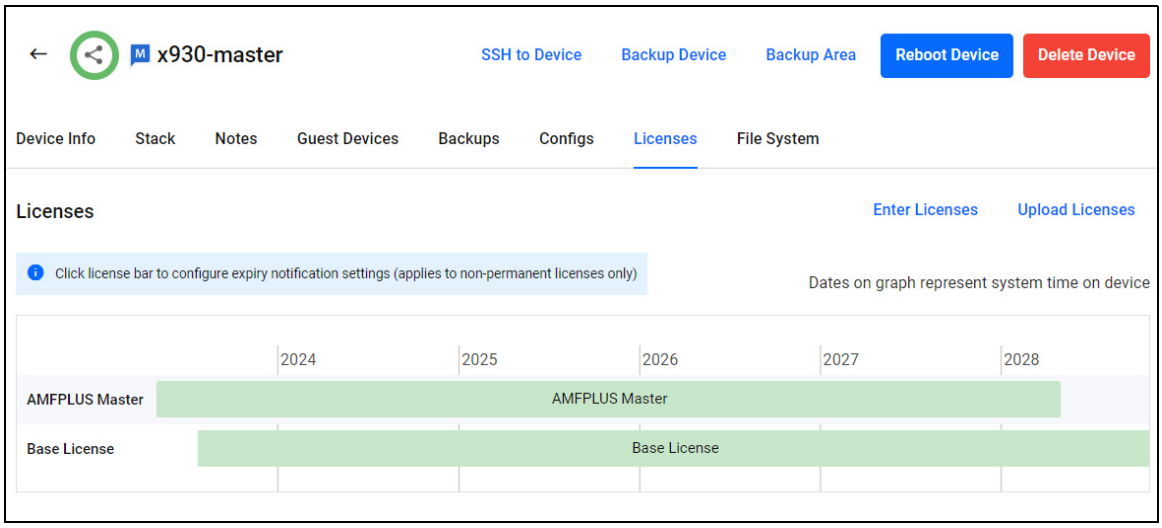


When comparing two configuration files, the tool displays differences in full, or just five lines of either side, highlighting differences in bold and in color. Toggle between settings using the **Minimal** and **Full** buttons.



Licenses

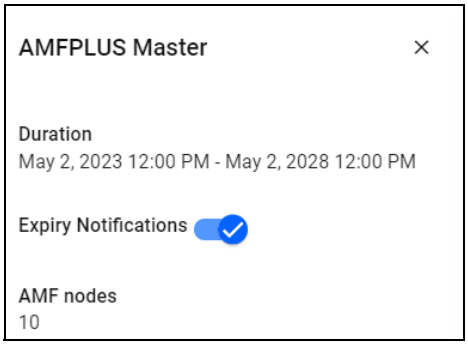
The Licenses tab displays all device licenses and their duration in a graph. You can add and examine licenses on an AMF device from the **Licenses** tab.



Note that this is different to the System Management Licenses tab, which shows all of the licenses on Vista Manager. For information about the System Management Licenses page see "System Management" on page 310.

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.

More license information and notifications



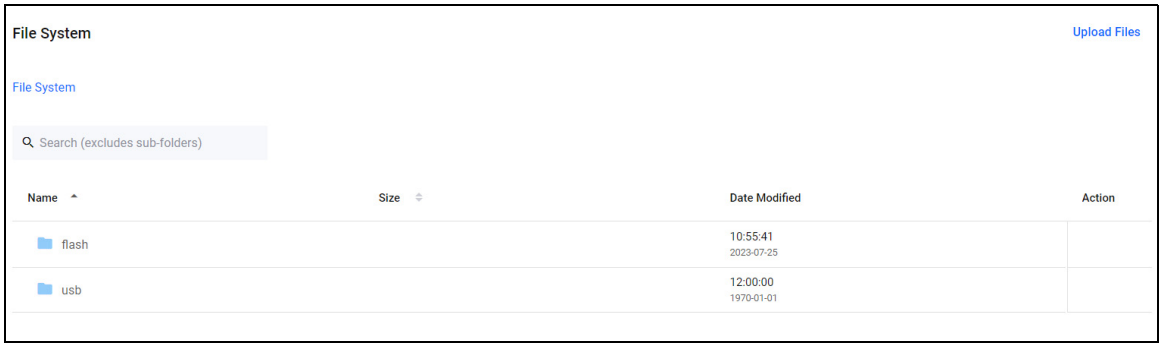
Click on a license bar to display a pop-up panel on the left with additional information about that license.

You can turn off expiry notifications. By default, all license expiry notifications are set to enabled. Click on a license bar that you wish to disable notifications for. A side panel will appear. A success message will pop up at the bottom of the side panel. A crossed-out bell will appear on the license bar if you disable notifications.

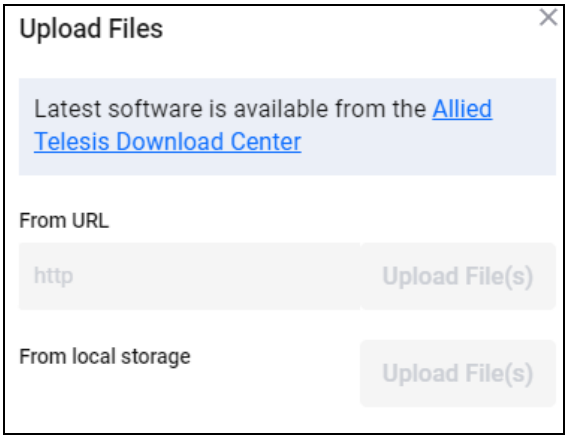
Note: This feature applies to non-permanent licenses only.

File System

The File System page provides a file directory with the software files that are stored on the selected device. This page allows your to upload software files to your device and browse folders stored on your device.



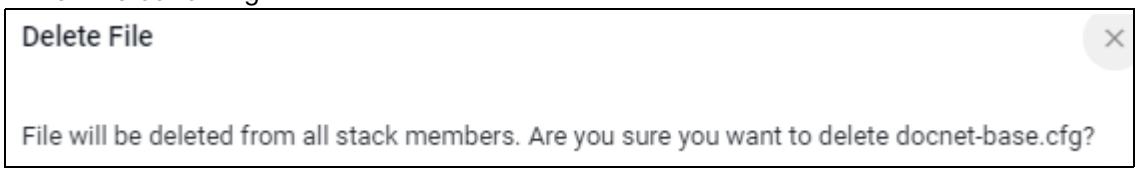
You can click on a folder name to view items in that folder.



You can to upload software by clicking the **Upload Files** button on the top right. This will show the Upload Files dialog, where you can upload software files from either a direct URL or from your device.

To delete a file:

1. Click **Delete** in the action column for the file(s) that you wish to delete.
2. A confirmation message appears. Click **Delete** to proceed. A success notification then appears on the bottom right.



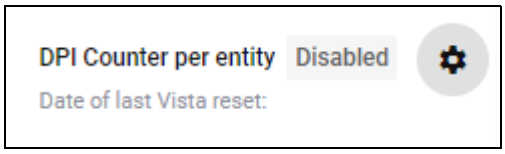
Note: File(s) selected for deletion on a stacked device will be deleted from all stack members.

There are some limitations to take note of:

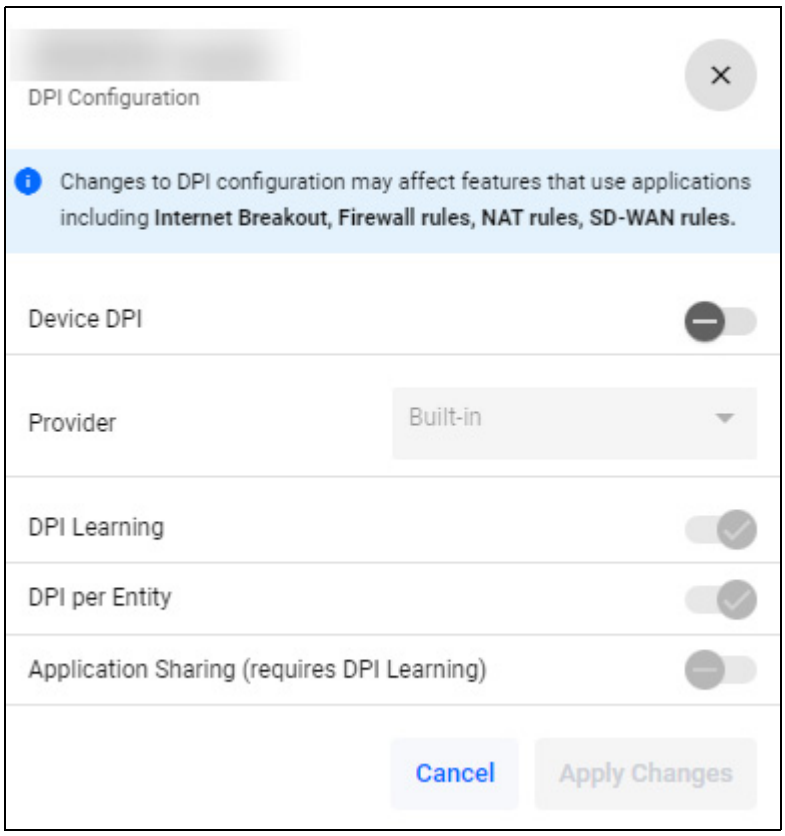
- Protected files cannot be deleted, this includes:
  - boot firmware release files
  - backup boot firmware release files
  - boot configuration files
  - backup boot configuration files
- Directories cannot be deleted.
- Wildcard characters (*) are not supported in the file search.

DPI per Entity

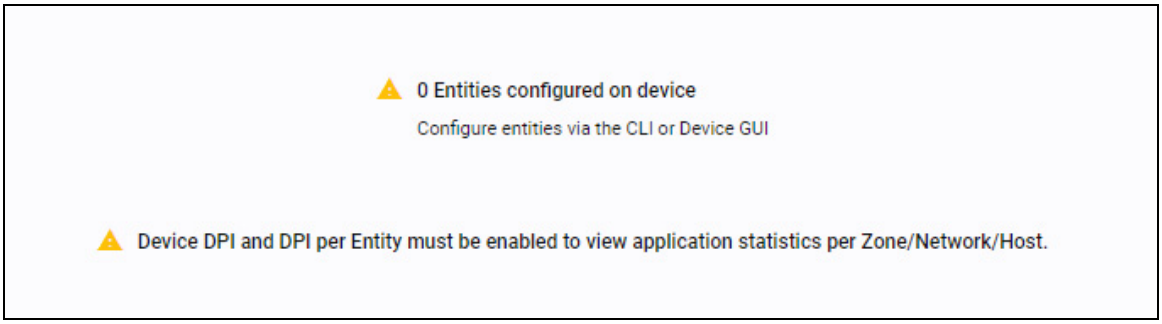
To view the DPI statistics, navigate to **Asset Management** and click on a device.

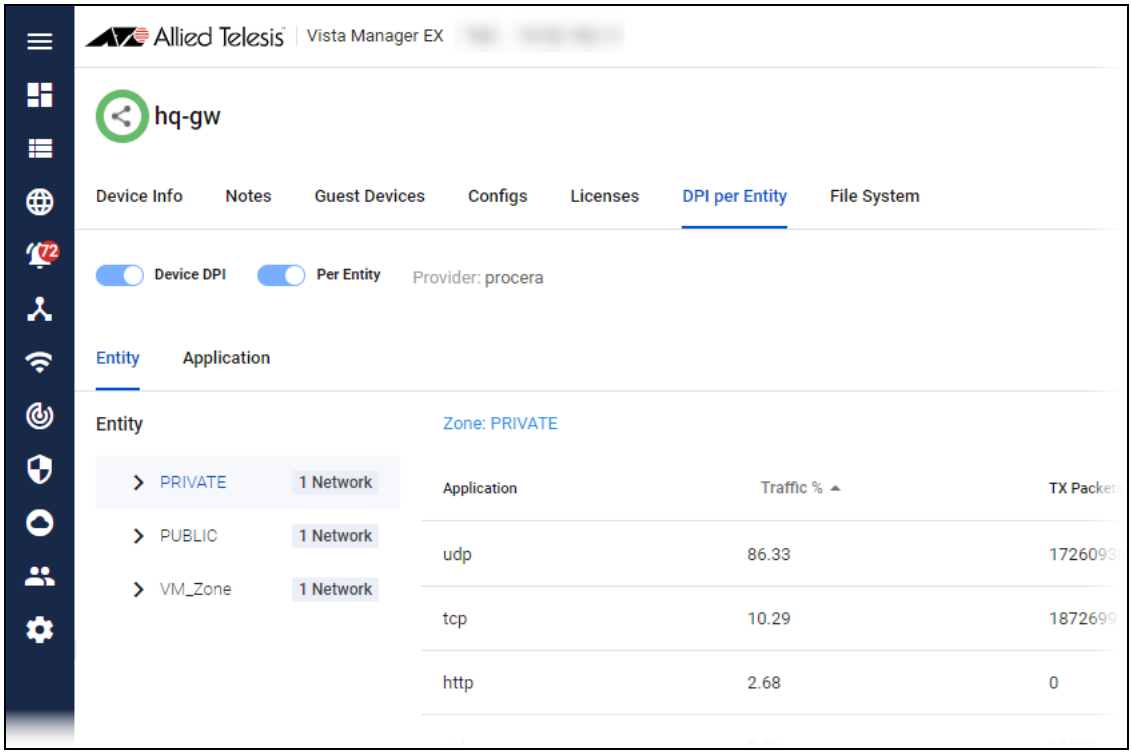


To enable DPI per Entity on devices, click the **cog icon** in the top right of the DPI per Entity screen. This will bring up the DPI Configuration window where you can toggle it on.



If no entities are configured on your device, then Vista Manager will show you a warning that none are configured. They can either be configured via the CLI or Device GUI. 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 percent of traffic at the top under the Traffic % heading. Clicking on a column sorts by that field. If there's an arrow to the left of the network name, you can drill down to see each host.

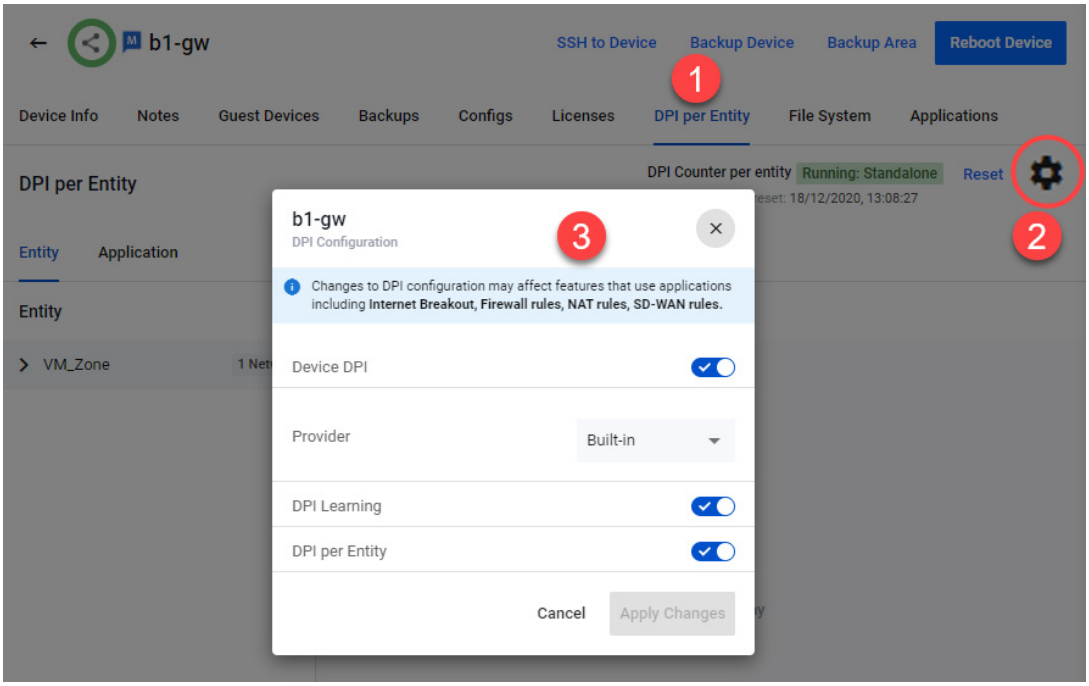
By clicking the Application tab, you can click on a particular application to see their stats. In the table, you can click on the zone to see the stats for networks, and drill down into a network and into hosts.

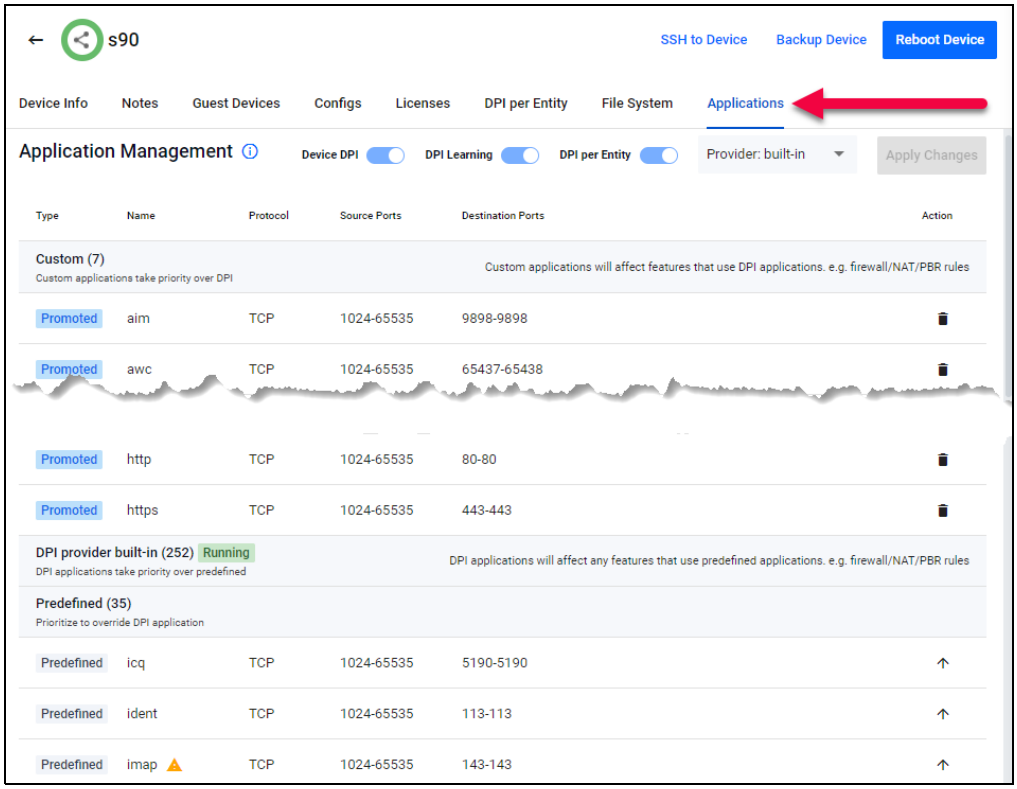
Application reconfiguration support

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.

To enable DPI:

1. Click on the DPI per Entity tab.
2. Click on the **Settings cog** icon.
3. This opens the **DPI Configuration** dialogue box.





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

Applications

You can click on the Applications tab to open the **Application Management** page.

The Applications tab is closely related to the SD-WAN feature. For more information see "WAN" on page 274. For further information, see the SD-WAN Feature Overview and Configuration Guide.

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.

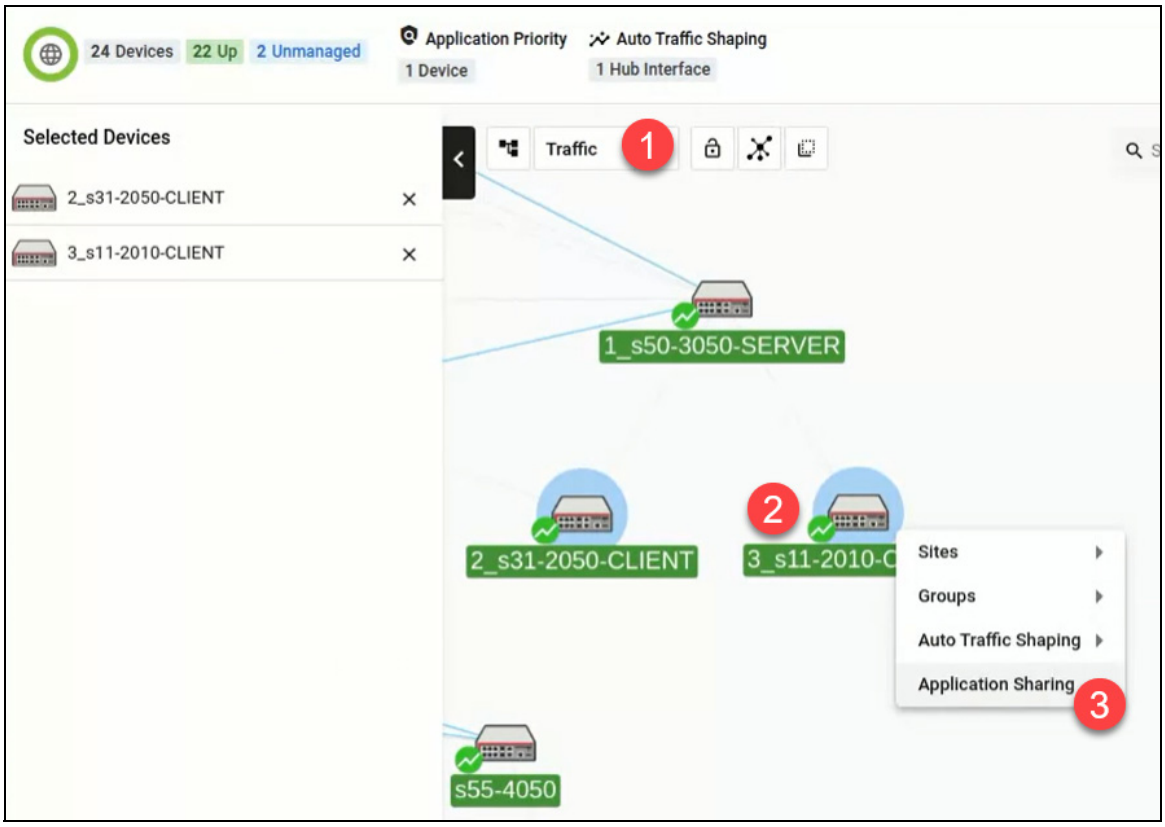
- **AR3050S**, **AR4050S,** and **ARX200** devices can be used as server devices that have advanced DPI engines available. This means that they can share their applications with other devices.
- **AR2010V**, **AR2050V,** and **TQ-R Series Routers** can be client devices. A server device sends these client devices the application data.

Note: This functionality requires AR-series devices to run AlliedWare Plus 5.5.1-1 or later.

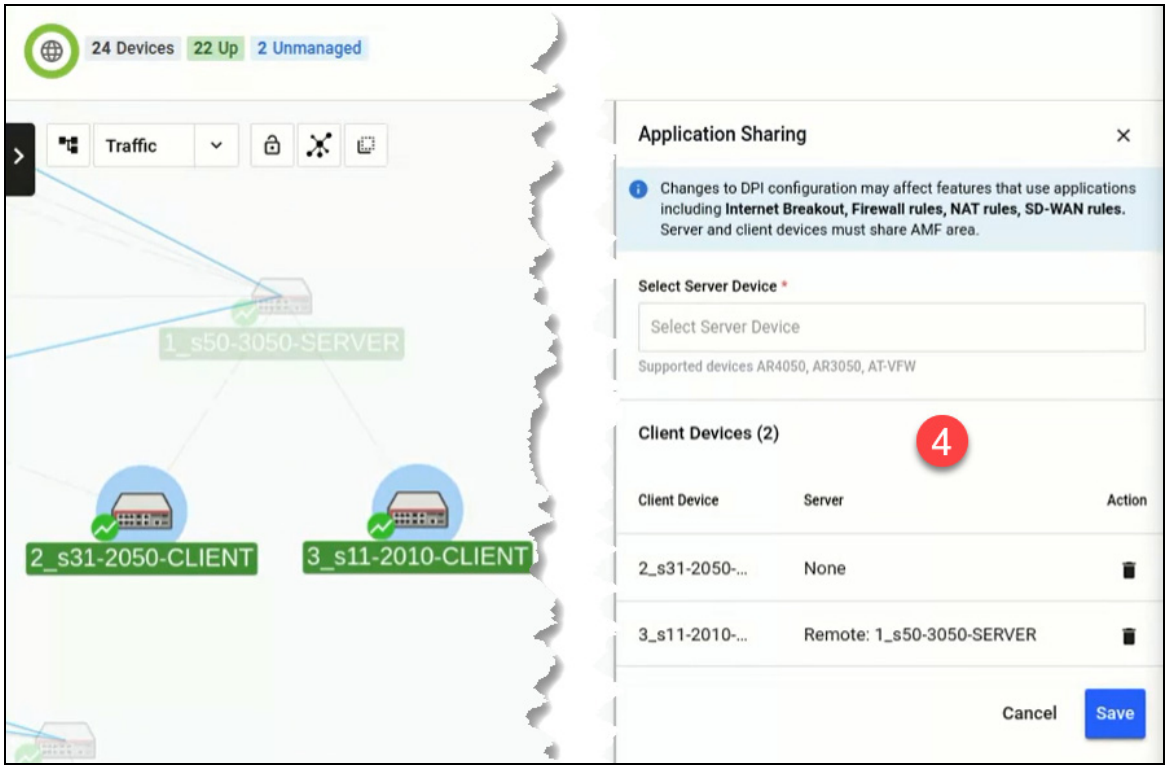
You can enable Application sharing in three different ways, see the following pages for more information on each method:

- "1: Enabling Application sharing via the Traffic map" on page 161
- "2: Enabling Application sharing via the Traffic map side panel" on page 163
- "3: Enabling Application sharing via the Device's Applications Tab" on page 164

1: Enabling Application sharing via the Traffic map

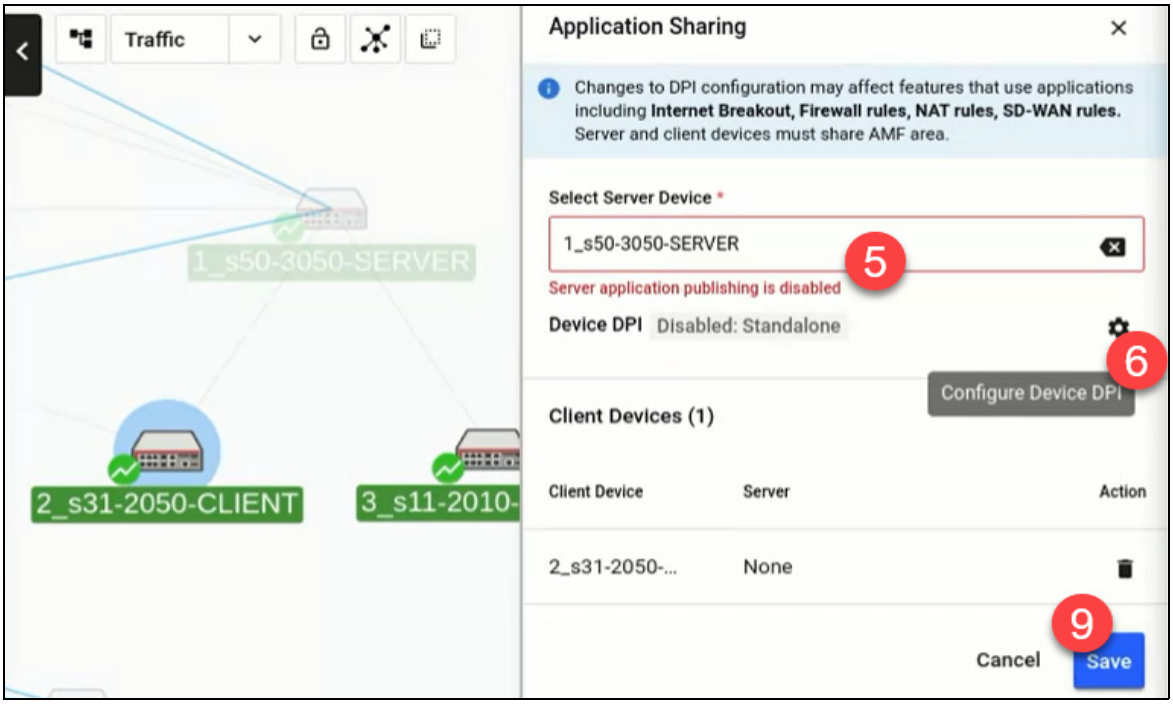


1. Navigate to the traffic map.
2. Select at least one client router.
3. Right-click on the selected router(s) and select **Application Sharing** from the menu.

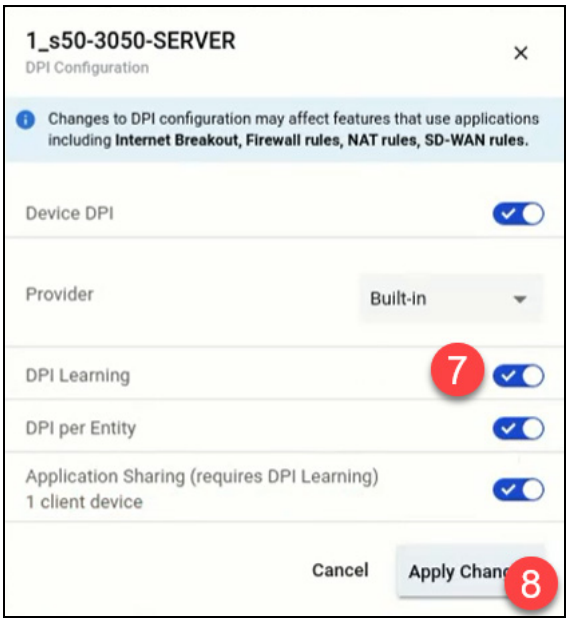


4. This opens up the Application Sharing side panel. You may remove or add more client devices here.

5. Next, select a server device from the drop-down list. Take note of the current DPI state of the server.



6. Click on the **Configure Device DPI** gear icon button if device DPI is disabled or to configure its settings.

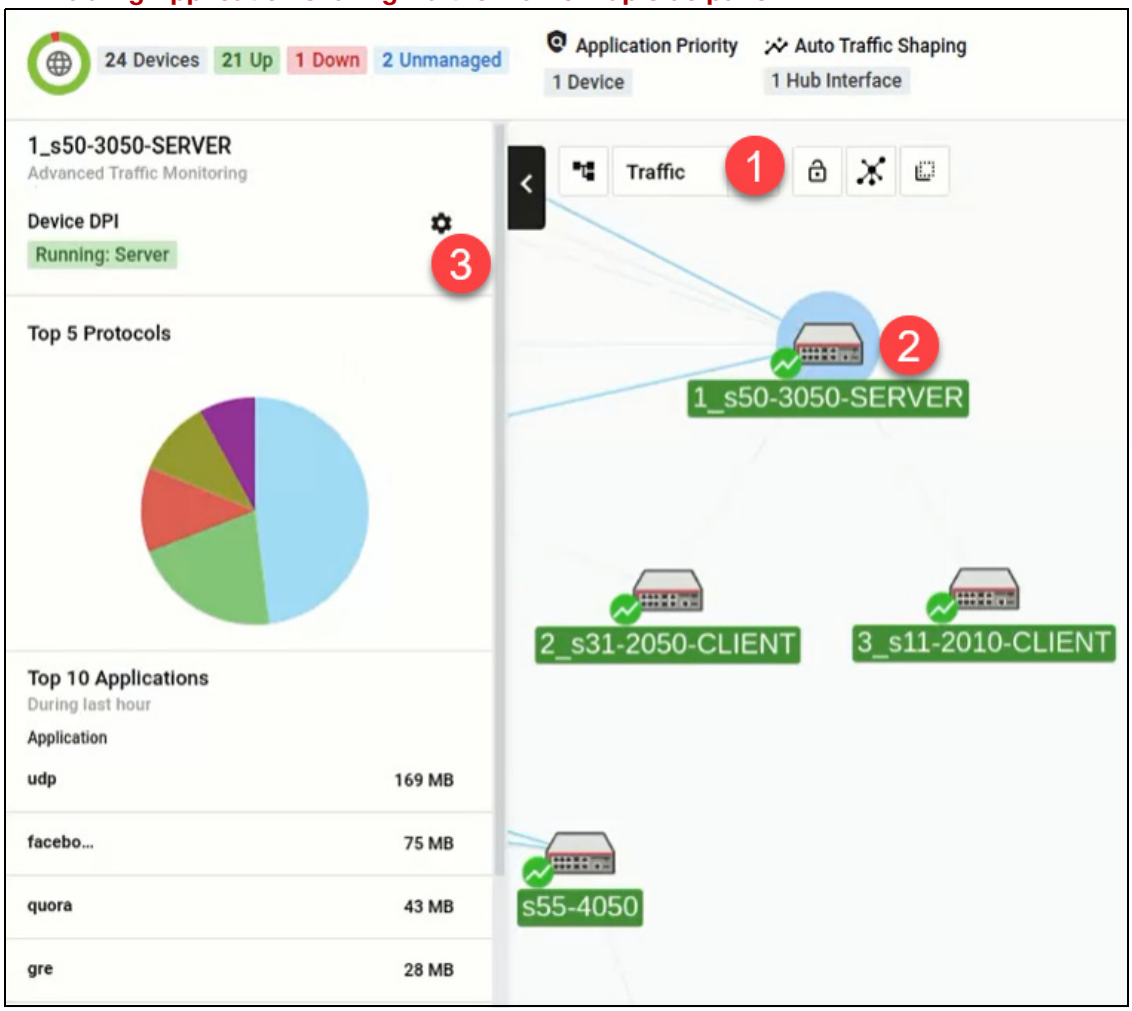


7. Turn on all settings to ensure a successful application sharing setup.

8. Click **Apply Changes**. This will close the DPI Configuration window.

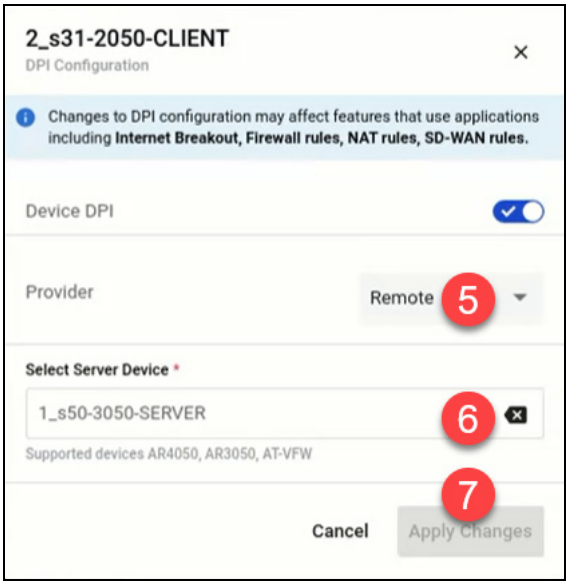
9. Finally, click **Save** to confirm the changes on the side panel.

2: Enabling Application sharing via the Traffic map side panel



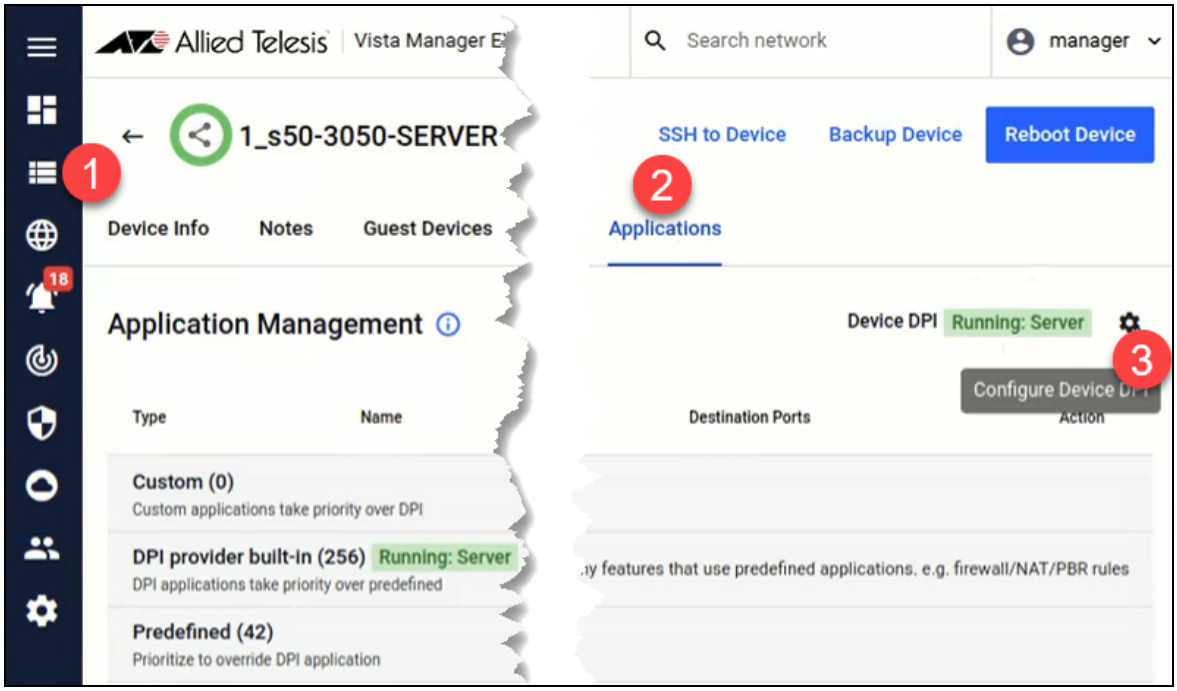
1. Navigate to the traffic map.
2. Select a supported server/client device. This opens up the Traffic side panel.
3. Click on the **Device DPI** gear icon button if device DPI is disabled or to configure its settings.
4. If a server device was selected, carry out **Steps 7-8 in Option 1**.

5. If a client device was selected, fewer DPI settings will be displayed. Select a **Remote** provider to choose a server next.



6. Select a server from the drop-down list.
7. Click **Apply Changes**.

3: Enabling Application sharing via the Device's Applications Tab

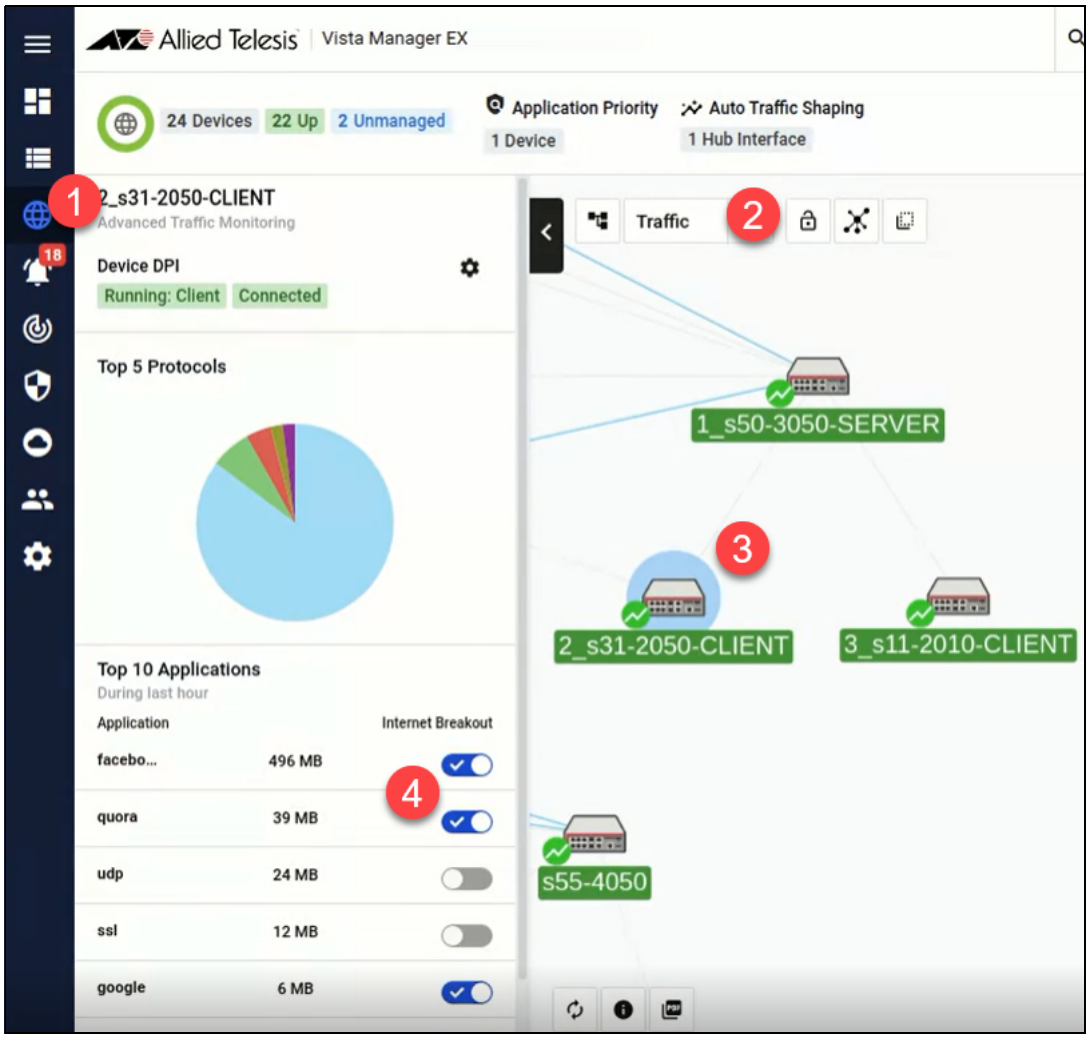


1. Navigate to **Asset Management**. Select a supported device from the list.
2. Next, go to the **Applications** tab of that device.
3. Click on the **Configure Device DPI** gear icon button if device DPI is disabled or to configure its settings.
4. If a server device was selected, carry out **Steps 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.

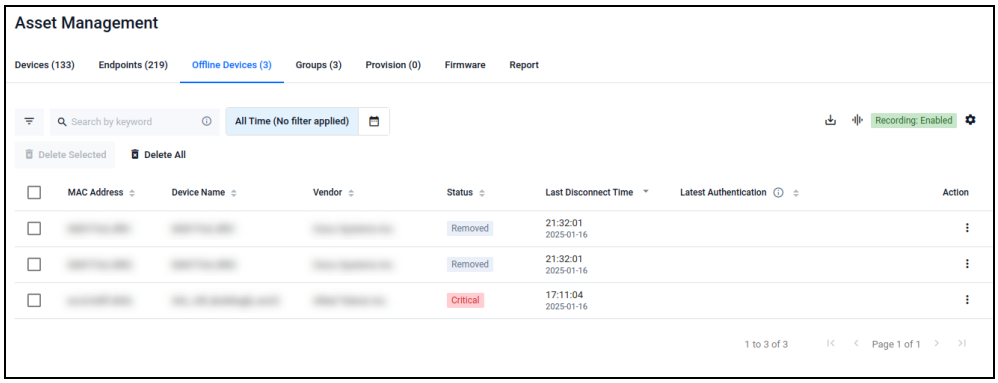
1. Navigate to the network map.
2. Select Traffic map mode.
3. Select a client device that you wish to enable Internet Breakout for.
4. On the Traffic side panel that launches, enable Internet Breakout accordingly.



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.

Offline Devices

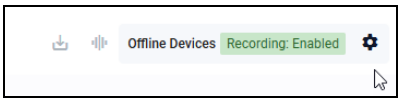
From version 3.13.1 onwards, the Offline Devices tab has been added to the Asset Management page. Note that this feature is disabled by default.

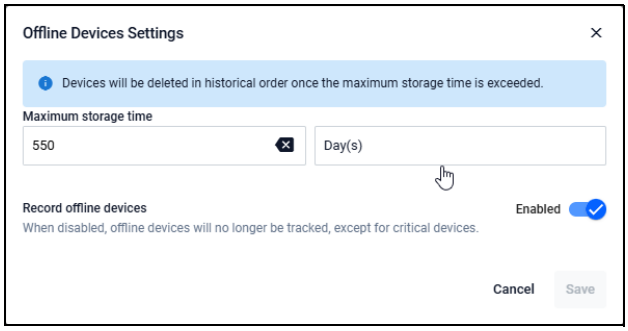


The **Offline Devices** tab lets you see all devices that have connected to the network and then left within the last 1.5 years. This feature helps you keep track of all assets that are or have been in your network, making it a useful audit tool. You can also generate a CSV file with this information. It is sorted with the most recently left device at the top.

- You can search devices by typing a MAC Address, Device Name, Vendor, or Device Type in the search field.
- You can change the table display using the Manage Columns, Filter Data, and Delete options. The table is sorted with the most recently left device at the top.
- Filter the Offline Devices tab by the last disconnect time by using the new **Asset Management** > **Offline Devices** > **Time Range Picker**.

Configure the Maximum offline device storage time within the range of 1 day to 2 years (731 days) by clicking the **Settings Cog**.





- Download a CSV file with all devices listed within the specified maximum storage time range. Click on the **Download CSV** button on the Offline Devices table.

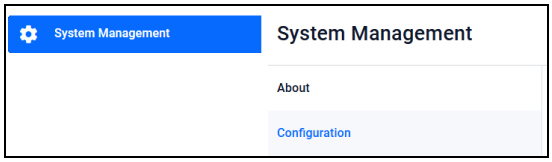
- To see all devices that are currently part of my network, use the existing **Asset Management** > **Devices** table.
- You can export a PDF of the list by clicking the Download button.

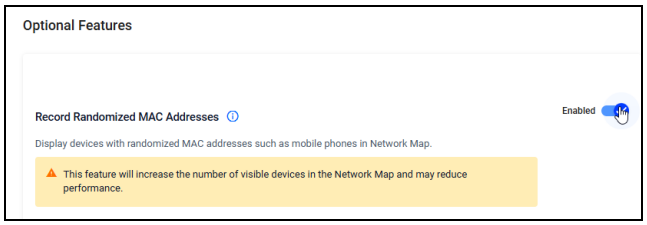
Note: When the feature is disabled, all existing data remains, but new data is not collected. Once the feature is enabled again, data collection resumes. However, devices that go offline while the feature is disabled will not be shown in the table.

Recording Randomized MAC Addresses feature

You can choose whether or not to record devices with randomized MAC addresses.

You can enable or disable the Record Randomized MAC Addresses feature from the **System Management** > **Configuration** page. This feature is disabled by default.



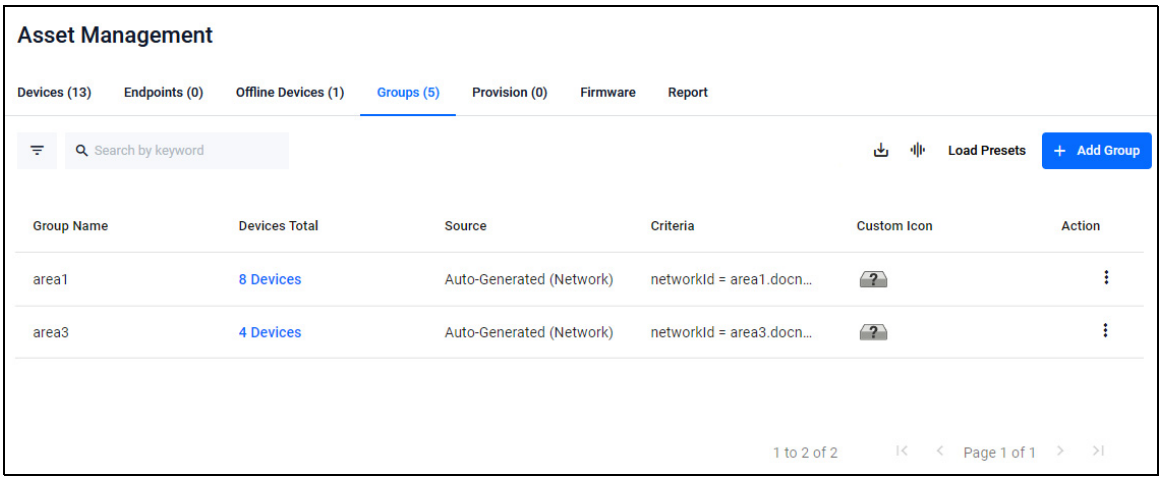


If you enable the Record Randomized MAC Addresses feature, and later decide there are now too many endpoints on the Network Map and Asset Management pages, you can remove the endpoints by disabling the Record Randomized MAC Addresses feature.

Note: It may take several minutes for this change to appear. When you disable the Record Randomized MAC Addresses feature, the previously collected information will be removed from the Offline Device table.

Groups

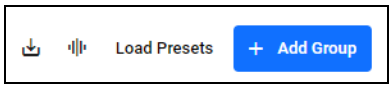
The **Asset Management** page allows you to create groups to organize your network. The groups list shows created groups in your network, how many devices are in that group, the source, network ID Criteria, a group icon, and further edit actions.



Creating Groups in the Asset Management menu

You can assign multiple devices to a group. Groups can also be created in the Network map; for information about this see "Groups" on page 65.

A user can create Network groups with read/write permissions in the **User Settings** page for each separate user. You can change permissions for different users for both sites and groups on the **User Management** page. For more information about sites and groups permissions see "User Management" on page 305.

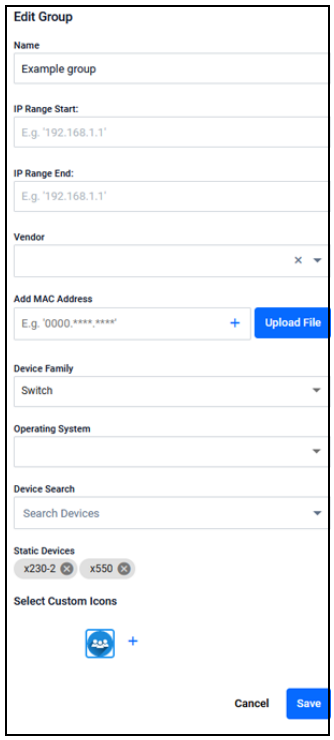


To create a group in the Asset Management menu, select the **+Add Group** button.

You can click the **Load Presets** button to load a ZIP or GZ file with groups from a previous version of Vista Manager.

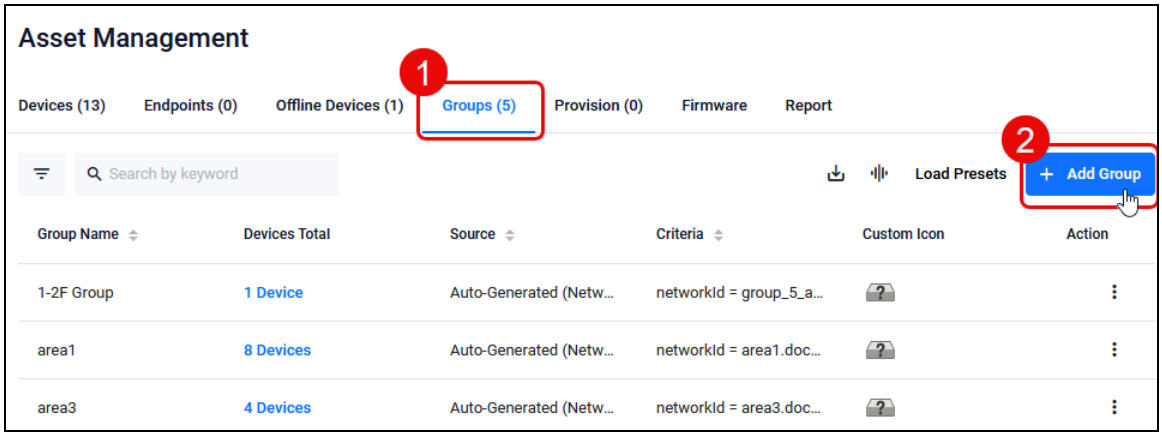
You can customize the groups in the side menu. You can specify a MAC address range, an IP address range, a vendor, or a combination of these. You can also select an icon to represent the group.

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.

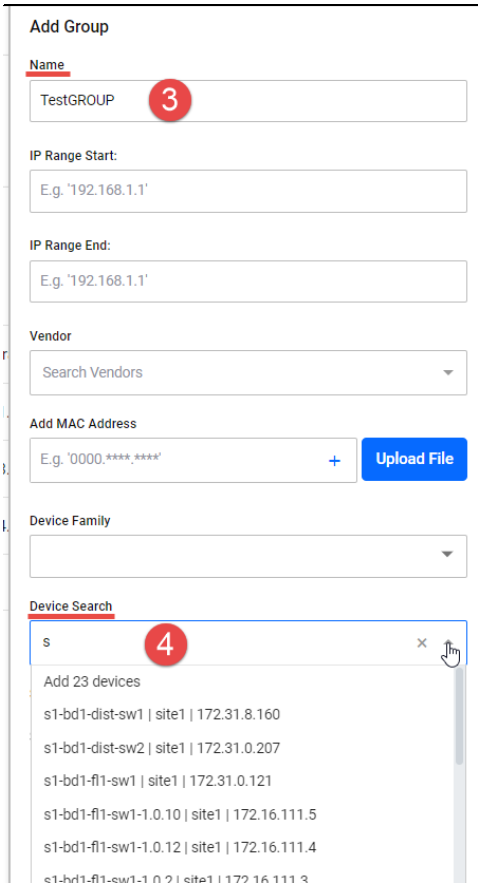


To add a group:

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



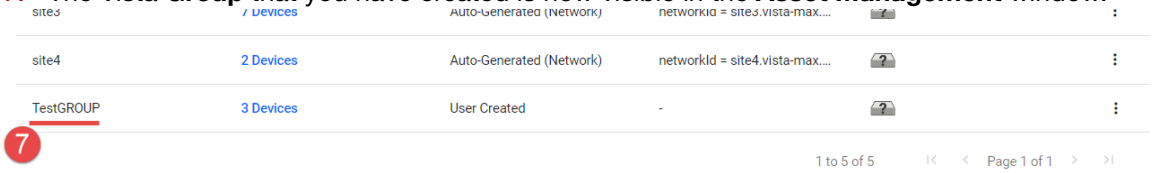
3. Enter a group **Name**
4. In the **Device Search** field, start typing a device name. A drop-down list appears.



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

6. Click **Save**.

7. The Vista **Group** that you have created is now visible in the **Asset Management** window.



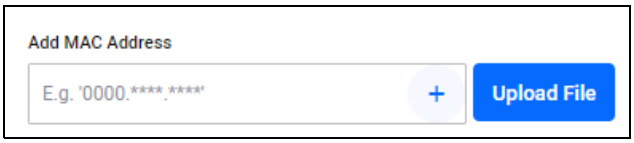
Note: From version 3.11.0, RADIUS batch support has been added. You can set-up device groups for this as above, before you continue configuring the RADIUS groups from the RADIUS page. For information on RADIUS groups, see "Groups" on page 65.

Adding a MAC address list

You can add multiple MAC addresses to a group by uploading a .txt or .csv file containing a list of MAC addresses to the Groups tab of the Asset Management menu. Vista Manager EX then extracts the MAC addresses from the uploaded file and registers them with the group.

To do this click on the **+ Add Group** button.

The Add Group sidebar will appear where you can type a single MAC address and click the **+** to add it, or upload a file with multiple MAC addresses in it.



You can use commas, spaces, and new lines 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.

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.

Provisioning

Provisioning is the process of equipping a new AMF Plus node (device) with everything it will need to operate in an AMF Plus network as needed.

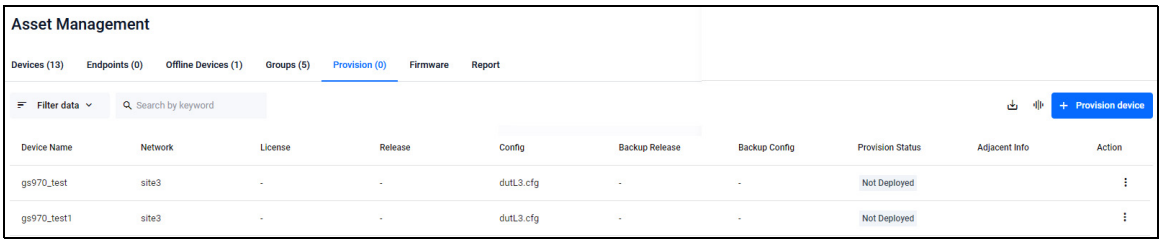
For example, when a new device is connected to the network it can receive the required firmware, configuration, and licensing files from a nearby device.

You can organize these files in advance through the asset management provisioning system.

During provisioning, you must also define the location of the new device (port it connects to). The new device must be plugged into the specified port to receive the files.

For more information on AMF node provisioning, including how to configure this through the device's CLI, see the AMF Plus and AMF Feature Overview and Configuration Guide.

You can provision a device through the **Asset Management** menu.



Provisioning a new device

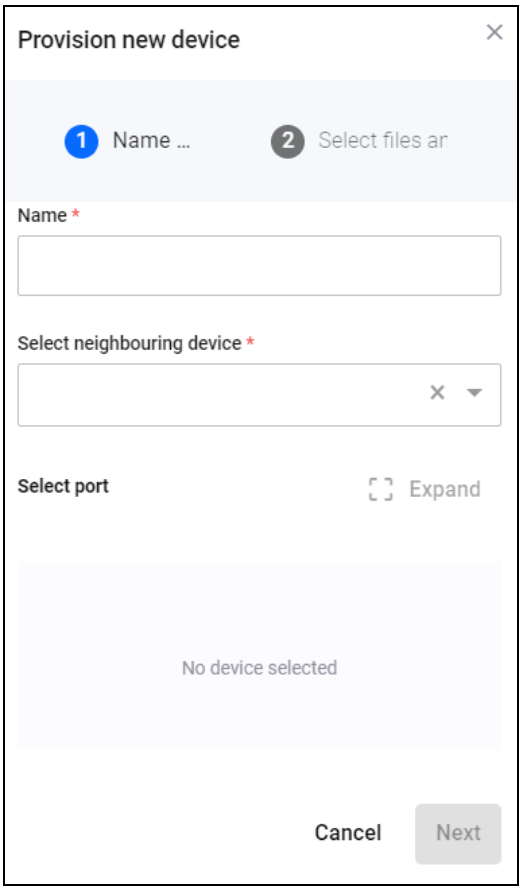
When you click the **+ Provision Device** button, the sidebar will open a dialogue where you are able to provision a new device. You can set up network provisioning between devices that you wish to connect.

1. **Name Device**

- Name the new provisioning setting
- Select the neighbouring device
- Select the port from the diagram of the device that appears

2. **Select files and deploy**

- Add a config file (.cfg), you can add a backup config file as well
- Add a release file (.rel), you can add a backup release file as well
- Add a Device License file (.txt)
- Add a Device Gui file (.gui)



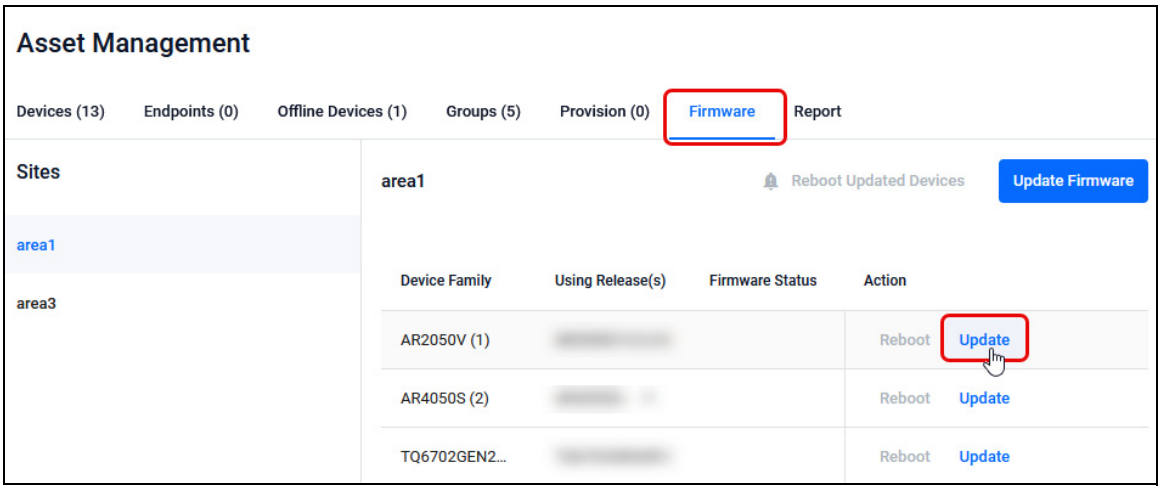
Once you have completed the provisioning, the provisioned device node will appear on the Provisioning tab.

The number next to the title **Provisioning (0)** will change to reflect how many devices have been provisioned.

Firmware

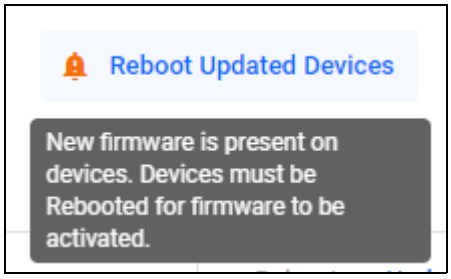
Device firmware management

The asset management page 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.



If a device needs a firmware upgrade, then an orange triangle icon paired with orange text will show in the Firmware Status section. The Reboot Updated Devices button on the top left with the orange bell icon will become clickable.

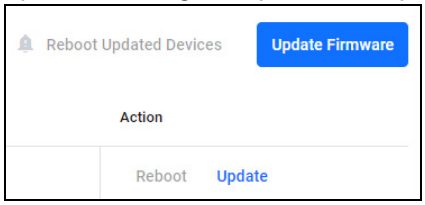
Note: You cannot upgrade the **TQ-R Series access point** firmware through Vista Manager EX. Use the device's CLI or GUI instead.



If you hover over this button, it will tell you the devices must be rebooted. Click this button to update these devices.

Click the blue **Update Firmware** button to update **all** device families in the selected AMF area.

Click on any of the blue **Update** action buttons to update a specific device family. The side panel opens, showing 4 steps. For this process, you will need a firmware release file for that family.



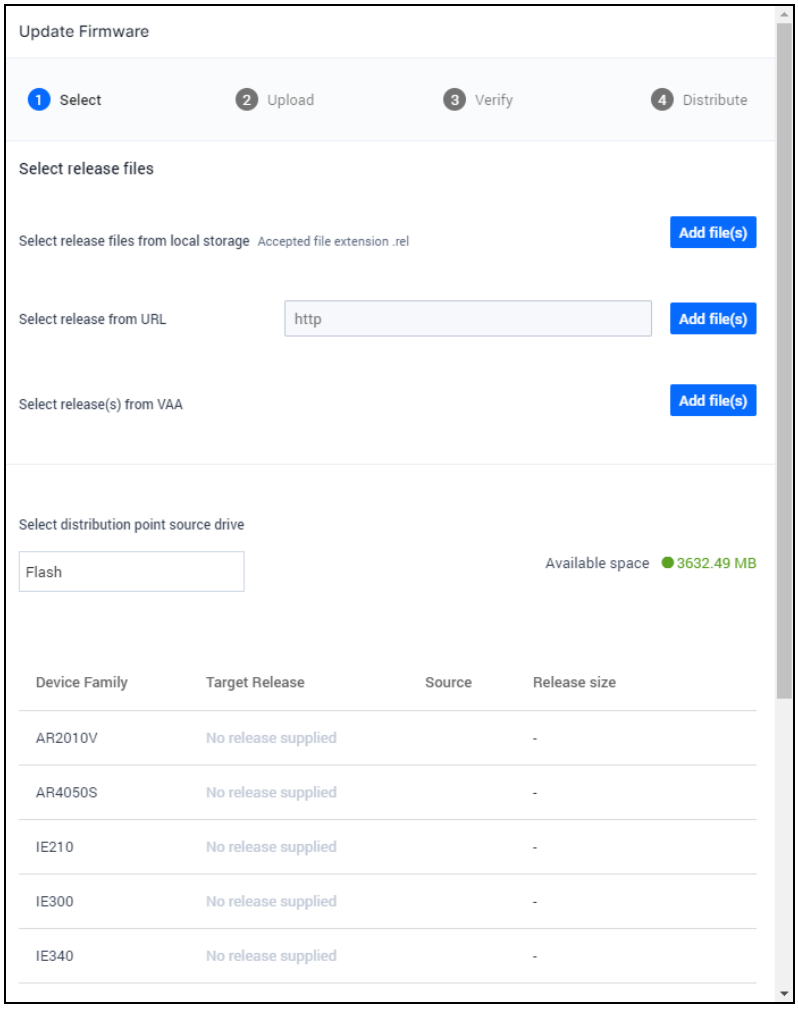
Note: This file is not the same release as the current file running on the devices.

Updating a device family

This section covers the process of updating firmware via the **Update Firmware** menu. The steps are broken up into different sections.

You can exclude selected devices from a given family when you perform a firmware upgrade. This feature is especially helpful if you need to upgrade only specific devices in a critical network, such as a hospital ICU network.

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



Step 1. **Select**

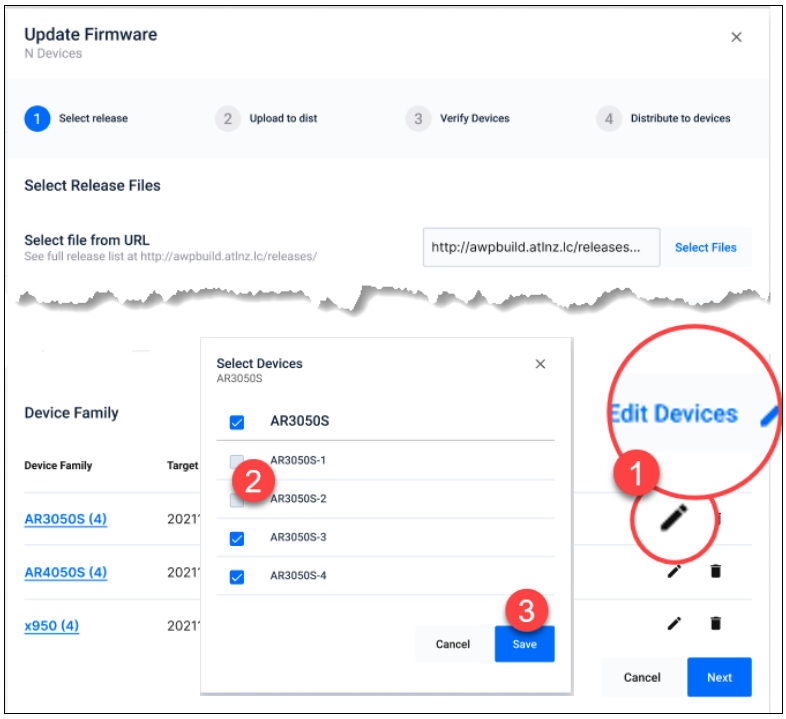
Select the release files for the Area Master. The permitted file types are .zip and .rel files. Vista Manager EX first extracts the zip file onto a temporary directory. The release file will then be distributed to the device family if there is a match. Otherwise, you will be notified of any invalid extract files.

The source options are:

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

To select specific devices, 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.
   - 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. **Upload**

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

Step 3. **Verify**

The status of the firmware update will show as **"*Verifying...*"**, and then either notify you of success or that a number of devices failed. If any failed, click **More info** to see exactly which devices failed and why. Assuming that they succeeded, click **Update Device** to distribute the firmware.

Step 4. **Distribute**

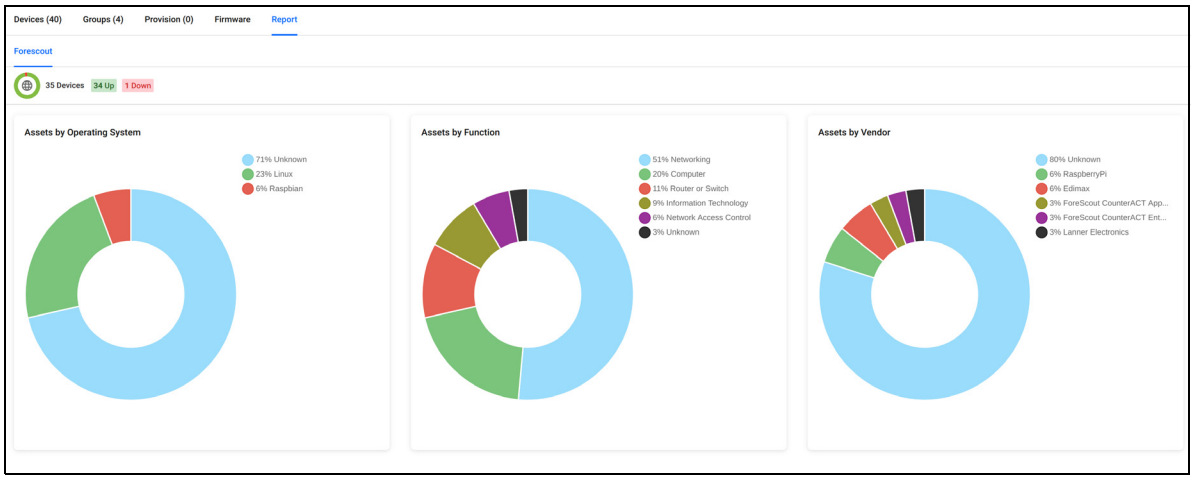
The status then shows as **"*Distributing to...*"**. Click Done once distribution finishes.

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: 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.

Report

The **Report** section of the **Asset Management** menu displays various device data discovered by plugins. By looking at the various donut charts, you can see how different assets in your network compare to each other.



In the example above, data from the Forescout plugin is displayed.

The header displays information of assets in your network at a glance, so you can quickly view the status and comparative information of devices in your network.

The following information is displayed in a donut chart format:

- Assets by Operating System
- Assets by Function
- Assets by Vendor

Note: If there is no plugin data then the Reports section will appear blank.

Plugins

AWC (Wireless Controller) plugin

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 plugin to Vista Manager. To see how to install the AWC plugin, see "Registering/Installing plugins" on page 26.

For documentation on how to use the AWC plugin, see the AWC Technical Documents.

SNMP plugin

The Vista Manager SNMP plugin 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 plugin is a powerful addition to Vista Manager EX, adding management flexibility by also supporting non-AMF devices. To see how to install the SNMP plugin, see "Registering/Installing plugins" on page 26.

As of update 3.11.0, the SNMP plugin can used as a part of your AMF network without the need for a license. The SNMP plugin is enabled automatically provided that all AMF masters and controllers have a valid AMF Plus license that is current and non expired.

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

When an SNMP device goes down and is no longer reachable, the plugin will report it as down and Vista Manager EX will display it on the network map with a Down status.

For documentation on how to use the SNMP plugin, see the SNMP Plug-in and Trap Receiver Technical Documents.

Trap Receiver plugin

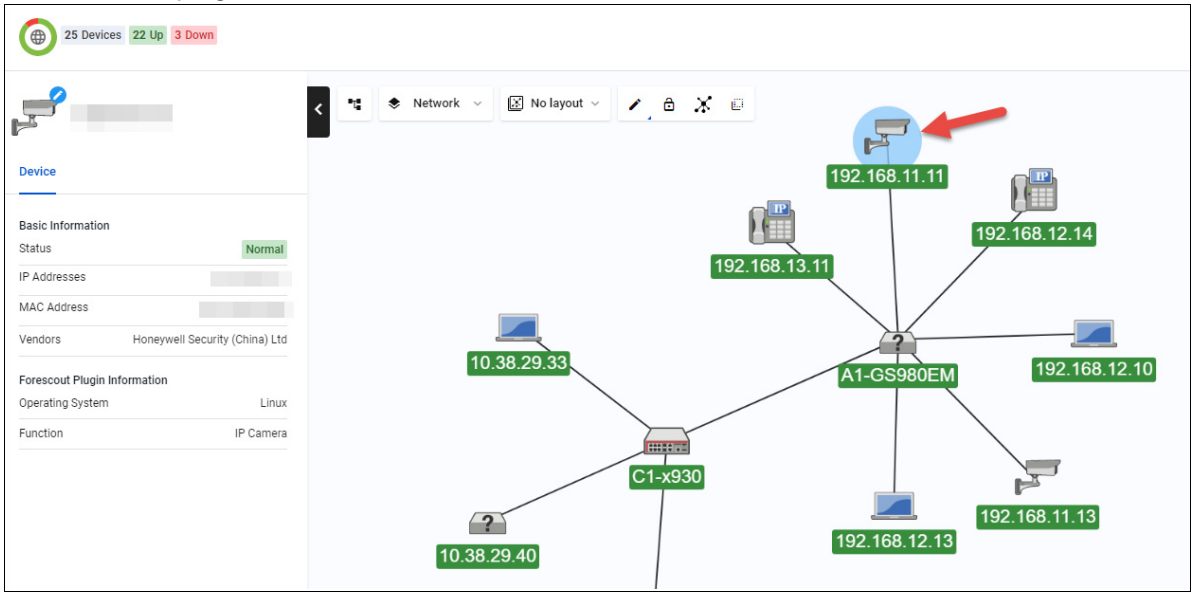
The Vista Manager Trap Receiver plugin captures information about your network. It allows you to see a wide range of third-party devices and traps received for them. See the SNMP Plug-in and Trap Receiver Technical Documents for more information.

Forescout plugin

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

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

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



You can also:

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

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

Forescout provides the status of a client, which can either be Up or Down:

- If Forescout returns an Up status for the client, Vista Manager EX will display the node as Up.
- If Forescout returns a Down status for the client, Vista Manager EX will display the node as Down.
- If Forescout does not return any data for the client (i.e., the client is not found in Forescout), Vista Manager EX will remove the client from the map instead of showing it as Down.

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

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

Prerequisites for installing Forescout

Vista Manager polls Forescout's Enterprise Manager API to get a list of endpoints along with information about these end points that a CounterACT device has collected from the device. If the customer has multiple CounterACT devices, you must first register them with Forescout's Enterprise Manager. To see how to install the Forescout plugin, see "Registering/Installing plugins" on page 26.

The Enterprise Manager is the controller that manages CounterACT appliance activity, policies, and collects information about endpoint activity. You can see the information retrieved from the Enterprise Manager from the Forescout Console program.

In order to run the Forescout plugin, you need to configure three things in the Forescout console application:

Step 1. **Install eyeExtend Connect**

Step 2. **Start the web API module**

Step 3. **Configure the web API module**

Note that this guide does not cover step 1, and instead covers the web API that connects with Vista Manager. When using this guide, we assume that you have all of your CounterACT devices registered with the Forescout console. For information about installing eyeExtend Connect, as well as documentation for the full installation of Forescout CounterACT, refer to the official Forescout documentation portal.

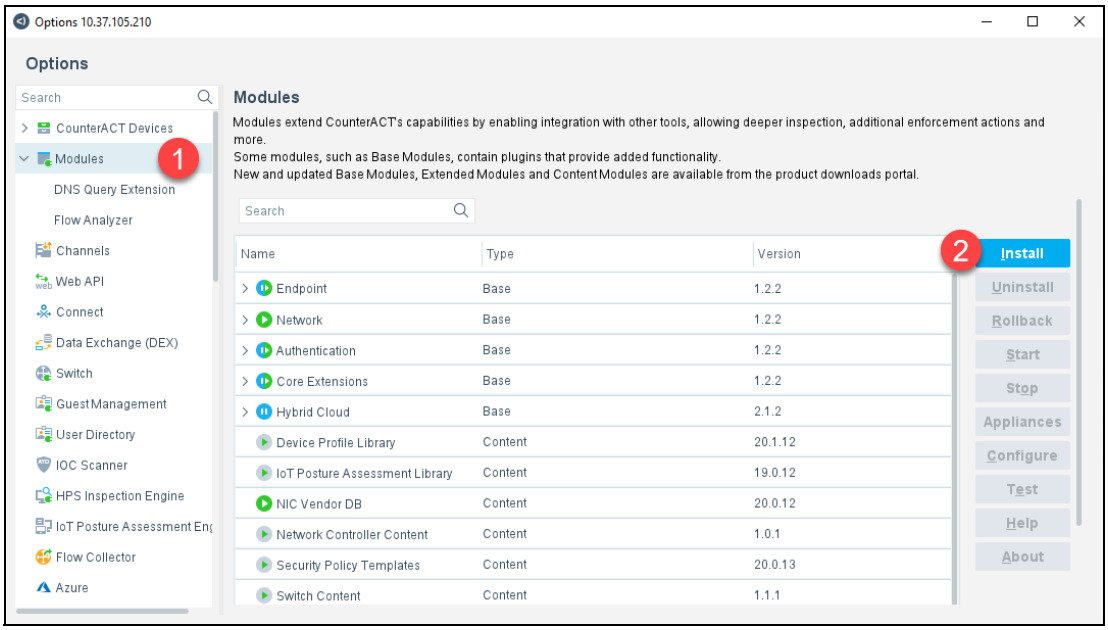
First, install eyeExtend Connect. Once eyeExtend is installed, proceed with installing the Connect web API from the Forescout Console.

Step 1. In the Forescout Console, go to **Options** > **Modules.**

Step 2. Click on the **Install** button, which will open your file browser.

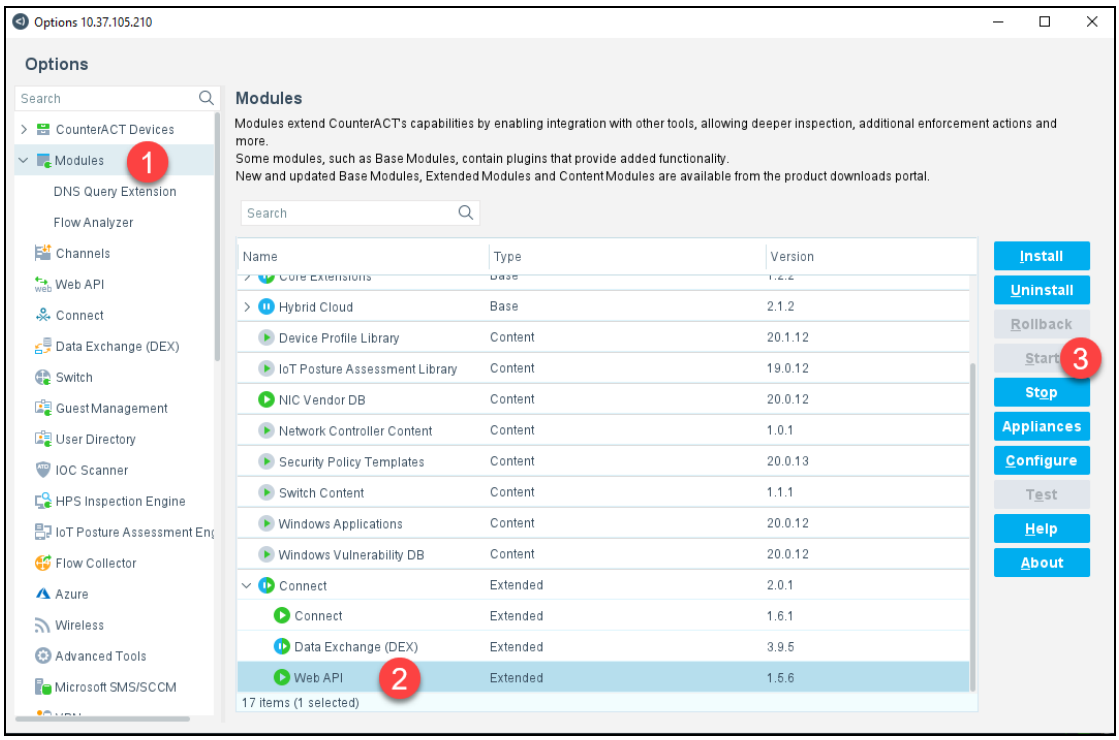
Step 3. Select the **Forescout Connect FPI File** to install the web API.

The web API will now appear in the Modules list under the **Connect** heading.



Note that you may have to start the web API after installing. If it is already active, the Start button will be grayed-out.

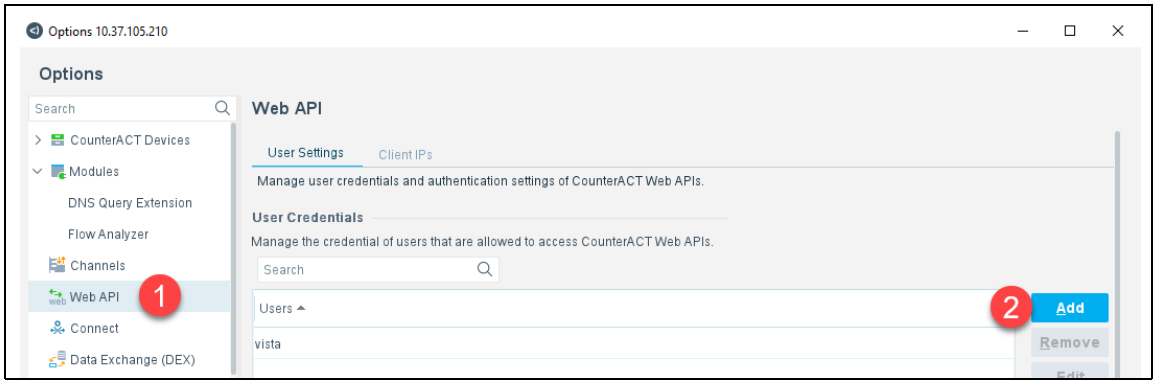
1. To start the module, go to **Options > Modules** in the Forescout console and scroll down to the **Connect** module.
2. Expand the connect module accordion menu and select **Web API.**
3. Click the **Start** button on the right side of the window to start the web API



Creating a Web API User

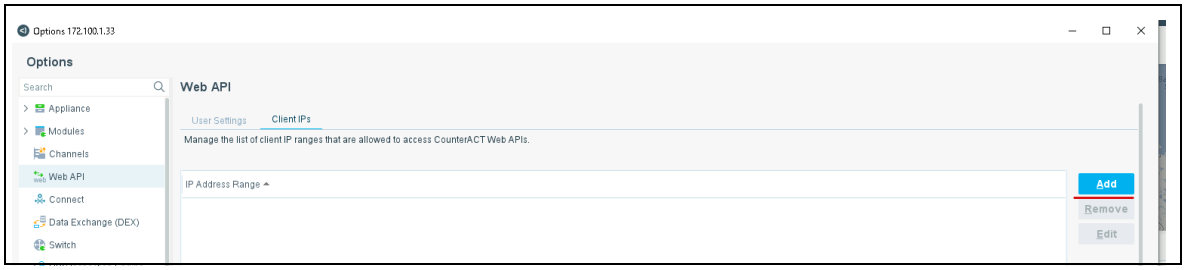
For Vista Manager to access CounterACT devices for polling, we will create a web API user.

- In the Options menu, select **Web API**
- On the Web API module click the **User Settings** tab
- Then, click **Add** to add a User.



Next, we will allow all IP addresses to access the Web API:

- On the web API module click the **client IPs** tab
- Then, click **Add**



Nozomi plugin

From version 3.12.0 onwards, the Nozomi plugin (Nozomi Networks) is now supported on Vista Manager. This means you can use the Nozomi plugin to discover and classify devices on your network. If you run an AMF network with AMF Device Discovery enabled, you can use Nozomi to add more information about devices into Vista Manager.

After you register the plugin, the Vista Manager will poll for devices and discover them using the plugin. The devices will then be displayed on the Network Map and Asset Management pages, and you can change any desired custom details.

Nozomi doesn't return a **state** for nodes. Also, Nozomi won't remove down devices from its inventory. When a Nozomi node is learned it will display on the network map as Up, even if the device is physically down.

When you manually remove or unregister the Nozomi plugin, the devices discovered by Nozomi will be removed from the map.

You must first configure the Nozomi Guardian sensor prior to registering it in Vista Manager. To see information about the initial configuration of Nozomi Guardian, see the Nozomi Plugin User Guide.

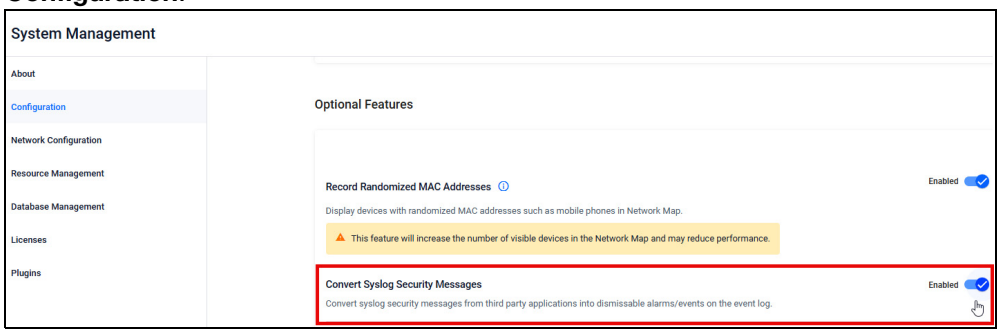
To see how to register the Nozomi plugin with Vista Manager, see "Registering/Installing plugins" on page 26.

How to setup Nozomi endpoint notifications in Vista Manager

From version 3.13.1 onwards, support for third party security features from the Nozomi plugin have been implemented into Vista Manager.

You can create alarms in Vista Manager when it picks up alerts from Nozomi above a certain severity level. You can also enable automatic blocking of endpoint devices above a certain severity level based on gathered Nozomi information. These changes implement additional security features from the Nozomi plugin.

To generate syslog event messages in Vista Manager when it receives a security related syslog from Nozomi, enable the **Convert Syslog Security Messages** feature in **System Management** > **Configuration**.



When Vista Manager receives a syslog message from Nozomi matching a security rule, it will create a event in the event log with a severity level of ALERT.

This creates a alarm visible on the Network map and the Event Log. This is also shown in the alarms count on the Endpoints table. These alarms can be dismissed to remove the alarm.

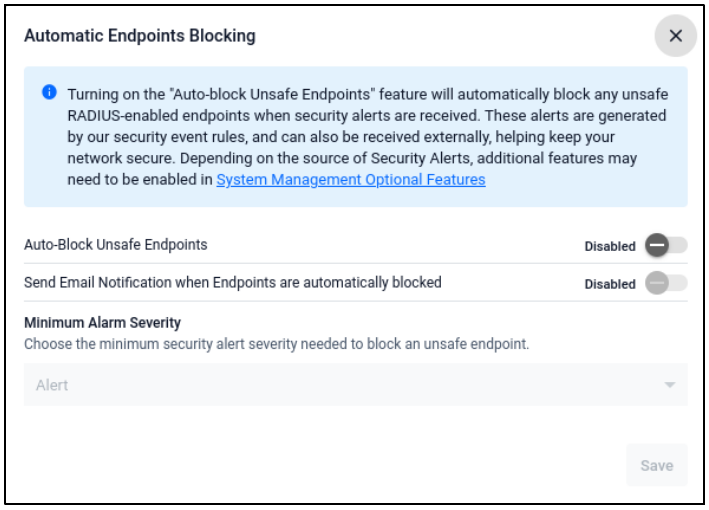
Nozomi alert-level based automatic blocking

You can also automatically block devices discovered by Nozomi, based on security severity levels. When you enable **Automatic Blocking** from the **Asset Management** page, you can choose the severity level that triggers the automatic blocking from **Alert**, or **Emergency** levels.

Depending on the source of Security Alerts, additional features may need to be enabled in **System Management** > **Optional Features**.

To enable Automatic Blocking, click the **Cog icon** on the **Endpoints** tab of the **Asset Management** page.

Toggle to enable Automatic Blocking, and select the minimum security severity level for the alarm to trigger from the dropdown.



- When you enable **Automatic Blocking**, endpoints will be automatically blocked if a security alarm above the chosen severity occurs.
- You can enable email notifications for security related alarms.

If an Endpoint has been automatically blocked you can manually unblock the device from the Asset Management table. See "Blocking or Allowing Endpoints" on page 197 for more information.

Microsoft Intune Plugin alerts

From version 3.13.1 onwards, you can view alert information that is gathered by Microsoft Intune in Vista Manager. Vista Manager integrates information from Microsoft Intune for its Intune plugin to obtain a full picture of the monitored devices and security alerts.

Devices enrolled in Intune are shown on the Network Map and Asset Management pages in Vista Manager.

Note that you must have Microsoft Intune and associated applications, such as Microsoft Defender and Azure Event Hubs, already configured. This includes endpoint devices synced with Intune. To see how to configure Microsoft Intune, see Microsoft Intune's Official Documentation.

Security alerts are shown in the Event log. These are linked to the device that the alert occurred on. If the device has been removed from Intune, then no device information will be included in the Event.

On the Network Map, an alarm badge will be shown on devices that have security alerts.

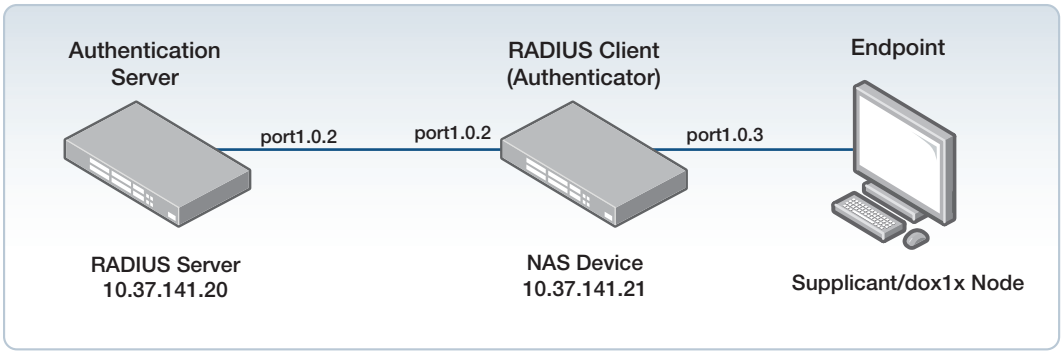
Do not enable the Automatic Blocking feature from the Endpoints table while using the Intune plugin. If you have previously enabled Automatic Blocking, disable it.

Intelligent Edge Security (IES)

Intelligent Edge Security (IES) allows you to manage endpoint communication with MAC-based authentication supported by AMF Plus devices.

You can use the Endpoints tab to enhance the security of your network by either **allowing** or **blocking** selected MAC authenticated devices that are connected to your Local RADIUS server. You can also configure this to automatically block endpoints that do not meet a set criteria.

You can set up the authentication server device to forward syslog output of permission or rejection logs to Vista Manager.



In order for the Endpoints feature to work, you must have a Local RADIUS server and a Network Access Server (NAS) device for authentication. This feature frequently polls the network and visually reloads the list to keep the endpoint list up to date.

You must also configure STOAT on the NAS device to collect endpoint information.

Configuring the RADIUS Authentication Server

First, we will configure the RADIUS Authentication Server. The device running the RADIUS Server is also running AlliedWare Plus version 5.5.3-2 or later. Alternatively, go to **Network Services**> **RADIUS**> **NAS** from the Device GUI.

From the CLI, configure the RADIUS Authentication Server with the following commands:

```
awplus(config)#radius-server local
awplus(config-radsrv)#auth-mac-promiscuous
awplus(config-radsrv)#nas 10.37.141.21 key secretkey1
```

We register the NAS device as a RADIUS client to the RADIUS Authentication Server.

Enabling **auth-mac-promiscuous** mode enables client devices to access the network immediately when they first connect. You might want to enable promiscuous mode where access is initially allowed for all endpoint devices, so you can block endpoint devices exhibiting suspicious behavior individually.

- When you enable promiscuous mode, the server responds with an authentication success to MAC-based authentication requests from endpoints not registered with the RADIUS server. You can set to manually accept or deny unregistered endpoints later.

Instead, if you would like to implement strict operation where communication is initially denied for all endpoint devices that do not have permission, remove the **auth-mac-promiscuous** command from the example above.

Note: If you don’t enter auth-mac promiscuous mode on the RADIUS server, then client devices will be unable to connect until you manually set them to ‘allowed’.

Full RADIUS Server Configuration Example

Below is an example configuration for a device acting as a RADIUS Server for the Endpoints feature. We use the IP of the NAS device with a Shared Secret key, and enable STOAT on the device. We then connect the server to the network with VLANs.

```
radius-server local
 server enable
 auth-mac-promiscuous
 nas 10.37.141.21 key secretkey1
!
atmf network-name My-Network
atmf master
!
!
service stoat
!
stoat collector enable
stoat collector key secretkey2
!
!
vlan database
 vlan 4080 name AMF
 vlan 4080 state enable
!
interface port1.0.2
 description Link_R21-3050
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 4080
 switchport trunk native vlan none
 switchport atmf-link
!
!
interface vlan4080
 ip address 10.37.141.20/25
!
!
ip route 0.0.0.0/0 10.37.141.120
```

Configuring a switch to be an Authenticator device (NAS)

Next, we will configure the Authenticator device (NAS). If you would like to use multiple switches as NAS clients, repeat this process.

STOAT must be enabled on the Authenticator device (NAS). The NAS device is running AlliedWare Plus version 5.5.3-2 or later. For more information about STOAT, see the Device Discovery using STOAT Feature Overview and Configuration Guide.

1. Enable the STOAT service and enable dot1x as the discovery protocol.

   We also create a destination to the IP address of the RADIUS Server.

```
awplus(config)# service stoat
awplus(config)#stoat discovery dot1x
awplus(config)#stoat destination 10.37.141.20
awplus(config-stoat-dest)key secretkey2
```

2. Connect the NAS device to the RADIUS server:

```
awplus(config)#radius-server host 10.37.141.20 key secretkey1
```

3. Define the list of authentication servers to use for MAC authentication. In this case, we only have one RADIUS Server, so we use the default group.

```
awplus(config)#aaa authentication auth-mac default group radius
```

4. Enable MAC-based authentication on the port(s) to be monitored:

```
awplus(config)#interface port1.0.1-1.0.3
awplus(config-if)#auth-mac enable
awplus(config-if)#auth host-mode single-host
awplus(config-if)#auth timeout quiet-period 60
```

Note: Host mode should not be set to multi-host. This can result in multiple endpoints being authenticated incorrectly.

You can set host-mode to **single-host** or **host-plus-voice**.

You may wish to limit the maximum allowed clients using the **auth max-supplicant x** command. (Replace x with the maximum number of client devices).

We also recommend you set the authentication timeout to default with the **auth timeout quiet-period 60** command.

5. Connect to Vista Manager to allow dynamic authorization

```
awplus(config)#auth radius send service-type
awplus(config)#radius dynamic-authorization-client 10.38.60.20 key
secretkey3
```

Enabling this allows you to disconnect suspicious client devices from Vista Manager.

6. Optionally, to enable Vista Manager to send Syslog messages to the NAS device, use the following commands:

```
awplus(config)#Log date-format iso
awplus(config)#log host 10.38.60.20
awplus(config)#log host 10.38.60.20 level informational program 802.1x
```

Full NAS Switch Configuration Example

```
radius-server host 10.37.141.20 key secretkey1
!
aaa authentication auth-mac default group radius
!
atmf network-name MyNetwork
!
service stoat
!
stoat discovery dot1x
stoat destination 10.37.141.20
 key secretkey2
!
!
!
auth radius send service-type
radius dynamic-authorization-client 10.38.60.20 key secretkey3
!
vlan database
 vlan 4080 name AMF
 vlan 4080 state enable
!
interface port1.0.1
 description Link_R20-3050
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 4080
 switchport trunk native vlan none
 switchport atmf-link
!
interface port1.0.3
 description ###Supplicant###
 switchport
 switchport mode access
 switchport access vlan 4080
 auth-mac enable
!
interface vlan4080
 ip address 10.37.141.21/25
!
ip route 0.0.0.0/0 10.37.141.120
```

Configuring a TQR Series Wireless AP as a NAS device

This section is specifically for configuring a TQR Series device as a NAS Client device for the Authentication Server.

If you would like to use multiple TQR Series devices as NAS clients, repeat this process.

In this example, the TQR series device is already set up. If you have not yet configured the device, please see the Quick Tour section of the AWC Plugin User Guide.

Note: When using IES with TQR series devices, we enable both MAC-based authentication (dot1x) and the TQR device's wireless discovery together for STOAT detection. This means that the Network Map shows both of the connection links.

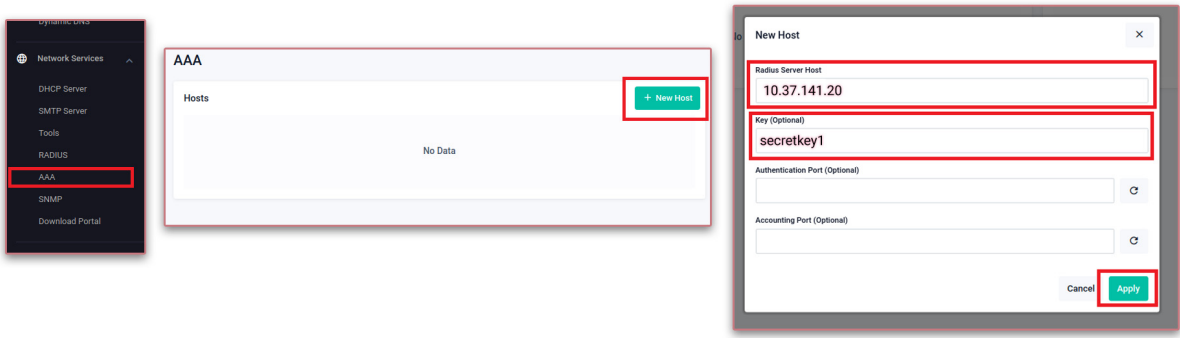
TQR series devices support device detection via wireless only.

1. Connect the NAS device to the RADIUS server:

```
awplus(config)#radius-server host 10.37.141.20 key secretkey1
```

You can also do this from the TQR's Device GUI.

- Go to **Network Services** > **AAA**
- Click the **+ New Host** button
- Enter the RADIUS Server Host IP address, and specify the secret key (secretkey1)



2. Enable the STOAT service and enable dot1x as the discovery protocol:

```
awplus(config)#service stoat
awplus(config)#stoat discovery dot1x
awplus(config)#stoat discovery wireless
awplus(config)#stoat destination 10.37.141.20
awplus(config-stoat-dest)key secretkey2
```

Above, we also create a destination to the IP address of the RADIUS Server.

For TQR devices, we enable both MAC-based discovery (dot1x) and TQR series wireless discovery for STOAT collection.

3. Configure MAC-based authentication for the wireless network configuration.

if you would like to detect devices on multiple networks, you must add settings to each wireless network. In this example, we use network 1 and network 17.

```
awplus(config)#wireless
```

```
awplus(config)#network 1
awplus(config)#mac-auth radius auth group radius
awplus(config)#mac-auth radius send service-type
awplus(config)#mac-auth radius dynamic-authorization-client 10.0.0.254
key secretkey3
awplus(config)#unassociated-client-list acquire
awplus(config)#exit
```

- Above we specify the authentication group to use. In this case we only use one RADIUS server.
- We also configure RADIUS to send dynamic authorization messages to Vista Manager (10.0.0.254).

We repeat this for network 17:

```
awplus(config)#network 17
awplus(config)#mac-auth radius auth group radius
awplus(config)#mac-auth radius send service-type
awplus(config)#mac-auth radius dynamic-authorization-client 10.0.0.254
key secretkey3
awplus(config)#unassociated-client-list acquire
awplus(config)#exit
awplus(config)#exit
```

4. Specify the interface to use as the starting point when communicating with the RADIUS server.

   This interface is the interface with the IP address specified in the **nas** command on the RADIUS server.

   ```
   awplus(config)#ip radius source-interface br1
   ```

   In this case, the bridge interface (br1) is the bridge interface connected to the RADIUS server. If you would like to use MAC-based authentication on multiple wireless networks, add a bridge interface for each network.

5. Define the list of authentication servers to use for MAC authentication. In this case, we only have one RADIUS Server, so we use the default group.

   ```
   awplus(config)#aaa authentication auth-mac default group radius
   ```

6. Enable MAC-based authentication on the port(s) to be monitored

   ```
   awplus(config)#interface port1.0.1-1.0.3
   awplus(config-if)#auth-mac enable
   awplus(config-if)#auth host-mode single-host
   awplus(config-if)#auth timeout quiet-period 60
   ```

7. Optionally, to enable Vista Manager to send Syslog messages to the NAS device, use the following commands:

   ```
   awplus(config)#Log date-format iso
   awplus(config)#log host 10.38.60.20
   awplus(config)#log host 10.38.60.20 level informational program 802.1x
   ```

Endpoint Syslog Messages

The syslog messages that are output when an endpoint connects or disconnects differ depending on whether the client device is a switch or a TQR series wireless AP.

In the case of a switch, the following three types of syslog messages are output:

1. MAC-based authentication success log

```
MAC Authentication successful for [RADIUS user
name]@[endpoint MAC address] on [switch port number]
```

```
MAC Authentication successful for 00-00-53-00-5e-
00@0000.5300.5e00 on port1.0.2
```

2. MAC-based authentication failure log

```
MAC Authentication failed for [RADIUS user name]@[endpoint
MAC address] on [switch port number]
```

```
MAC Authentication failed for 00-00-53-00-5e-
00@0000.5300.5e00 on port1.0.2
```

3. Device Disconnection Event Log

```
Supplicant [RADIUS user name] has been disconnected by DM
from [AVM EX IP address]
```

```
Supplicant 00-00-53-00-5e-00 has been disconnected by DM
from 192.198.1.250
```

In the above examples, the RADIUS username is the same MAC address as the endpoint MAC address. The format may differ depending on your configuration.

For TQR series wireless APs, the following two types of syslog messages are output:

1. Connection log

```
vap[connected wireless band].[VAP number]: STA [endpoint
MAC address] associated with BSSID [BSSID of connected
wireless AP] ([SSID of connected wireless AP]) RSSI [RSSI
value]
```

```
vap1.0: STA 00:00:53:00:5e:80 associated with BSSID
00:00:53:00:5e:20 (FreeForAll) RSSI -28
```

2. Disconnection log

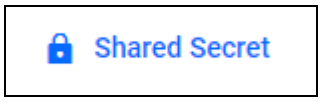
```
vap[connected wireless band].[VAP number]: STA [endpoint
MAC address] disassociated from BSSID [BSSID of connected
wireless AP] ([SSID of connected wireless AP]) reason
[reason value]
```

```
vap1.0: STA 00:00:53:00:5e:80 disassociated from BSSID
00:00:53:00:5e:20 (FreeForAll) reason 1
```

Connecting to Vista Manager

Configure Vista Manager to send RADIUS Dynamic Authorization messages (Disconnect clients, CoA (Change of Authorization)).

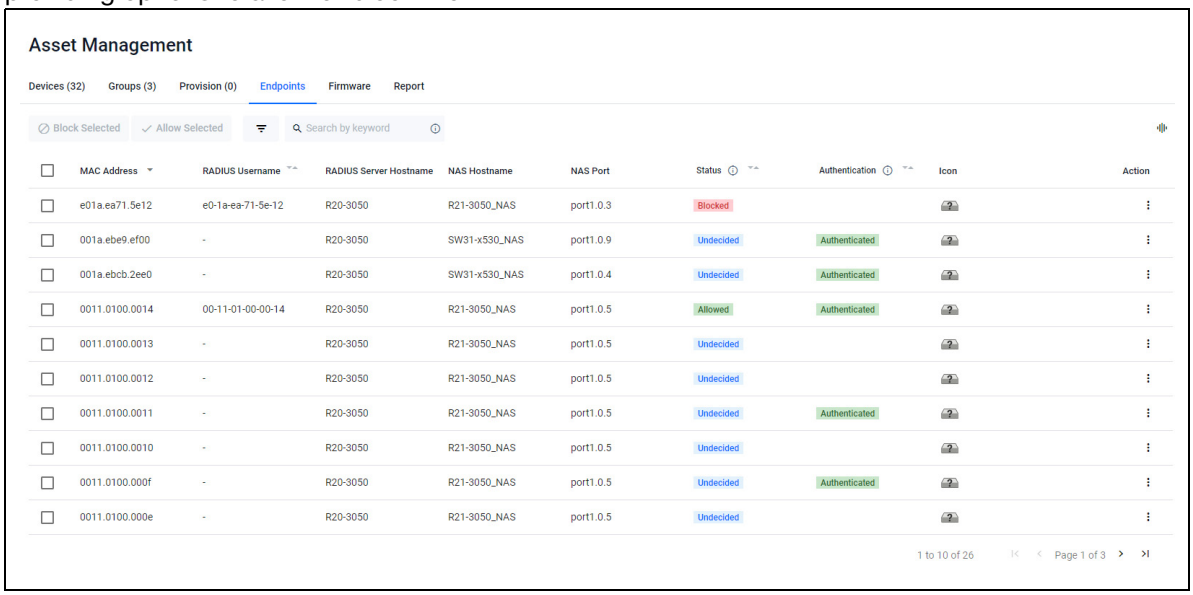
1. Go to the **Network Services** > **RADIUS** page.
2. Click the **Shared Secret** button in the top right.



Once the Authentication RADIUS server, NAS, and Vista Manager are configured, you will see the connected endpoints on the Asset Management page under the Endpoints tab.

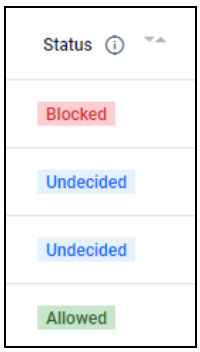
Configuring endpoint permissions from Vista Manager

The Endpoint tab helps you to manage supplicants/endpoints by displaying their status and providing options to allow or block them.



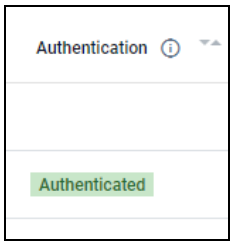
There are two major columns that help determine the status of endpoints: the Status column and the Authentication column.

The current status of the device is displayed in the Status column:



- Undecided - a RADIUS user does not exist on the RADIUS server, and no decision has been made yet on whether to block or allow it. See "Default authentication in promiscuous mode" on page 197 for more information.
- Blocked - a RADIUS user exists to block this endpoint on the network and is set to reject on the RADIUS user page
- Allowed - a RADIUS user exists to allow this endpoint on the network, and is not set to reject on the RADIUS user page

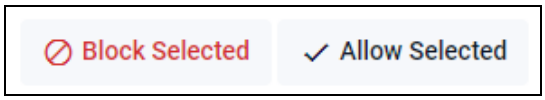
The Authentication column shows the authentication status as it is learned through AlliedWare Plus Device Discovery.



- A blank or empty column indicates that the endpoint is unauthenticated and unable to connect to the network.
- A column containing the ‘Authenticated’ keyword indicates that the endpoint is authenticated and able to connect to the network.

Blocking or Allowing Endpoints

Select one or multiple devices you wish to configure by selecting the checkbox next to a device. The Block Selected and Allow Selected buttons will become selectable once you select a device.



When you click the **Block Selected** button:

- The selected RADIUS users will be added to the RADIUS server if they do not already exist, or updated with the "Reject" keyword based on the selected endpoints' MAC addresses.
- Once the RADIUS users are created or updated, the Status column will display Blocked for the selected devices.
- A Change of Authorization (CoA) request will be sent from Vista Manager to the NAS device to disconnect the selected devices as part of the blocking process.
- If the CoA request is successful, the Authentication column will be cleared for these devices.
- The Network Map includes a ‘Blocked’ icon next to the client devices that you have blocked.
- You can see a "blocked" badge on the blocked and unauthenticated devices icon in the Network Map.

Note: The table may take several minutes to reflect these changes, as it depends on the endpoint attempting to reconnect and being re-learned by Device Discovery.

When you click the **Allow Selected** button:

- The selected RADIUS users will be added to the RADIUS server if they do not already exist, or updated by removing the "Reject" keyword (if it exists) based on the selected endpoints' MAC addresses.
- Once the RADIUS users are created or updated, the Status column will display "Allowed" for the selected devices.
- During the next reconnect attempt, the selected devices will be allowed access to the network.
- The Authentication column will display Authenticated for allowed devices.

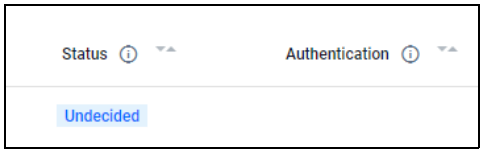
Default authentication in promiscuous mode

Enabling or disabling promiscuous mode decides if clients are authenticated by default or not.

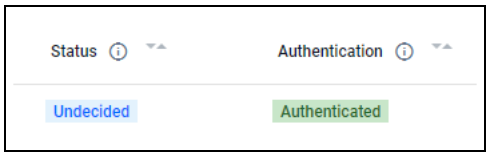
Depending on if you have your RADIUS server’s authentication set to promiscuous mode or not, using the **auth-mac-promiscuous** command, the Endpoints table will show different badges. Promiscuous mode is disabled by default.

When promiscuous mode is disabled, when the RADIUS server receives authentication from the NAS device, it is not automatically authenticated. The RADIUS server checks its database entries to make sure the corresponding MAC address matches the client's, and if not, then it does not give the client access to the network and does not authenticate it.

Visually this displays on the Endpoints table as both blank in the **Authentication** column, and **Undecided** on the Status column.



However, if you enable promiscuous mode, when the RADIUS server receives information from the NAS device, the client will be authenticated by default, even if its credentials do not exist in the database.



To see more information about enabling promiscuous mode on the RADIUS Server, see "Configuring the RADIUS Authentication Server" on page 187.

For further support, see the Local RADIUS Server Feature Overview and Configuration Guide.

You can set up Vista Manager to automatically block endpoints based on security alerts received from third-party applications. For more information, see "Nozomi alert-level based automatic blocking" on page 185

RADIUS Endpoint column data

From version 3.13.1 onwards, statistical data from RADIUS server connections are added to the Endpoints table on the Asset Management page, and the RADIUS User page.

The following columns have been added to the Endpoints page:

- The **Last Interaction Time** column displays the local timestamp for the most recent connection between an endpoint device and its associated RADIUS server
- The **Failed Connection Attempts** column displays the count of unsuccessful attempts from an endpoint device to connect to the specific RADIUS server since the server's last reboot.
- The **Successful Connections** displays the count of successful connections made by an endpoint device to the specific RADIUS server since the server's last reboot.

The value of these columns is updated every 5 minutes.

Similar columns are added to the RADIUS User table. You can track the timestamp of the most recent interactions between a RADIUS user and the RADIUS server.

These **RADIUS User** columns include:

- The **Last Interaction Time** column displays the local timestamp for the most recent interaction between a RADIUS user and its associated RADIUS server. If the RADIUS user has no connected physical device, the value in this column may be empty.
- The **Failed Login Attempts** column displays the count of unsuccessful login attempts made by the RADIUS user since the server's last reboot.
- The **Successful Logins** column displays the count of successful logins of the RADIUS user since the server's last reboot.

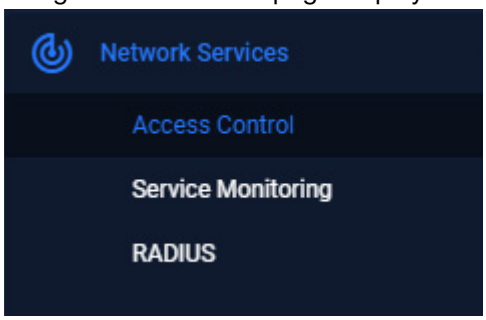
You can sort the table data by the column types. The RADIUS users table will refresh when there are user changes on the RADIUS server, for example, user creation or user deletion.

Network Services

Access Control list

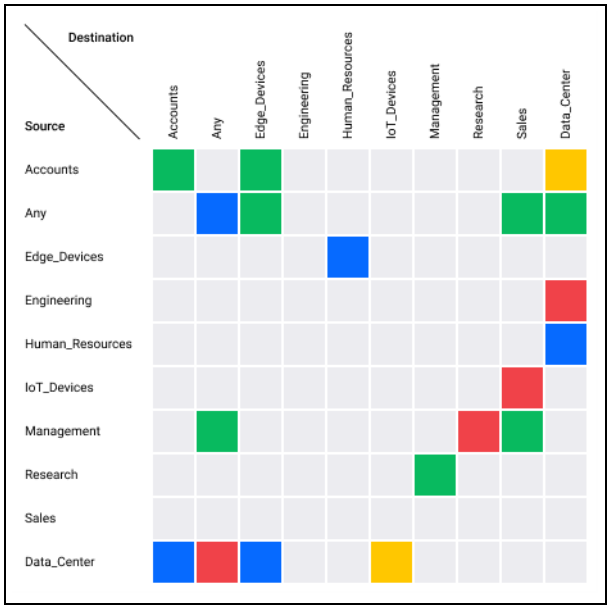
The Access Control List (ACL) matrix provides a visual representation of the Access Control Lists applied to your network.

To view the Access Control List matrix, select **Network Services** > **Access Control** from the navigation menu. This page displays the Access Control List matrix.



Using the Access Control List matrix 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.

The axes of the Access Control List matrix show the source/destination IP host groups discovered across the network. Each host group contains one or more hosts or subnets. You can use a host group 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.

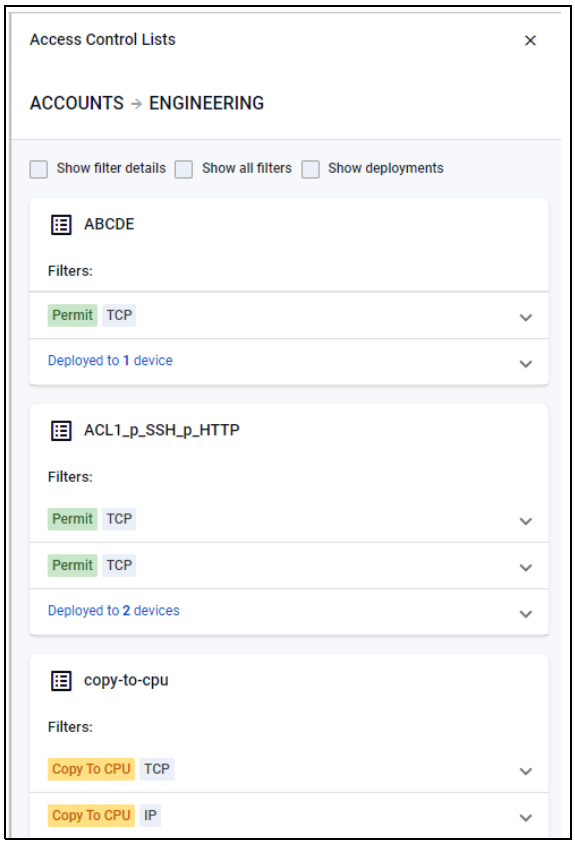


Click on a colored cell to learn more detail about the ACLs with the cell's matching source and destination groups. When you click on a cell, the Access Control Lists side-panel will expand, and show deployment and filter details. These details include:

- the filter type and action.
- any source, destination, or port group configuration.
- a section where the access control list is deployed.

Any Access Control lists with identical names and configurations are combined in the side panel.

For example, if ten switches have the same ACL, it will appear only once in the side panel. You can click on the Filters section to reveal where the ACL is deployed. If there are no interfaces listed, the ACL exists but is not deployed to any switchports.



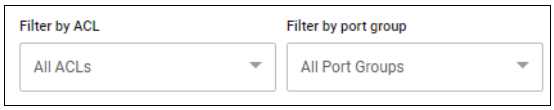
An Access Control list can contain multiple filter lines. Each line starts with a single action (Permit, Deny, etc), then the filter type, followed by the source and destination matching criteria. Rather than using a host group, you can use 'any' for a wildcard match for source and/or destination.

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.

ACL and port group filters

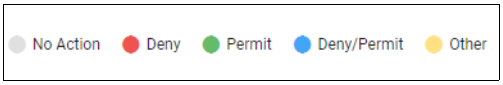


Two selection filters are available above the Access Control List matrix.

- **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 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.

Cell color key

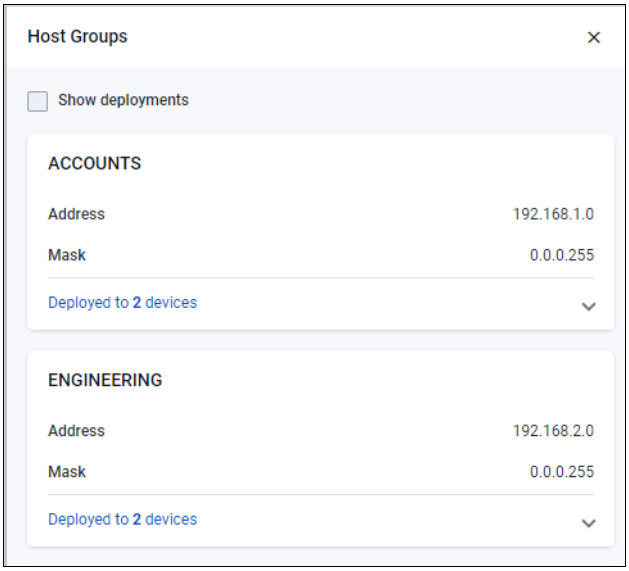


The color of each cell indicates if a matching Hardware ACL has been found for that combination of Source and Destination host groups. The cell colors show the following conditions:

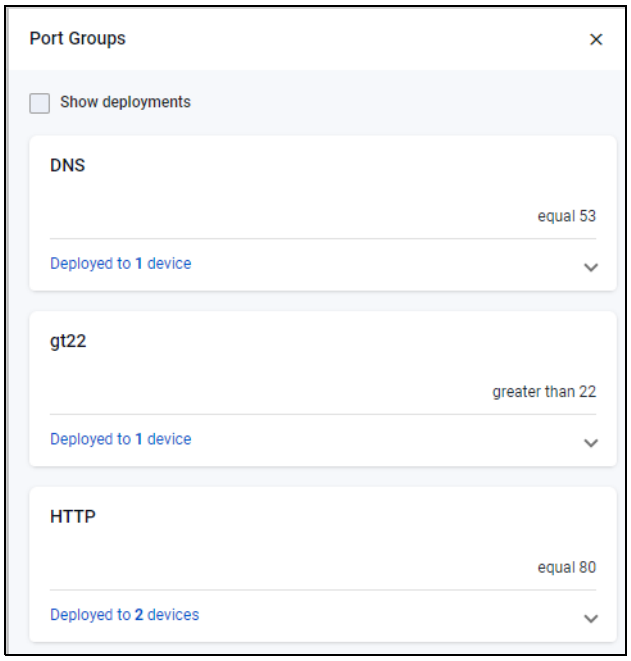
Cell Color	Condition
Red	At least one deny filter is deployed in a hardware ACL for the source/destination cell combination. There are no permit filters configured for the source/destination combination.
Green	At least one permit filter is deployed in a hardware ACL for the source/destination cell combination. 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.

Host groups and port groups buttons

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

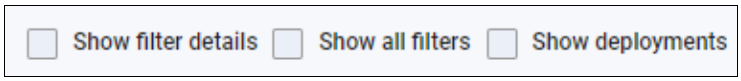


Host groups define one or more lists of hosts using the **acl-group** command. These hosts can have masks in the same way hosts specified in existing ACLs do. The Host groups button shows details of the host groups, and where they are deployed.



Port groups 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.

Filters and deployments



There are several check boxes that provide additional information.

- **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.

Creating new hardware ACLs

You can create use the Alliedware Plus CLI to create hardware ACLs and associated host/port groups on a switch. 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
```

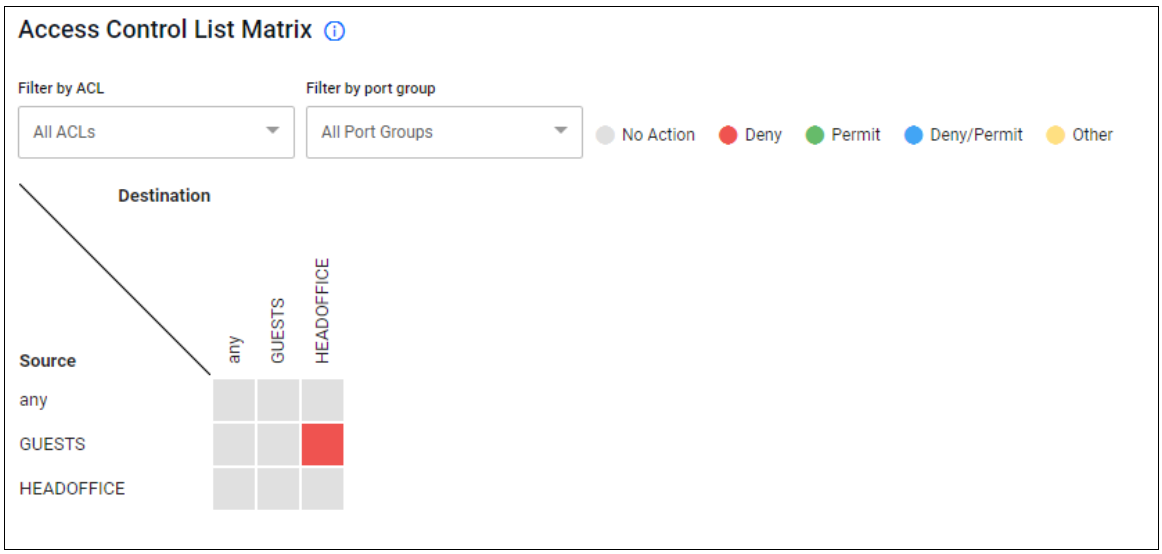
3. Create the hardware ACL to deny TCP packets matching port group SSH from source host group GUESTS to destination host group HEADOFFICE.

```
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:



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
```

Service monitoring

As an administrator, you can use Service Monitoring to learn the status of services running on devices within Vista Manager. 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.

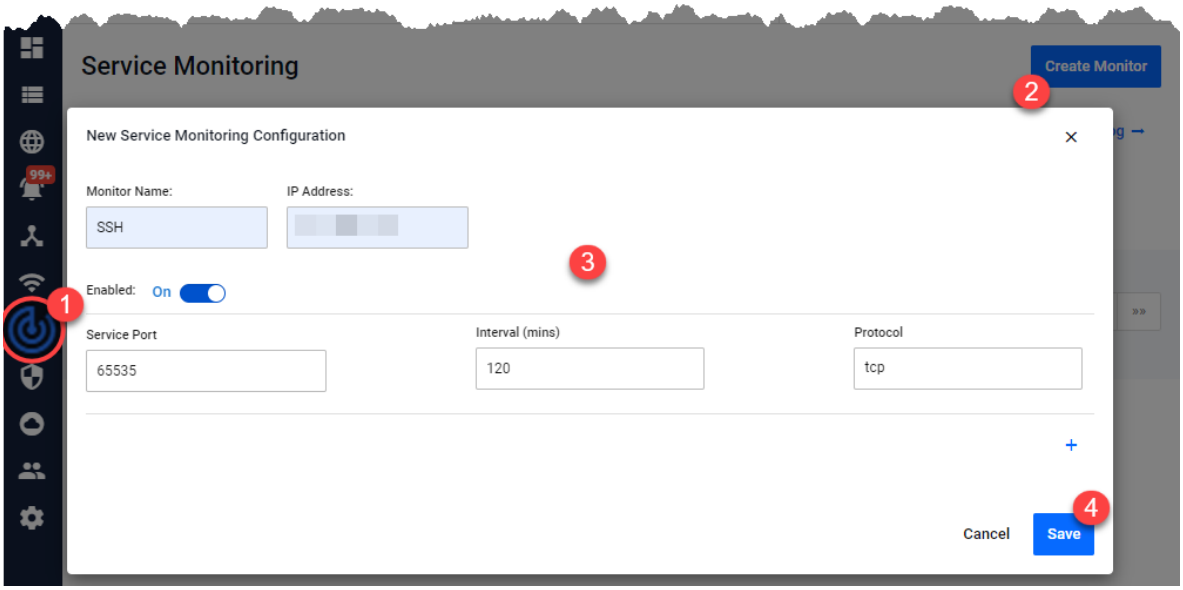
A user that is set to read-only cannot select the ‘Create Monitor’ button, and can only view the contents of the page.

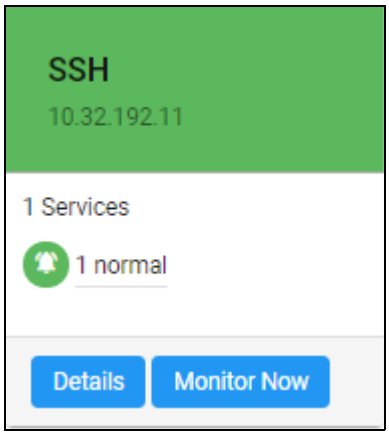
You can change permissions for Service Monitoring on the User Management page.

Creating a monitor

To create a monitor:

1. Click on the **Service Monitoring** section 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 - either TCP or UDP
4. Click **Save**.



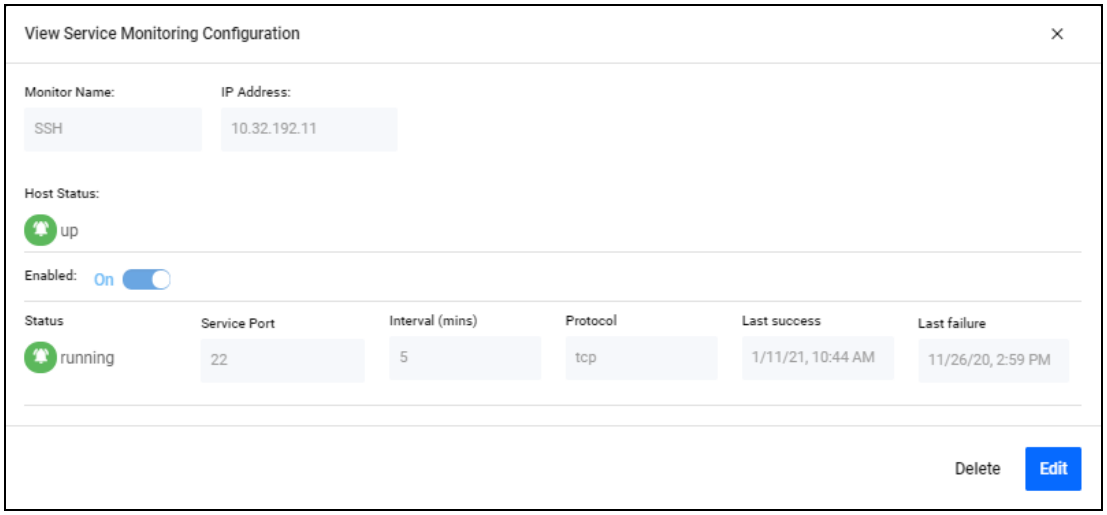


The monitor has now been created and will be displayed on the service monitoring page. Click on **Monitor Now** to begin monitoring the service.

Service Monitoring statuses

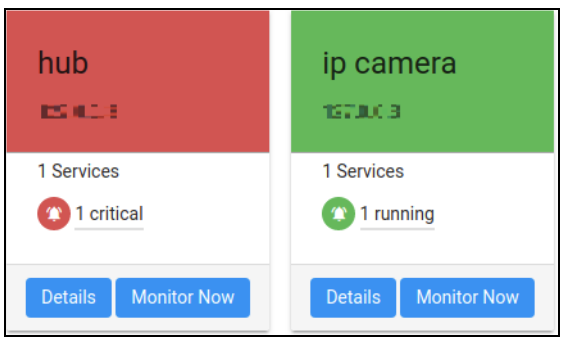
The service statuses may be one of the following:

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

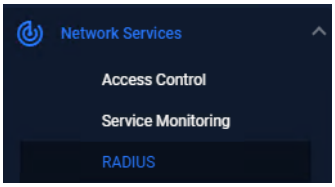


The status categories and the statuses that fall into each category are as follows:

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



RADIUS

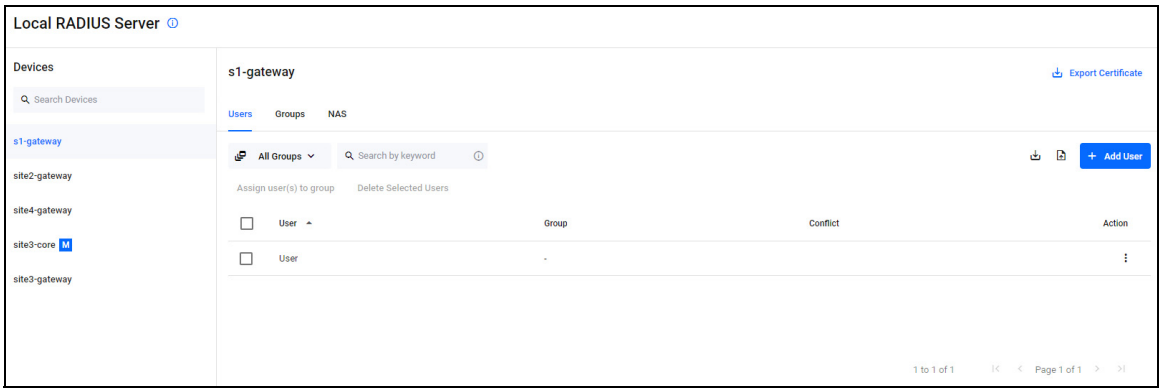


The main purpose of RADIUS (Remote Authentication Dial In User Service) is to enable the authentication of network users stored in a database on a server known as a RADIUS server. You can access RADIUS from the Network Services drop-down.

When users connect to the network, the device (usually a switch) the users connect to can challenge the users for authentication, and pass on the authentication to the RADIUS server to check. Based on the result of the check against its database, the RADIUS server informs the switch whether or not to allow the connected user access to the network.

From version 3.12.0, the New Edge Security feature has added the Endpoints category to the Asset Management page, which shows clients on your network. A local RADIUS server works to easily authenticate devices from the table on this page. To see more information about Endpoints, see "Firmware" on page 173.

For more information about RADIUS, see the RADIUS Server Feature Overview and Configuration Guide.



Local RADIUS Server

RADIUS lets users view and edit local RADIUS server configurations on AlliedWare Plus devices. The RADIUS page displays a list of all AlliedWare Plus devices with local RADIUS enabled. In some situations, like a remote branch office, it is convenient to use an AlliedWare Plus™ switch as the RADIUS server for user and device authentication, rather than to have another, separate RADIUS server. Hence, RADIUS server capability is provided as a built-in feature of AlliedWare Plus. The built-in RADIUS server is referred to as Local RADIUS server.

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

You can view a list of devices with RADIUS server enabled, and view the RADIUS server configuration of a RADIUS server–enabled device.

You can also import or export RADIUS user settings to or from a device, as well as edit the RADIUS server user/group configuration of a device.

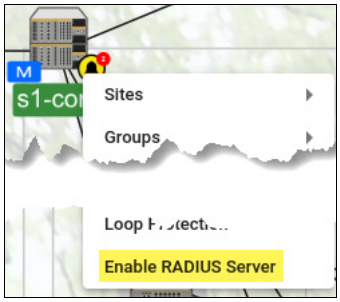
Share multiple RADIUS entities from one device to another by first exporting CSV files, editing them offline, and importing them onto the new device.

Users need read/write permissions to use RADIUS settings, for information on setting up user permissions see "User Management" on page 305.

Enabling Local RADIUS on devices

You can enable local RADIUS on devices from the network map.

To enable/disable RADIUS server on a device, right click on a device to bring up the context menu for the device on the **Network Map:**

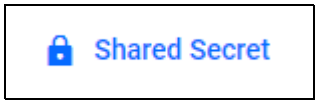


For information on how to do this, see "Enabling RADIUS on devices from the Network map" on page 64.

Shared Secret

The Shared Secret button appears on the RADIUS page from version 3.12.0 onwards, in order for the endpoints feature to work.

To set a shared secret, click the **Shared Secret button** in the top left of the RADIUS page.



The Shared Secret key is used by the Vista Manager to send a CoA (Change of Authorization) message to the NAS device. For more information see "Intelligent Edge Security (IES)" on page 187.

Adding RADgate as an external RADIUS Server

From version 3.13.1 onwards, Allied Telesis' new RADIUS application RADgate is supported as a plugin in Vista Manager. This means you can add RADgate as an external RADIUS server and manage it from Vista Manager.

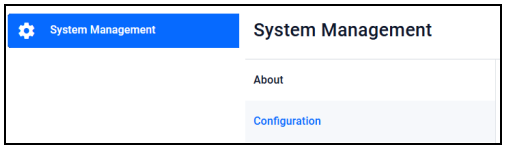
RADgate runs as a separate application, and can be accessed directly from Vista Manager for any advanced configuration. For more information about RADIUS, see the RADIUS Feature Overview and Configuration Guide.

Note: The AT-RADgate RADIUS server is not yet available in all regions. See your Allied Telesis representative for more information.

As a Vista Manager plugin, the RADgate user database and information are synced to Vista Manager for an integrated view and simplified user access management. To use RADgate as part of Vista Manager's Intelligent Edge Security (IES) solution an AMF Plus license is required.

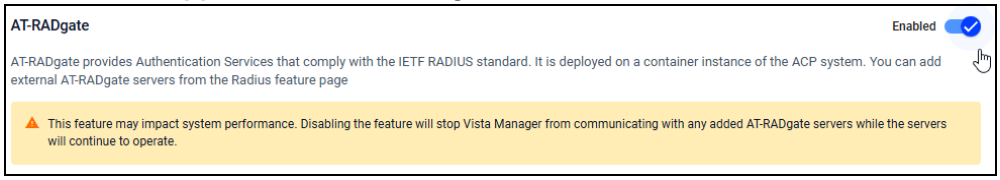
The following steps describe enabling RADgate as a Vista Manager plugin, and adding it as an external RADIUS server.

1. Go to **System Management** > **Configuration**



2. Scroll down to **Optional Features**.

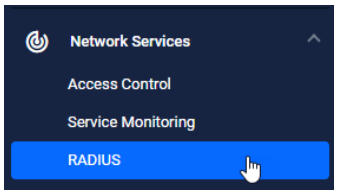
3. Use the **Toggle** to enable AT-RADgate:



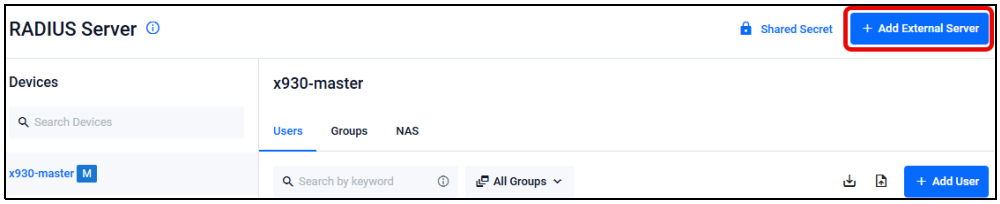
4. The RADgate feature is now enabled.

To add an External RADIUS Server for RADgate:

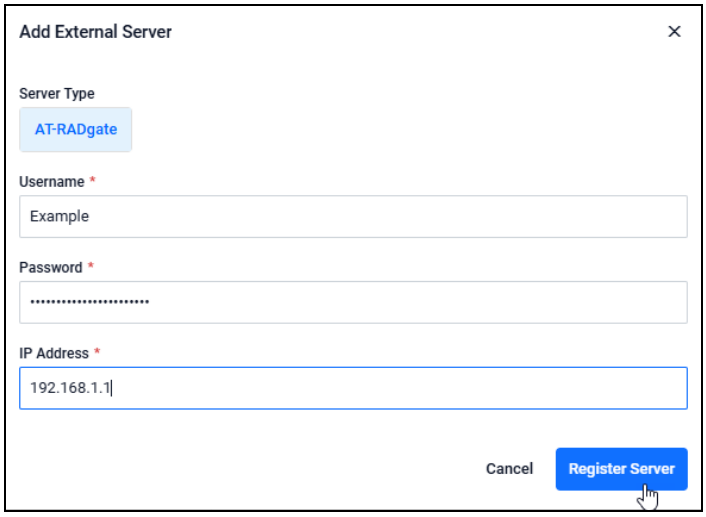
Go to the **Network Services** > **RADIUS** page



Click the + **Add External Server** button



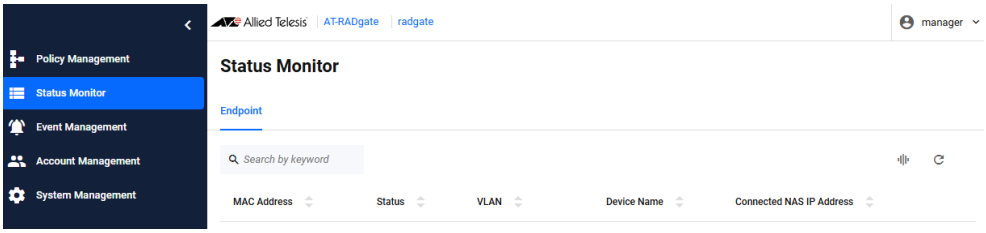
Enter the server credentials and IP address



Click **Register Server** to add it to Vista Manager.

- The server will appear in the side panel. You can freely add users from the RADIUS page, and they will display in Vista Manager as well as in the RADgate application.
- The newly added server also appears as a device on the Network Map.
- You can delete the RADgate server by clicking the Delete button on the RADIUS page, but you cannot delete local RADIUS servers.

To check information about the RADIUS Server, please check the RADgate application. To do this, **right-click** on the RADgate server device icon on the map.



Note: If you disable the AT-RADgate feature from **Optional Features**, it will disconnect from Vista Manager. However, if you re-enable the feature from Vista Manager, then the connection to AT-RADgate servers will be resumed.

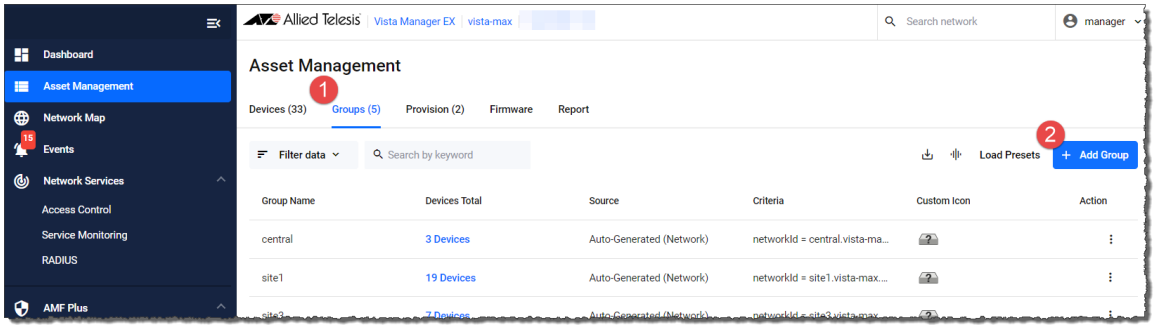
Managing multiple RADIUS devices with groups

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

Previously, you could manage individual devices, but you needed to configure each device one by one. With this update, you can manage Vista grouped devices in the same way as is currently possible for a single device.

First, create a group in the **Asset Management** page:

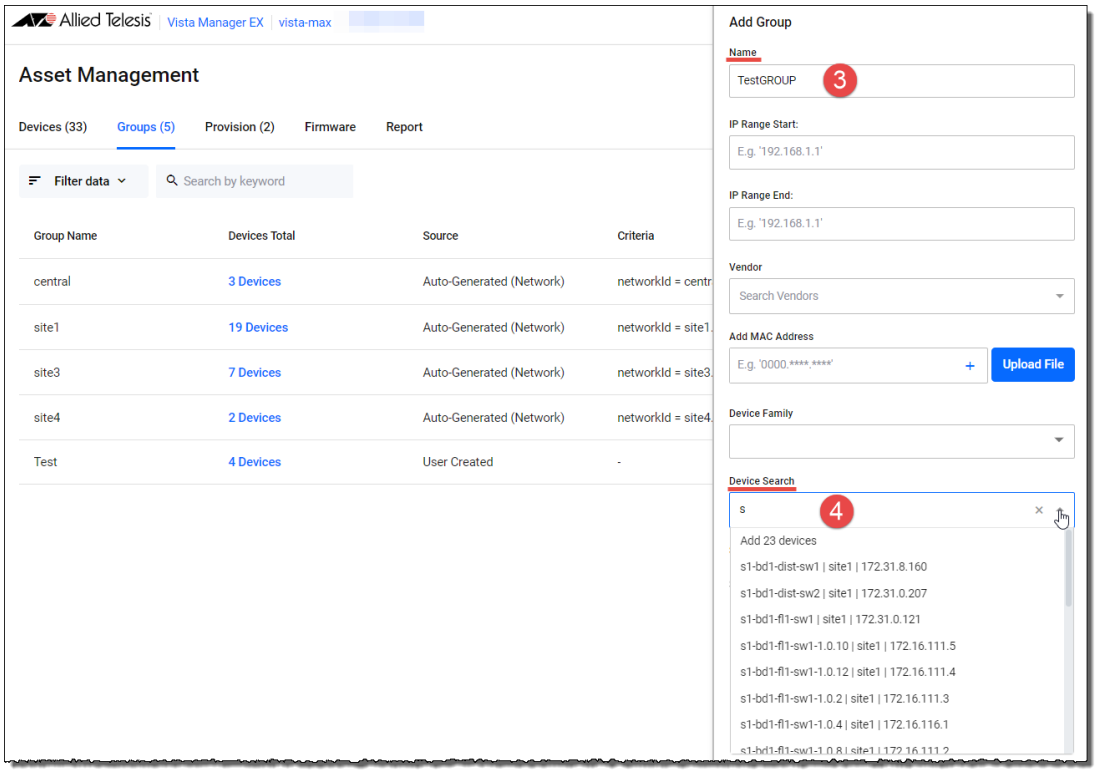
1. Create a group of devices for RADIUS:



1. Go to **Asset Mangement** > **Groups** and click **+Add Group**
2. Enter a group **Name**.

3. In the **Device Search** field, start typing a device name.

4. A drop-down list appears. Each device is added one-by-one under **Static Devices.**

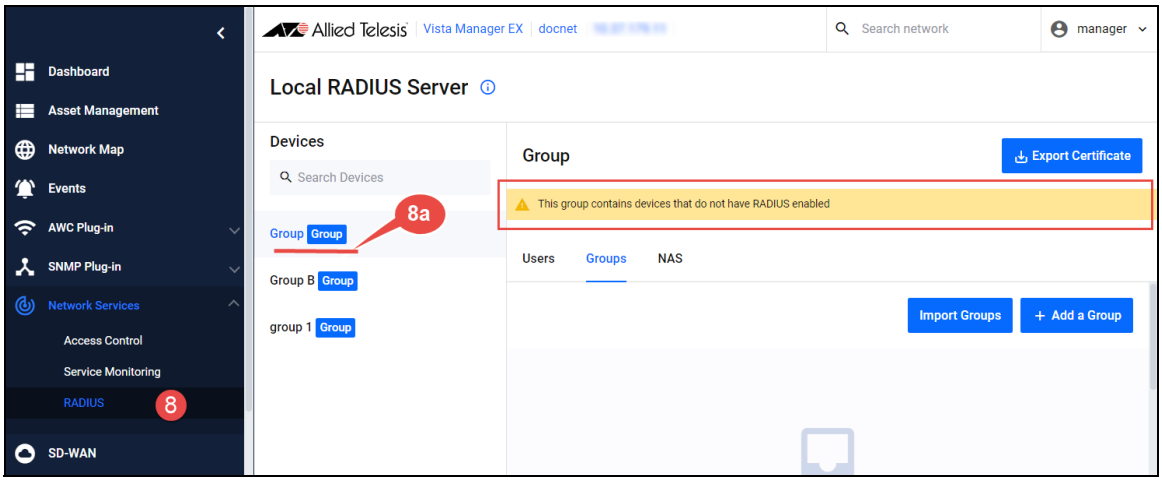


5. Select the devices you want to add under the **Device Search** heading. The selected devices will display under the heading.

6. Click **Save**.

7. Go to **Network Services** > **RADIUS**

8. From the RADIUS page, you can see the newly created groups..



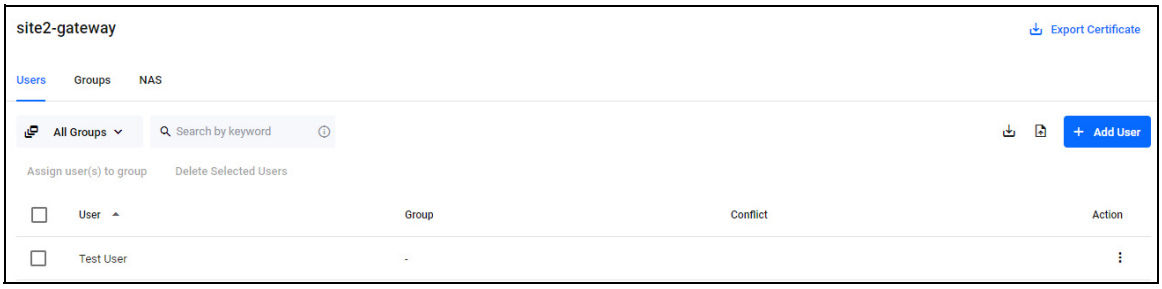
If you see the yellow warning banner at the top of the page with the text: "***This group contains devices that do not have RADIUS enabled***", then you need to enable local RADIUS server on these devices. To enable RADIUS on devices, see "Enabling Local RADIUS on devices" on page 210.

Step 8a. Click a group to configure.

The following sections describe the Users, Groups, and NAS tabs on the Local RADIUS Server page.

Users

From the **Users** tab, you can import or export CSV files of user lists, and add users from site devices on the side.

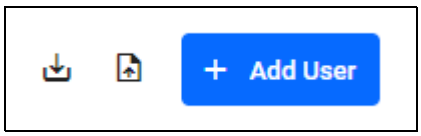


The **Users** tab allows you to:

- add/edit/delete users to the local RADIUS server of a selected device.
- import/export multiple user entries to/from a device.
- manage users assigned to RADIUS groups.
- export RADIUS user information to your local PC in pk12 format.
- export the local CA certificate to a local PC.

To configure RADIUS Users:

1. Click **+ Add User**



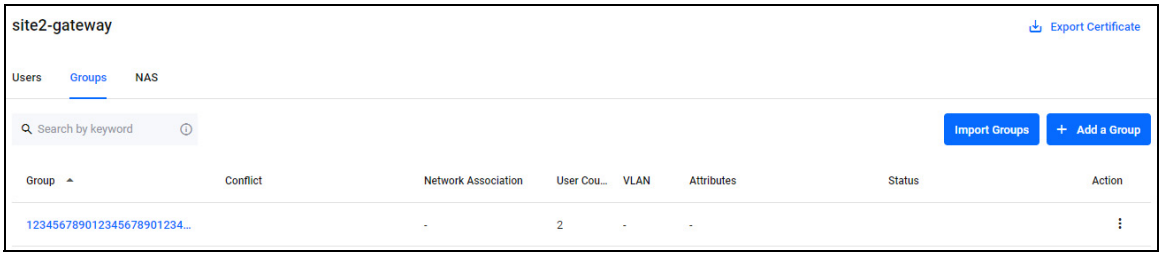
2. Input name of user (This will be MAC address if doing port authentication).
3. Input password of user (This will be MAC address if doing port authentication).
4. Optional - Select a Group that user will belong to.
5. Click **Save**

RADIUS clients that you interact with on the Endpoint section of the Asset Management page are listed as User entries on the RADIUS server, and you can see their status when you click on the NAS device on the sidebar. If the client devices are blocked, the Status column will show a Reject badge, otherwise nothing will display.

To see information about how endpoints work in Vista Manager, see "Firmware" on page 173.

Groups

Groups on the RADIUS page are listed under the Groups tab. You can add groups from the table on this page.



The Groups 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, manage, and 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:

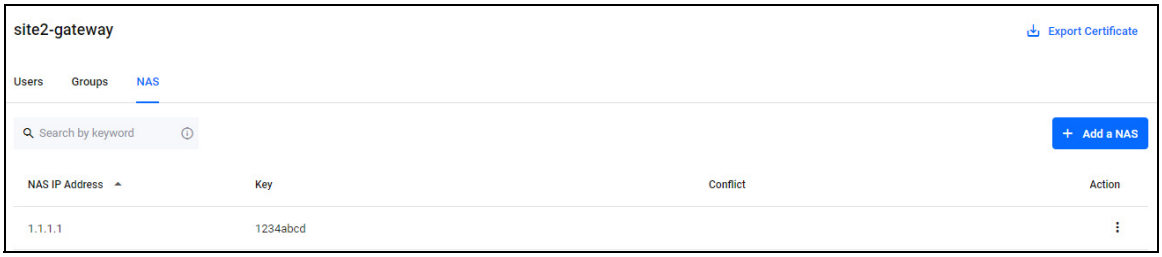
- see all attributes for a group
- add/delete one or multiple attributes of a group.

To Configure a RADIUS group:

1. Click **+ Add a Group**
2. Input the name of the group
3. Optional - Input dynamic VLAN to be used for this group
4. Optional - Add Radius Attribute key: value info and click **+**
5. Repeat the above step for each attribute to add
6. Click **Save**

NAS (Network Access Server)

A Network Access Server (NAS), also known as a RADIUS Client, or simply an authenticator, is a device on a network that is used for authentication. When a user requests network access, the Network Access Server initiates RADIUS communication.



You can add a NAS by supplying a device IP Address and a key.

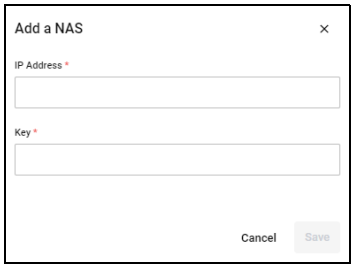
The **NAS** tab allows you to view, delete, or add a NAS to the local RADIUS server of a selected device.

Click the **+ Add a NAS** button to add a NAS by supplying the device's IP Address and a NAS Key.

Note that the key on a NAS Device is different to the Shared Secret key that you set up in RADIUS.

- The NAS key is to connect a NAS device to RADIUS. It is used to identify the NAS device.
- The Shared Secret enables Vista Manager to send messages to NAS devices. It is used to identify Vista Manager as a dynamic authorization client (DAC).

You can manage up to 1000 network access servers.



For more information, see the RADIUS Server Feature Overview and Configuration Guide.

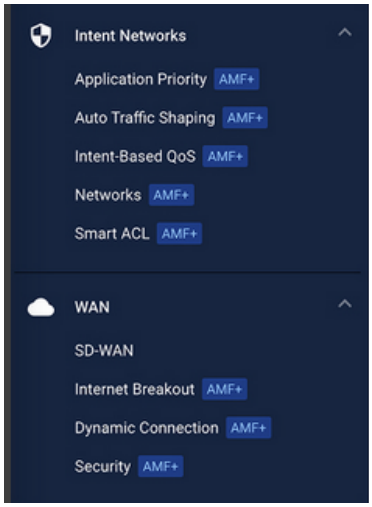
Using AMF Plus Features

Introduction

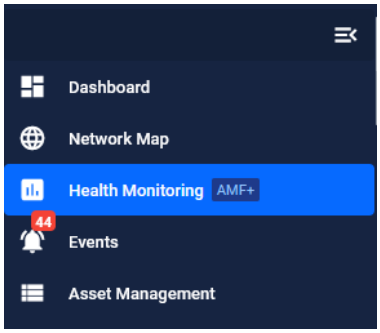
Allied Telesis Autonomous Management Framework™ Plus (AMF Plus) features provide network optimization, automation, management, and visualization. The uniquely designed intent-based configuration, reporting, and map facilities of Vista Manager EX make these powerful tools simple to configure, initiate, and manage.

In 3.14.0, AMF Plus features have been reworked, and Intent Networks replaces the former menu. To access AMF Plus features, navigate to the Intent Networks and WAN sections.

You can recognize if a feature is AMF Plus specific by the AMF+ badge in the left-hand menu.



Note that Health Monitoring has moved from the AMF Plus menu to above the Events menu item.



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?

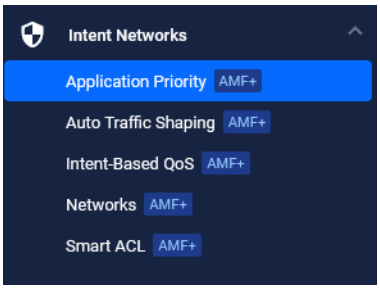
It is possible for an AMF Master/Controller to have a combination of both AMF and AMF Plus node/area licenses.

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.

Intent Networks Menu

The Intent Networks menu is made up of several tools to help you manage your network.



See the following sections for more information:

- "Application Priority" on page 220
- "Auto Traffic Shaping" on page 224
- "Intent-based QoS" on page 227
- "Networks" on page 264
- "Smart ACL" on page 265

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.

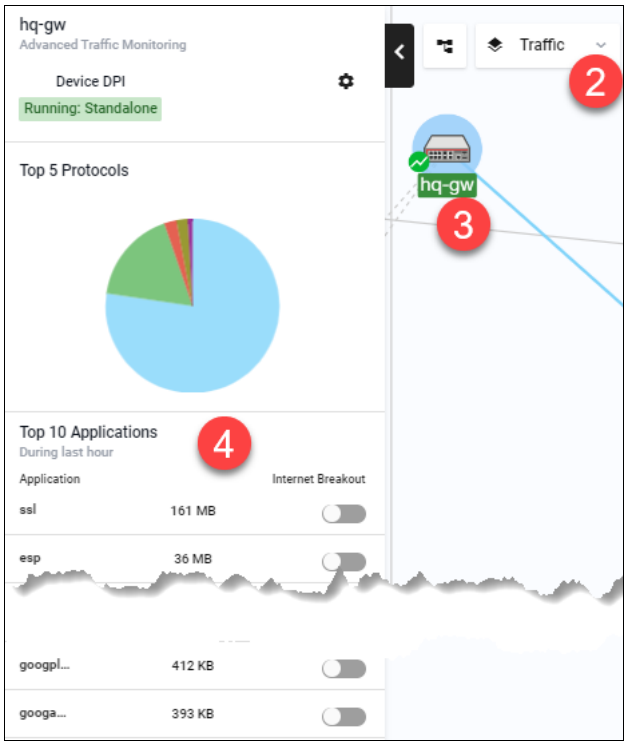
A policy is the overall title for a set of rules and priorities. It also defines the type of algorithm for how it calculates the priority of traffic. Traffic for any unassigned applications set in the rules will fall into the **Default** policy class. The default class is not directly visible when creating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



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.

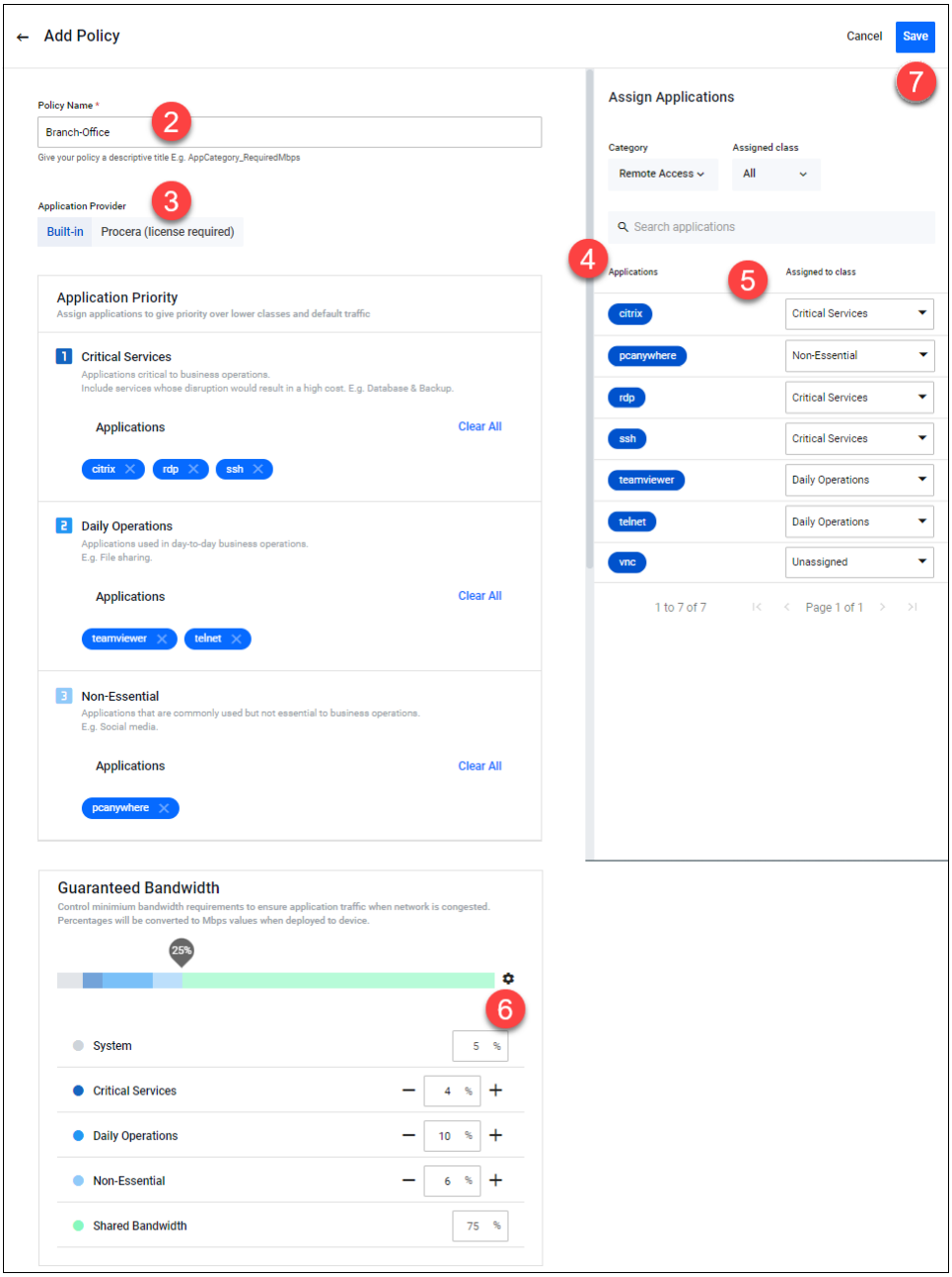
All of the above approaches open the **Add Policy** page.

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.

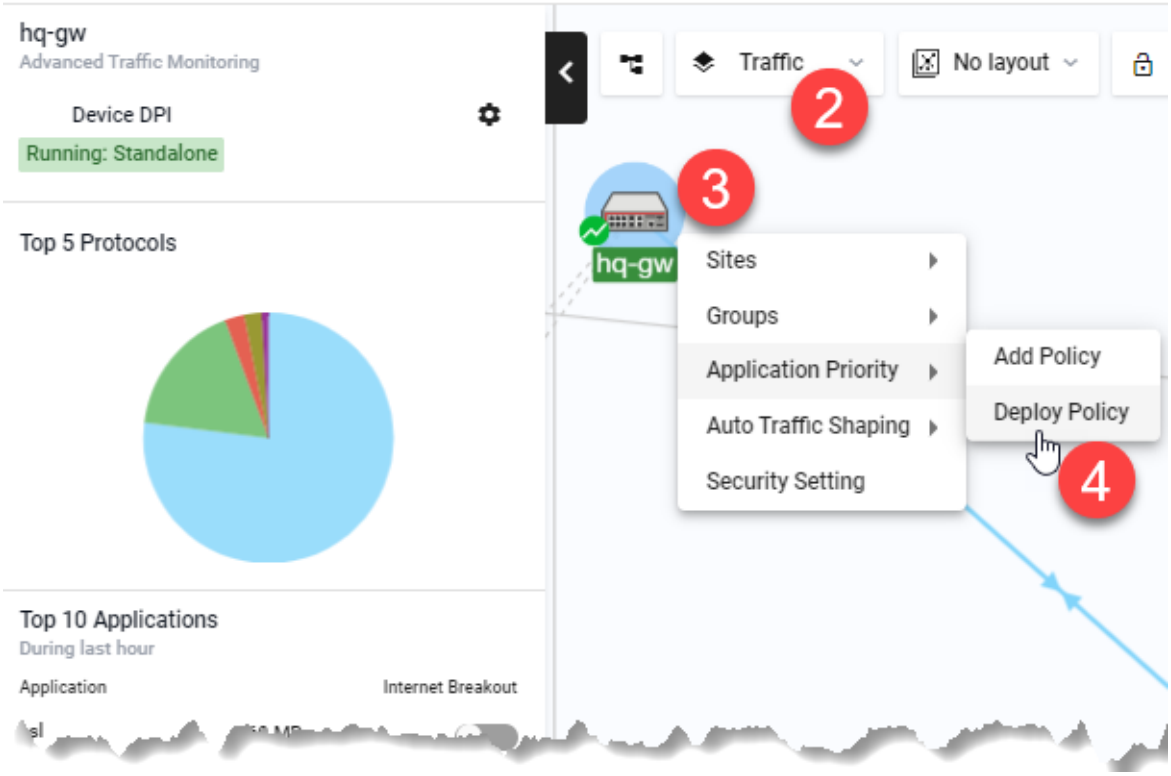
Note: The reserved percentage of guaranteed bandwidth for system traffic is displayed here. The 5% value is based on the default value that traffic control sets on a device. The actual value may vary depending on what device(s) the user deploys the policy on to. Vista Manager will just show **5% as the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

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



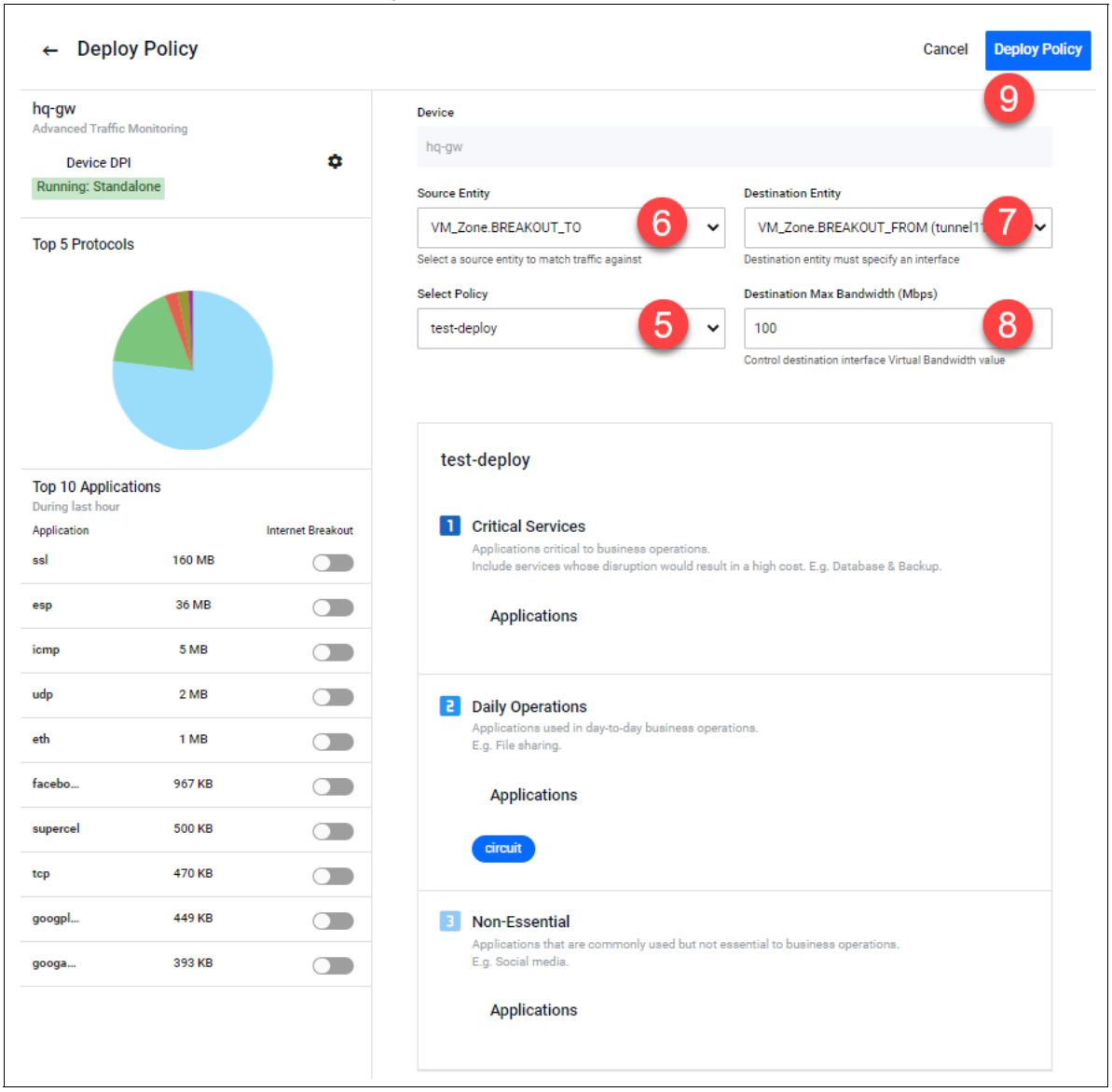
Step 3: Deploy a policy.

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.



Auto Traffic Shaping

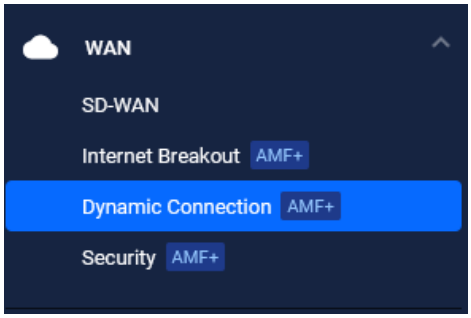
This feature dynamically adjusts the maximum transit capacity of remote locations (spoke tunnels) to not exceed the receive capacity of the central site (hub). This is termed the **maximum Rx bandwidth** of the hub.

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%.

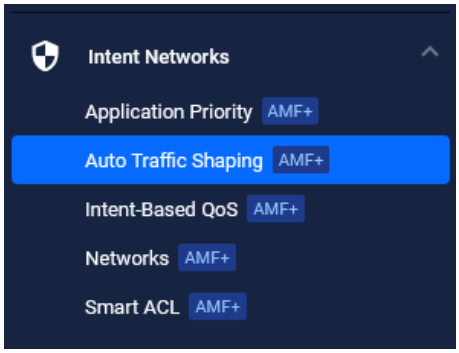
Prerequisite step: Configure tunnels between spokes and hubs.

To configure the tunnels, Go to **WAN** > **Dynamic Connection.**



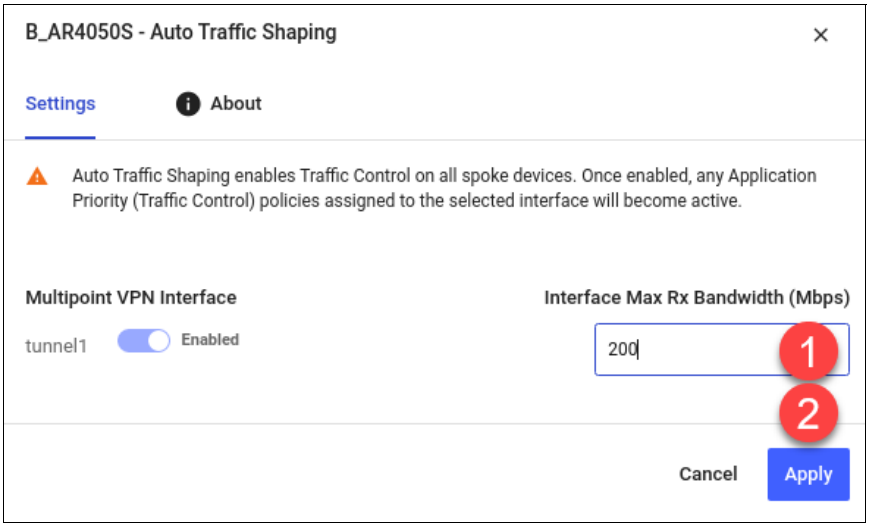
Step 1: Configure the Interface Max Rx Bandwidth value.

Go to the Auto Traffic Shaping page from the Intent Networks sub menu.



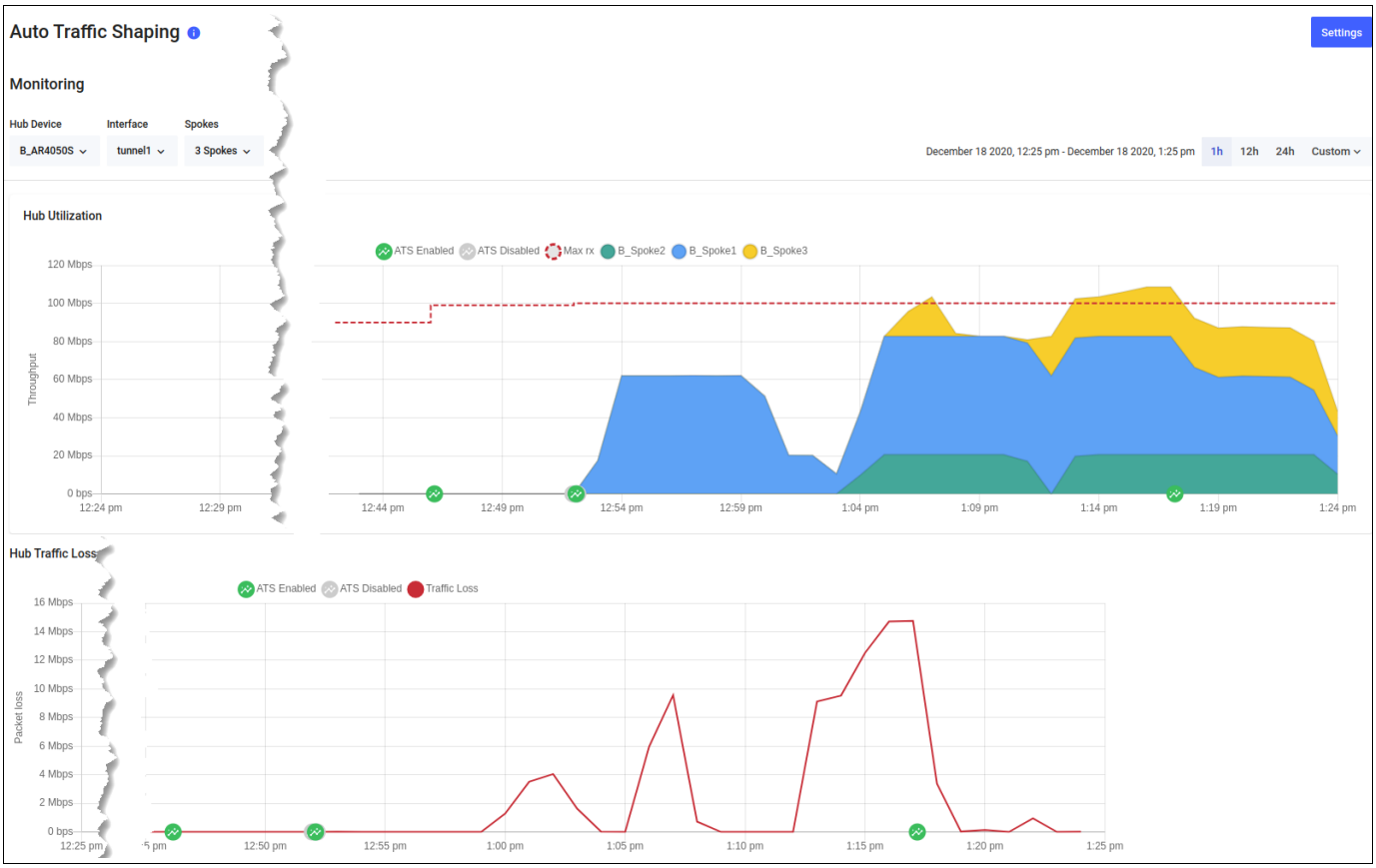
Click the blue Settings button.

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



Step 2: Monitor hub utilization and traffic loss.

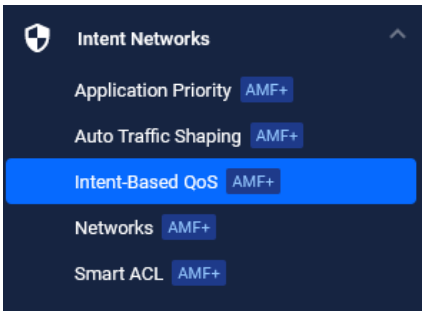
View charts in the Monitoring page, where you can use filters to specify what traffic is shown.



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

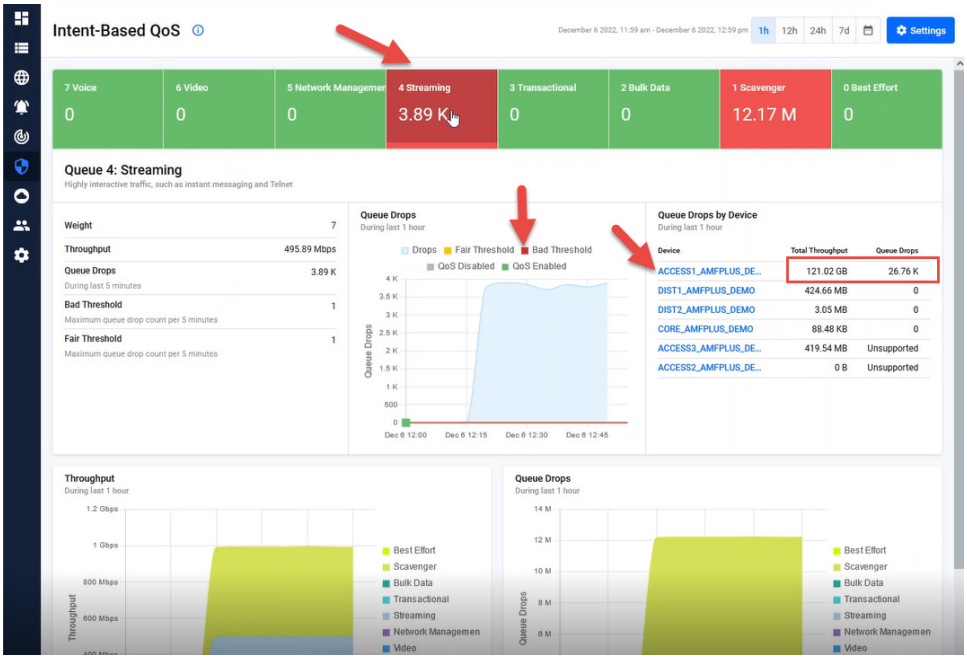
First you need to **manually** apply a default QoS configuration VISTA_DEFAULT_POLICY to all switches in your network. Please see "Configuring the Vista Manager EX default policy in the CLI" on page 243 for guidelines and some complete configuration examples.

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.



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.

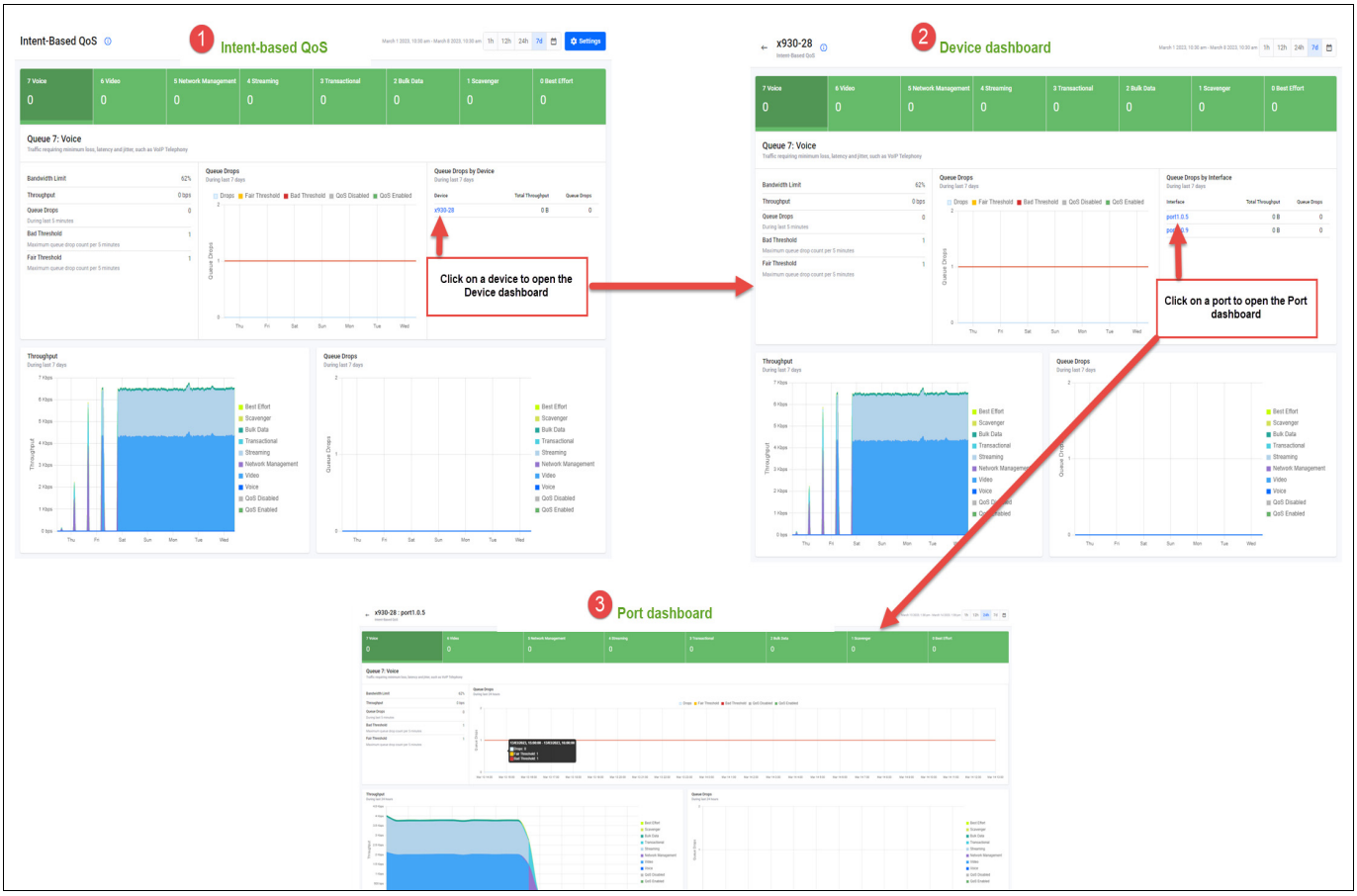
Using the Dashboards

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.

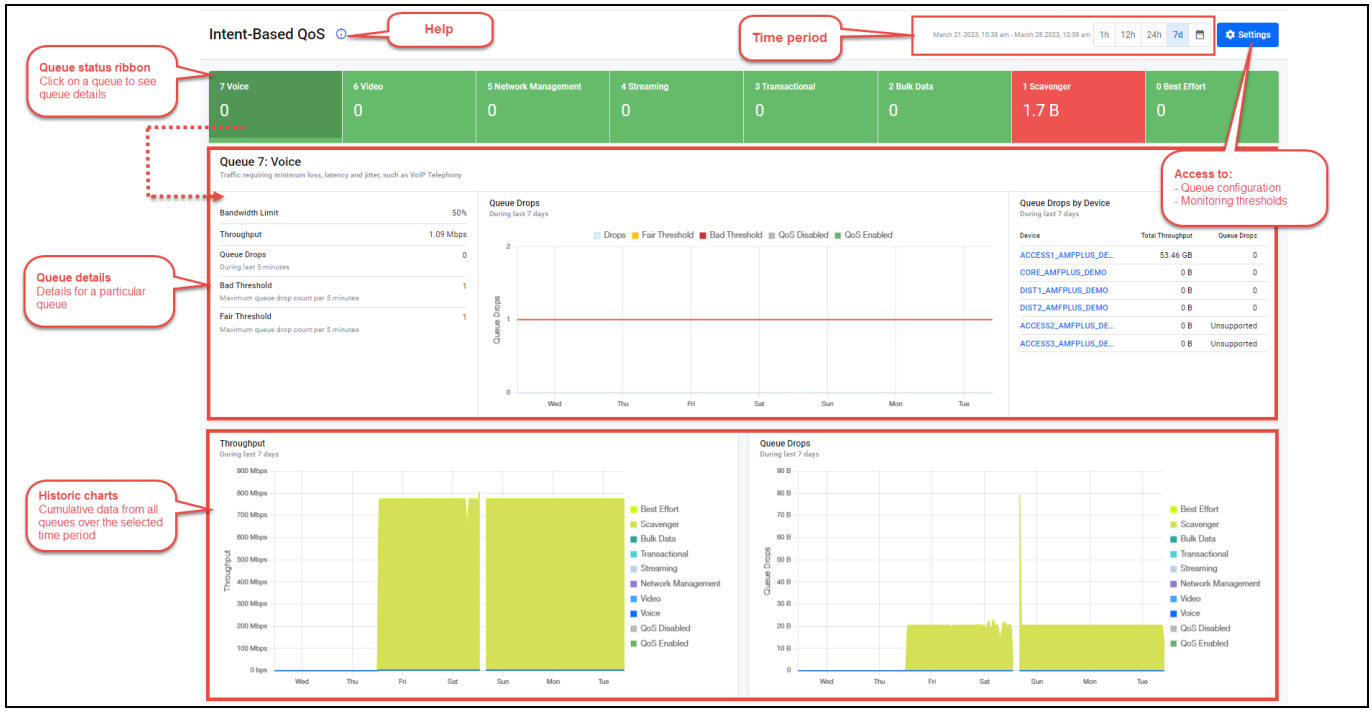
The three dashboards allow you manage QoS configurations on your network. You can use them to drill-down from a wide-angle view of the network traffic, select a device, and then select a port on that device.



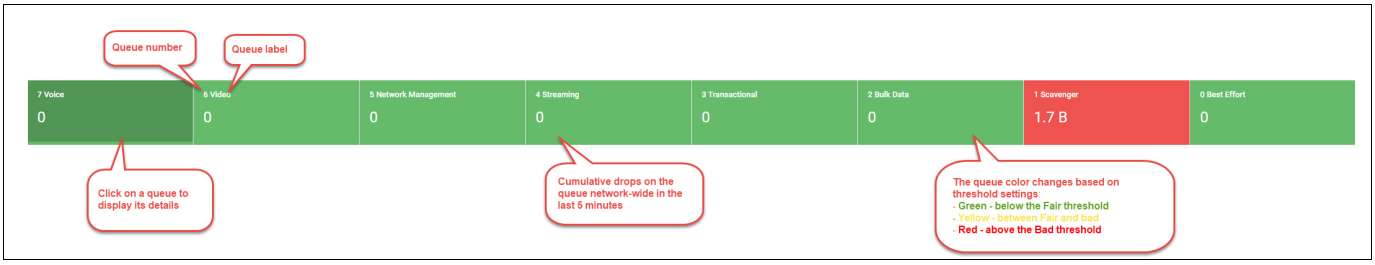
Navigating the dashboards

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.



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



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.

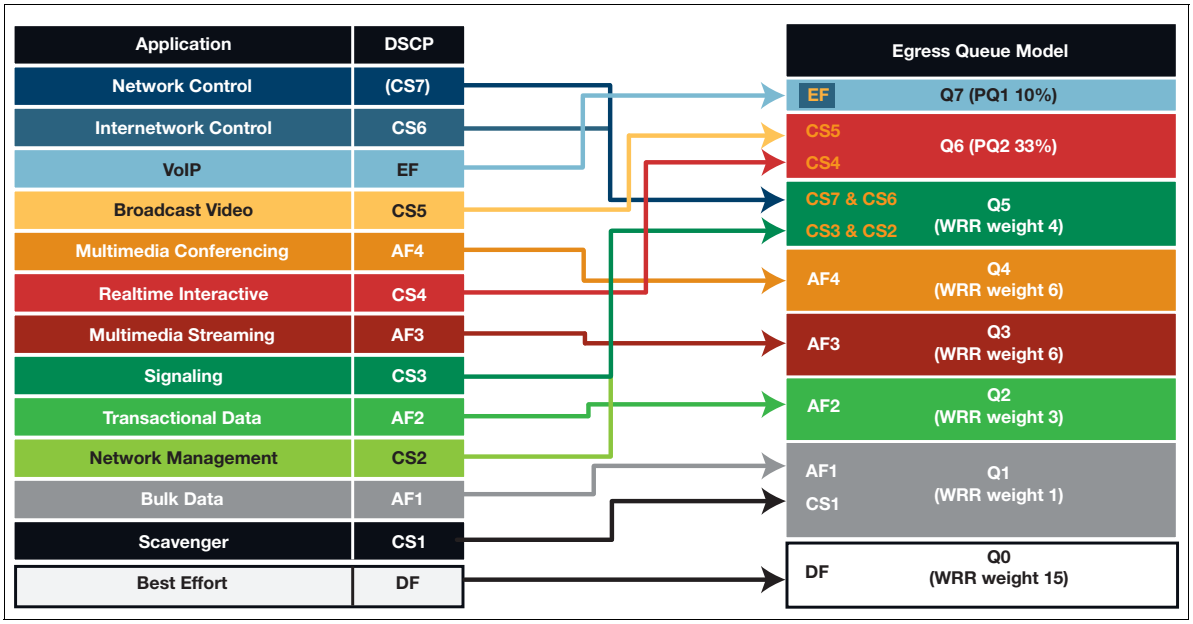
Where do the dashboard queue names come from?

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.

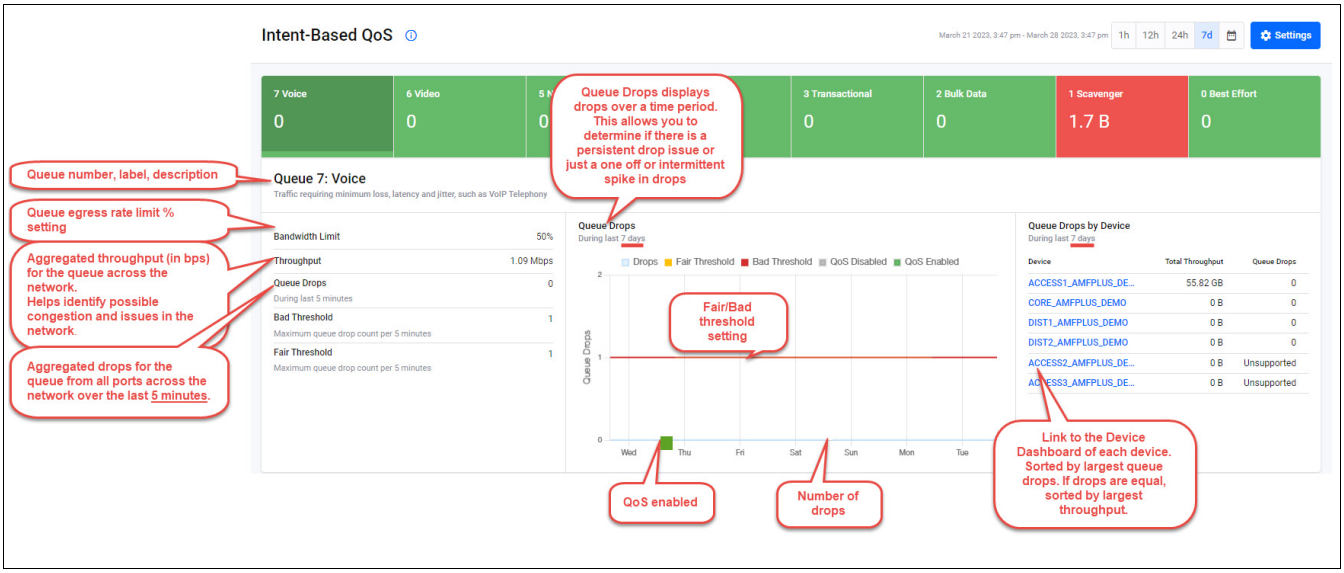
We recommended traffic is place into the correct queues, but there is no strict requirement. For example, there is nothing stopping you from putting Voice traffic into the Streaming queue. However, the labels in Intent-Based QoS cannot be changed.

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.



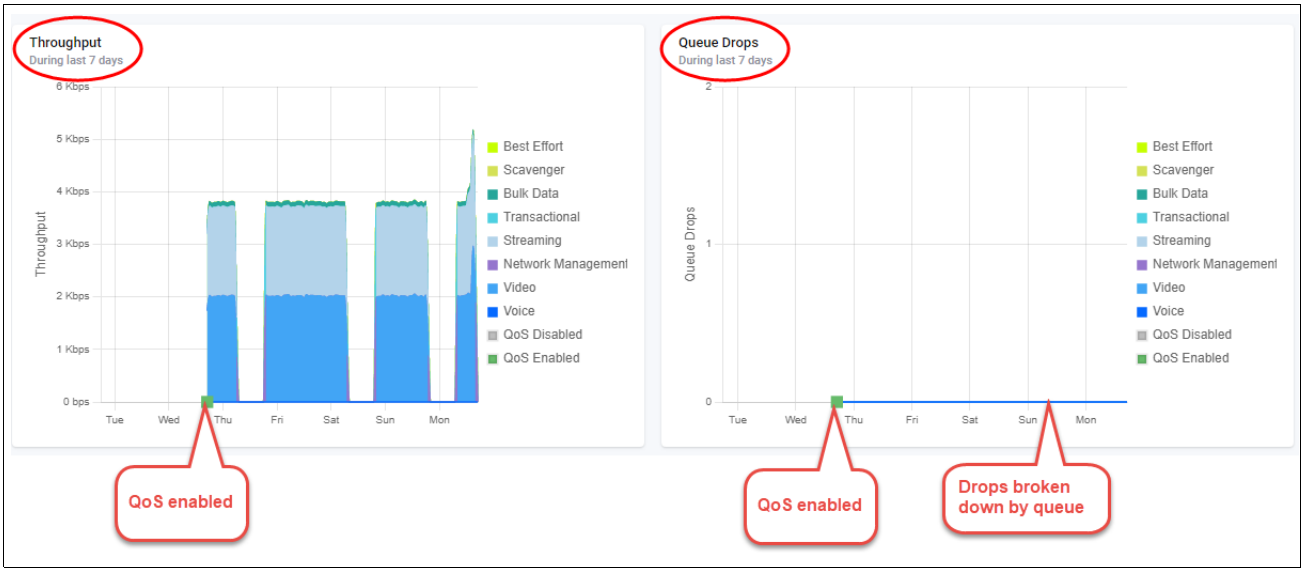
Queue details

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.



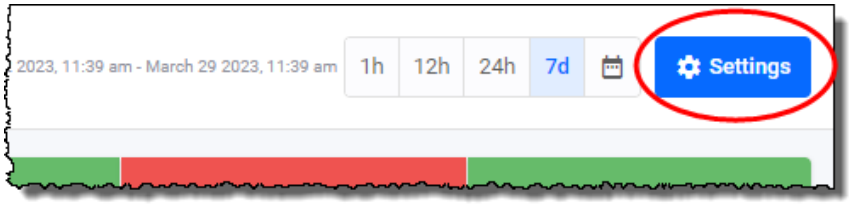
Historic charts

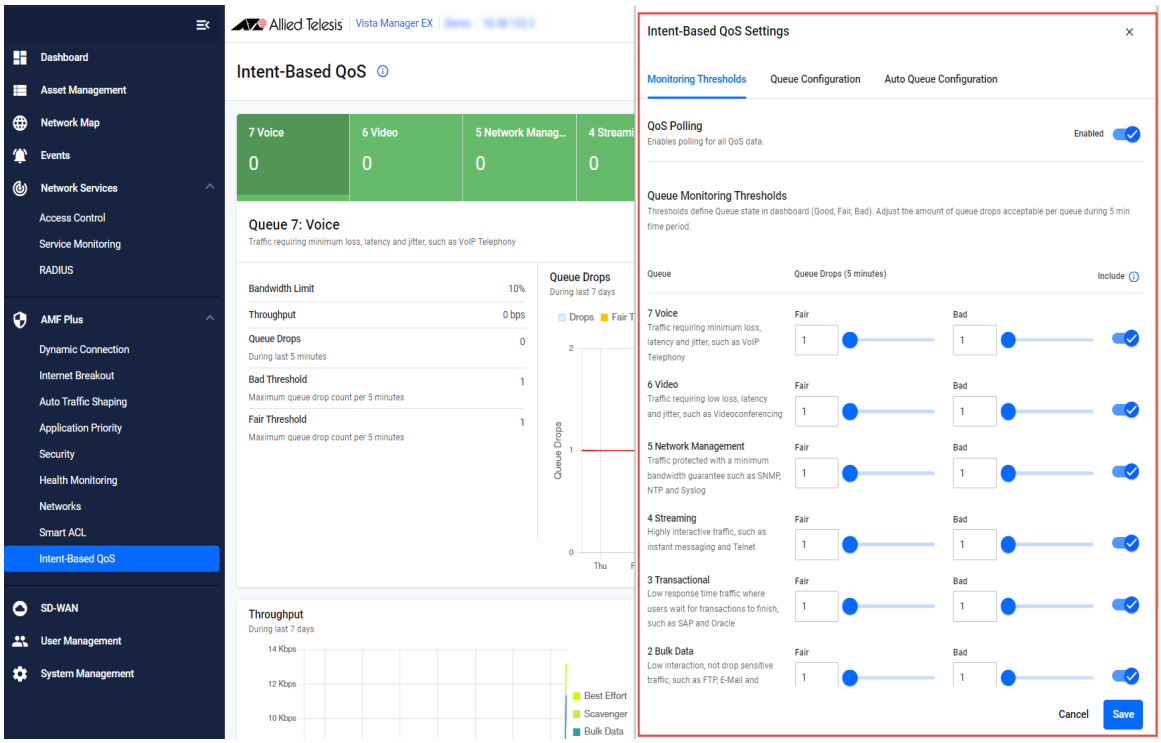
The historic charts display past details for all queues across all devices on the network. In the left chart below you can see the throughput per queue aggregated from ports over the selected time period, in this case the last 7 days. In the right chart, you can see drops per queue aggregated from ports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



Configuring the queue settings

Use the **Settings** button to access the **Intent-Based QoS Settings** window.





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.

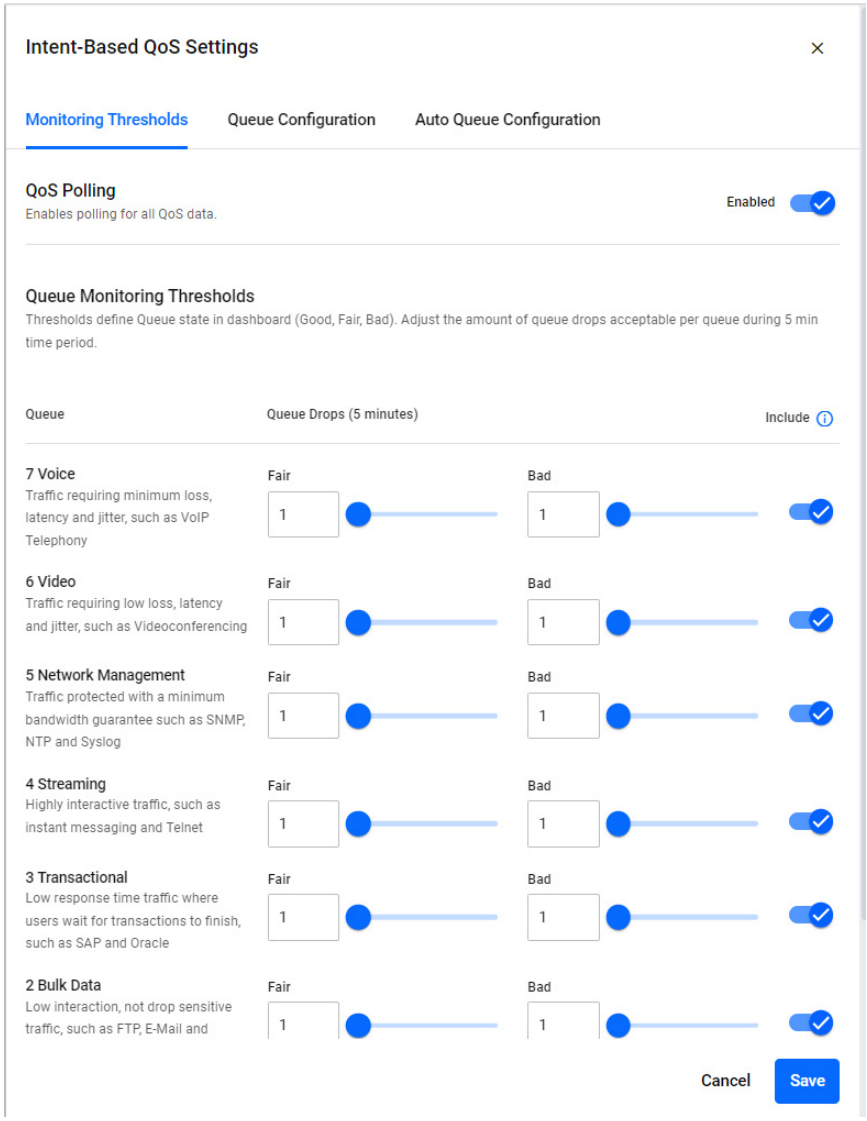
If you don't see a screen resembling the one shown above, where no data appears in the dashboard, it indicates that the default values have not been configured. You will need to use the CLI to configure these settings. This is described in the section "Configuring the Vista Manager EX default policy in the CLI" on page 243.

There are three setting tabs: **Monitoring Thresholds**, **Queue Configuration** and **Auto Queue Configuration**:

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.

Thresholds define the queue state display in the dashboard (Good, Fair, Bad). The thresholds are based on the acceptable number of dropped packets per queue during a 5-minute time period. You can set threshold values for each queue individually.



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.

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.

Priority queues send their packets first, in order of priority. This means that queue 7 sends packets until it is empty (or reaches its bandwidth limit), then queue 6 sends packets. Queues 0-5 only get to send packets when both queues of 6 and 7 are empty or have reached their bandwidth limit. If you don't restrict the queue bandwidths, the highest priority queues could stop the other queues from getting any bandwidth on particularly busy interfaces.

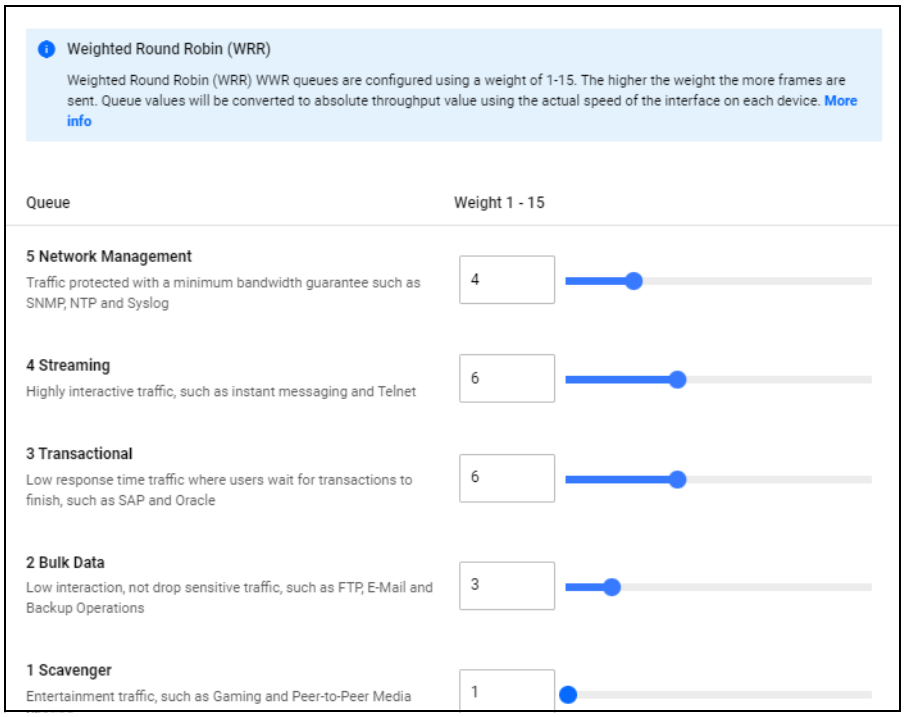
The settings allow you to limit the bandwidth used on the interface on each device, by setting the egress rate limit % value of the queue. This allows you to reserve bandwidth on the interfaces of the devices for other lower priority queues, which stops the highest priority queues from ever using all the bandwidth.

- You cannot set the egress rate limit to zero, because this is the same as disabling traffic flow from the interface.
- You can set the egress rate limit to 100%. This means that the queue in question will use as much of the egress bandwidth as it can, up to the capacity of the interface.
- If you set both Strict Priority queues to an egress rate limit of 100%, then the higher priority queue (7 - Voice) will use as much capacity as it needs. The capacity that queue 7 does not use is available for the lower priority queue (6 - Video), which will use as much of that remaining capacity as it needs.
- If you try to set the total egress rate limit to over 100%, Vista Manager gives you a warning, because this will allow the Strict Priority queues to "starve" the WRR queues if the strict priority queues' traffic demand uses all the interface bandwidth.

Weighted Round Robin (WRR) queue settings

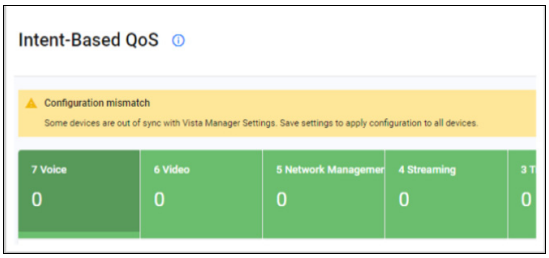
Use the Weighted Round Robin (WRR) queues for:

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



WRR queues have a weight of 1-15. The weights are relative to each other and work as ratios. When the egress interface is congested, a greater proportion of traffic is sent over queues with a higher relative weighting.

For example, a queue configured with a weighting value of 15 will send 15 times as much traffic as a queue configured with a weighting of 1 when the egress interface is congested. Likewise, if all queues are configured with a value of 15, all the queues will send the same amount of traffic. It is the relative difference that matters, so setting all queues to 15 is the same as setting all queues to 1.



Auto Queue Configuration tab

Autonomous Queue Configuration empowers you to automate QoS configuration changes across the network in response to changing traffic flows. If any queue's number of egress drops exceeds the 'bad' monitoring thresholds, the Auto Queues Configuration feature will adjust the resource allocated to that queue.

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

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

The priority queue optimisation algorithm

Each time the Autonomous Queue Configuration algorithm runs, Intent-based QoS inspects the egress queue drops for each priority queue in turn. These queue drops include all drops for the queue across the whole network.

If the queue is in a 'bad' state, Intent-based QoS increases the egress rate for the queue by 3%. It applies the new configuration to every QoS capable device in the network.

It determines a 'bad' state by summing all egress drops for the queue within each 5-minute monitoring period, since the algorithm last ran. This gives a number for each 5-minute period, called the “summed drops”. If the summed drops in any of the 5-minute periods exceed the 'bad' monitoring threshold, then the queue is considered to be in a bad state. You can change the monitoring threshold for each queue on the Monitoring Thresholds tab.

Intent-based QoS can automatically increase each queue up to the queue’s maximum egress rate.

The weighted round robin optimisation algorithm

Each time the Autonomous Queue Configuration algorithm runs, Intent-based QoS inspects the egress queue drops for each weighted round robin queue in turn. These queue drops include all drops for the queue across the whole network.

If the queue is in a 'bad' state, Intent-based QoS donates one unit of weight from a good queue to the bad queue. The good queue is called the 'donor' queue. The algorithm attempts to perform this transfer for all queues that are in a bad state.

It determines a 'bad' state by summing all egress drops for the queue within each 5-minute monitoring period since the algorithm last ran. If the summed drops in any of these 5-minute windows exceeds the 'bad' monitoring threshold, the queue is considered to be in a bad state. You can change the monitoring threshold for each queue on the Monitoring Thresholds tab.

The algorithm selects the 'donor' queue according to the following criteria:

- It must be in a good state, which means it has not exceeded the queue drops specified in its monitoring threshold.
- Its current weight must be greater than the minimum weight.
- Its current weight must be lower than the maximum weight.
- Among all the queues that satisfy the above criteria, the algorithm chooses the queue with the largest baseline surplus. The baseline surplus is the queue's initial weight minus the queue’s current weight.

The lowest priority queue which satisfies all these conditions is chosen as the donor queue. If no donor queue can be found, no weight will be transferred between the queues.

- If the recipient queue's current weight is already equal to its maximum weight, no weight will be donated to it.
- If the algorithm decides the weight must be changed, it applies the new configuration to every QoS capable device in the network.

You can limit the extent of the automatic weight changes by specifying min and max weights. Auto Queue Configuration will keep the queue weightings within those min and max weights.

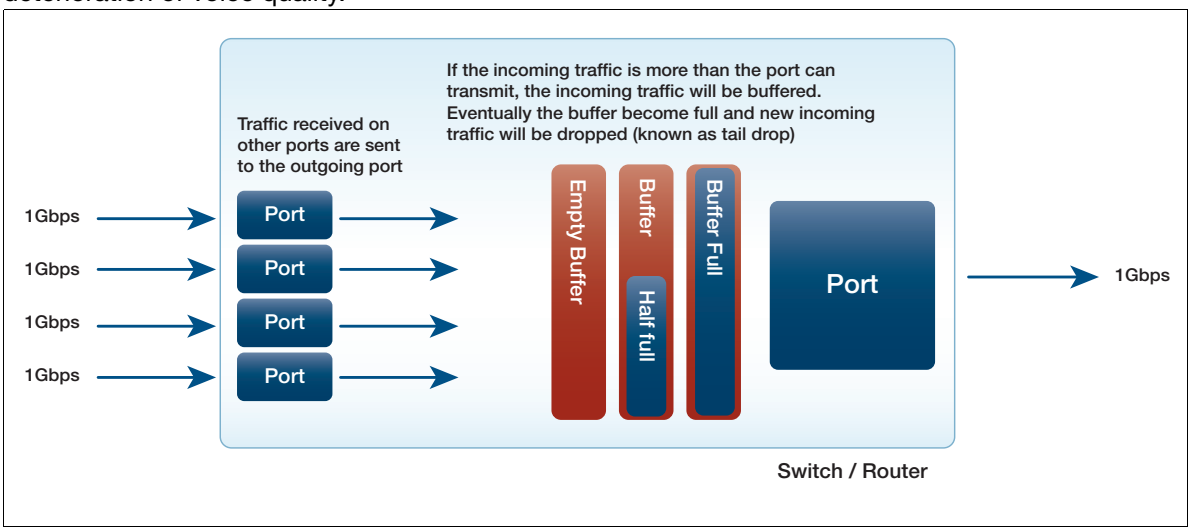
Port congestion

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.

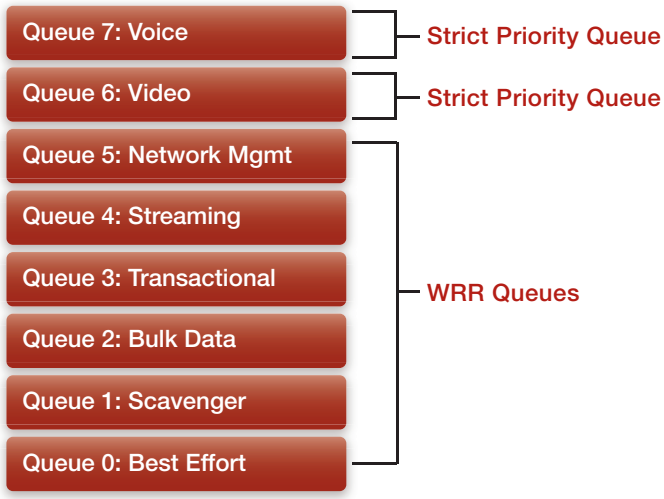
  The transmitting device may choose to resend the lost packet, but this could take some time, because it has to detect the packet has been lost.

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.

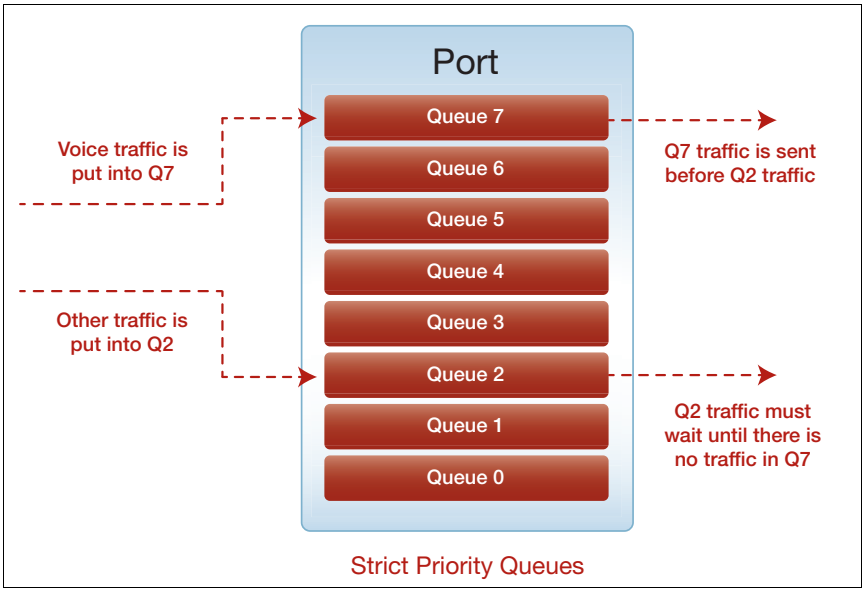


QoS egress queue types

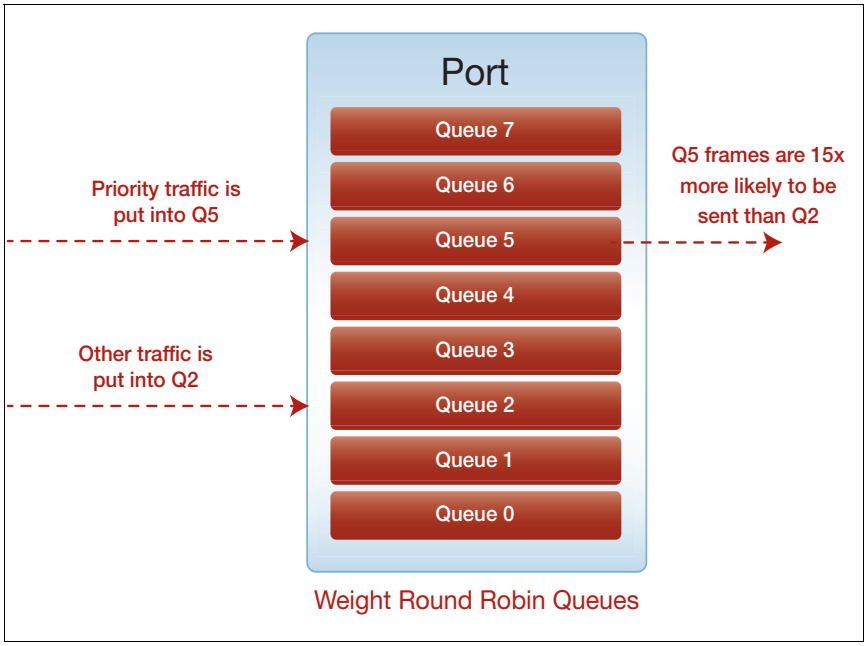
Egress queues help with application performance by allocating a preference to outgoing traffic. For example, voice traffic could be given a high priority so it will be sent before other types of traffic.

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.



- **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.

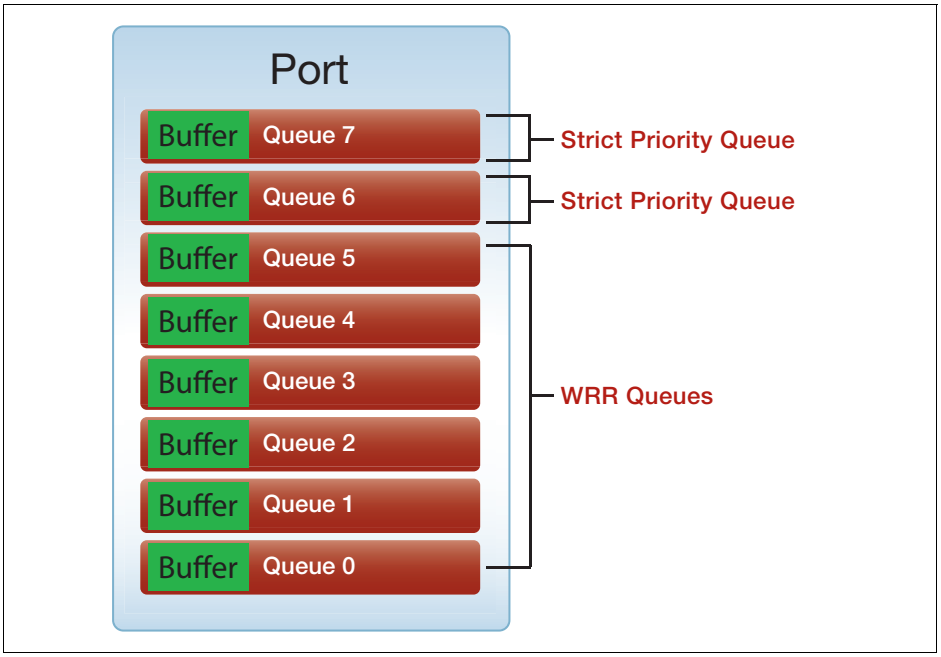


Advantages and disadvantages of WRR and Strict Priority queues

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.



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.

Configuring the Vista Manager EX default policy in the CLI

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

- For 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: SBx8100, x220 and GS980M, x530 and 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 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 1Gigabit 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 and GS980M, x530 and 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 QoS 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
```

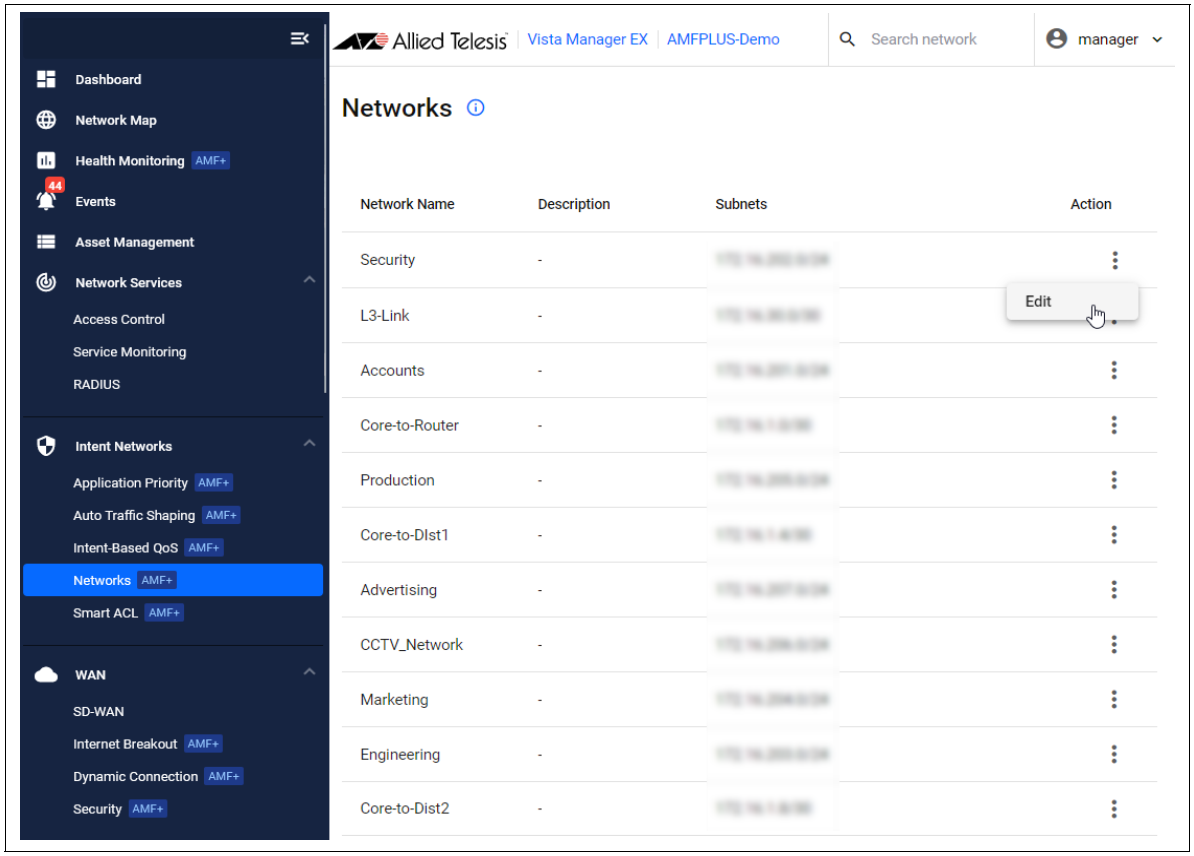
```
mls qos map premark-dscp 56 to new-cos 5
!
policy-map VISTA_DEFAULT_POLICY
 trust dscp
 class default
!
interface port1.0.1-1.0.18
 switchport
 switchport mode access
 service-policy input VISTA_DEFAULT_POLICY
 wrr-queue weight 15 queues 0
 wrr-queue weight 1 queues 1
 wrr-queue weight 3 queues 2
 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
```

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.

From version 3.13.1 onwards, you can enter a single dash, underscore or letters from languages other than English as a network name on the Networks page.



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

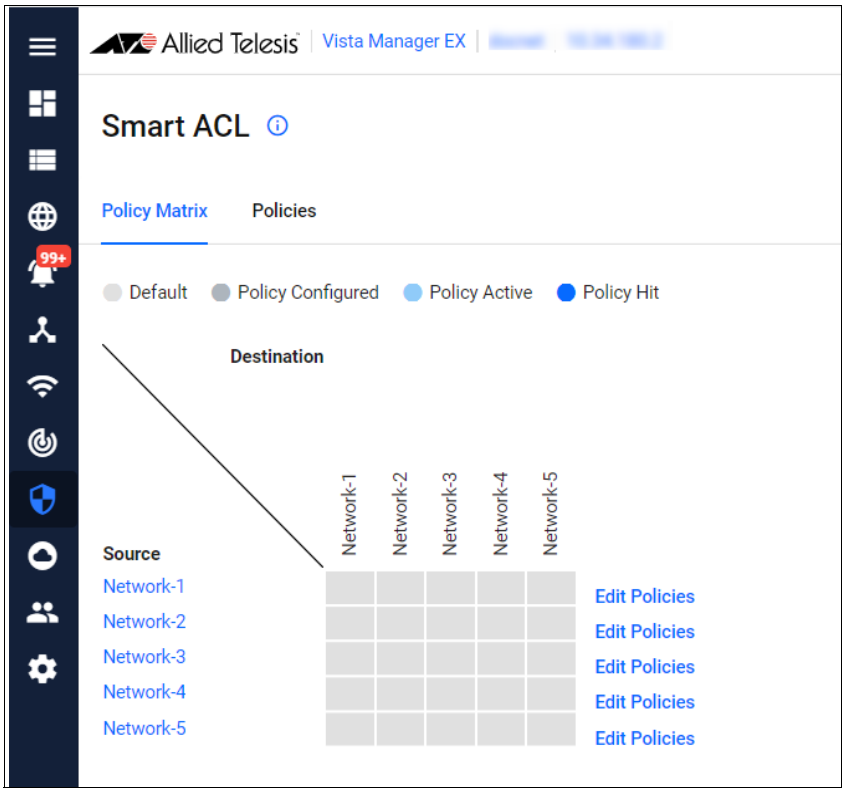
The Smart ACL tool allows you to manage ACLs across devices in the network. ACLs provide traffic flow control and decide which types of traffic are forwarded or blocked.

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.



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.

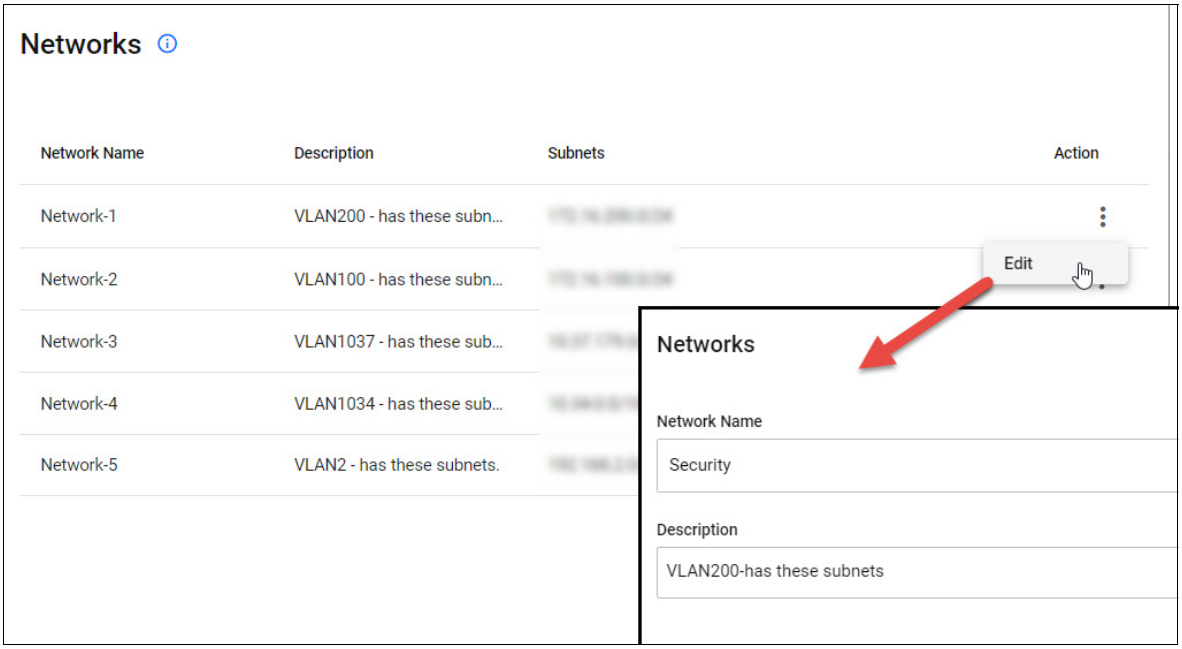
In brief, you first configure a network and optionally assign it a meaningful name, then create an ACL policy and apply it to the network. Let's look at each step in more detail:

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

   For example:

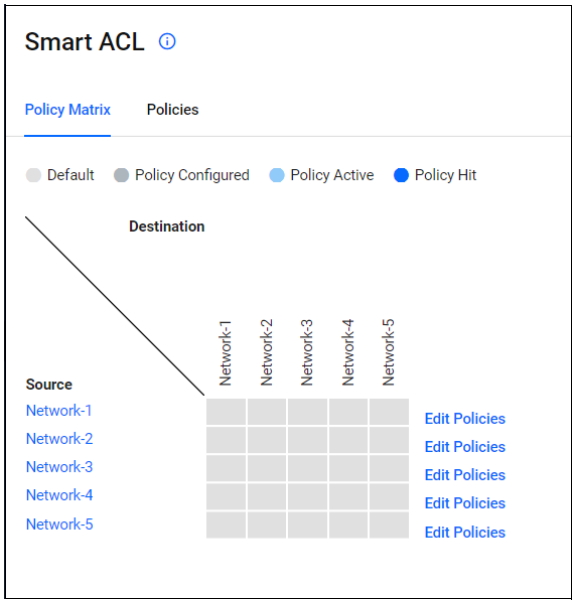
```
vlan database
 vlan 100

 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 **Intent Networks** > **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**.



3. Create an ACL Policy

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



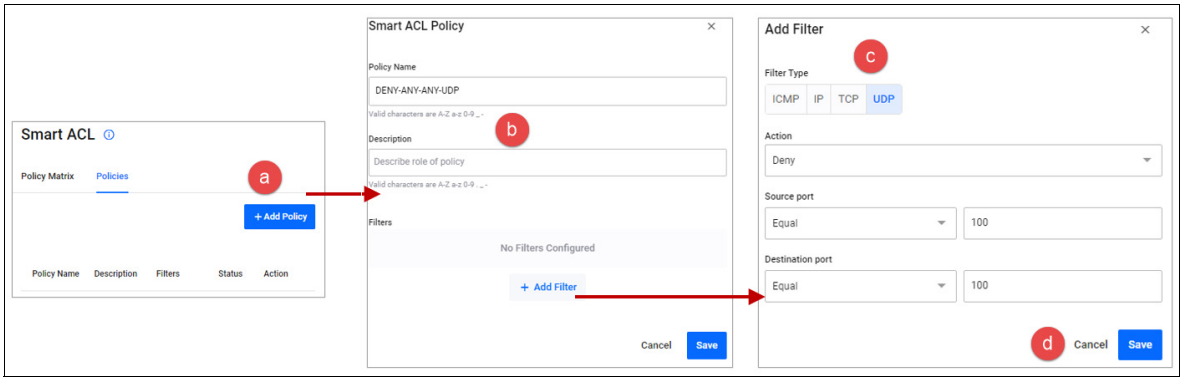
4. Select the **Policies** tab, then:

   a. Click **+Add Policy**

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

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

   d. Click **Save**.



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.

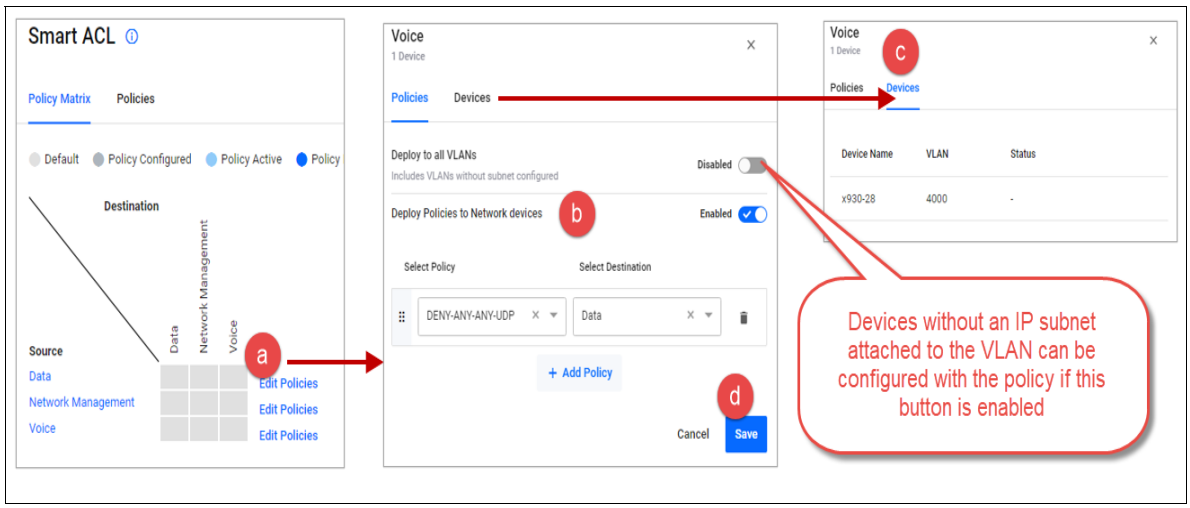
5. Back in the **Policy Matrix** tab, apply a policy to a network.

   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)

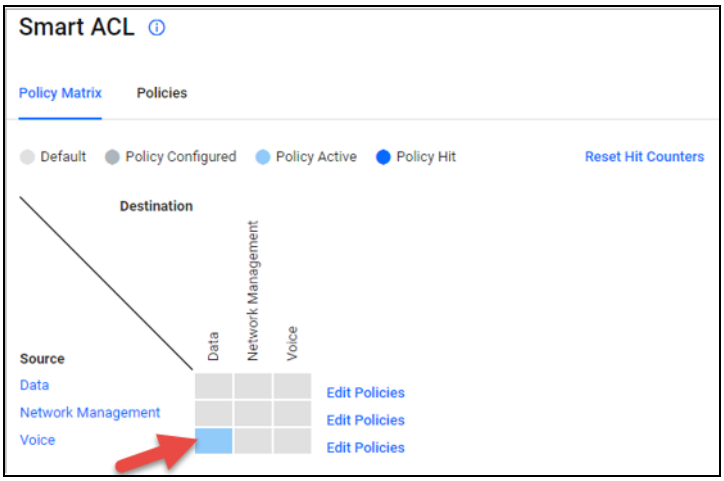
   d. Click **Save**



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**.

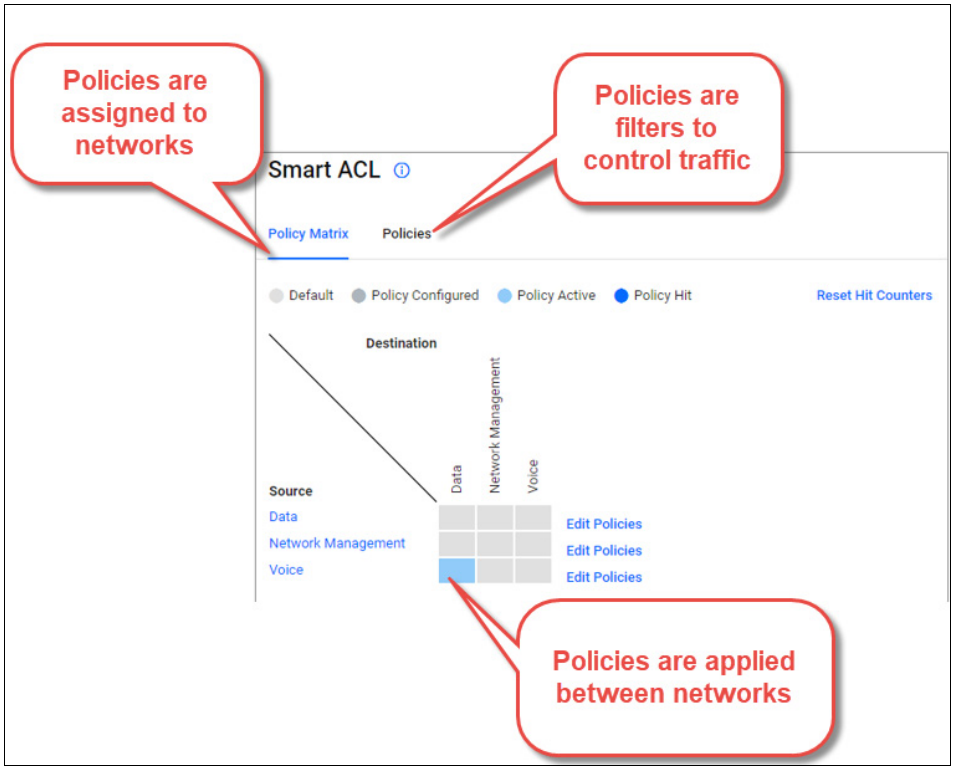


This completes the initial configuration.

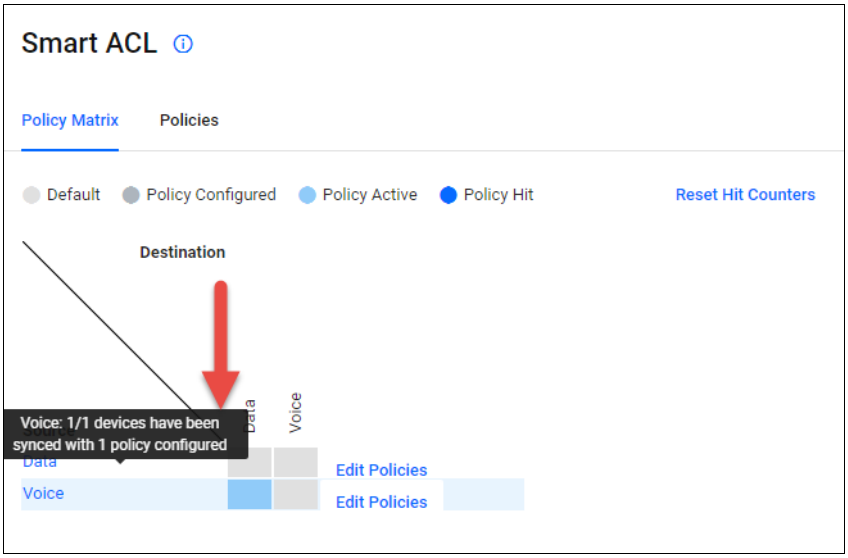
Understanding the Smart ACL Policy Matrix and its operation

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 synced and applied by Vista Manager EX automatically to VLANs using **per-VLAN ACLs**.

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**.



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.

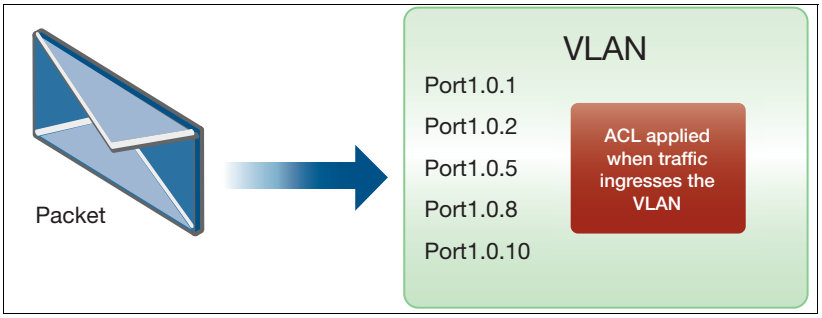


The benefit of this is every time a new device is added as part of the network and this subnet, the values will increase and the new device will automatically receive the policy.

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 266:

- 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:

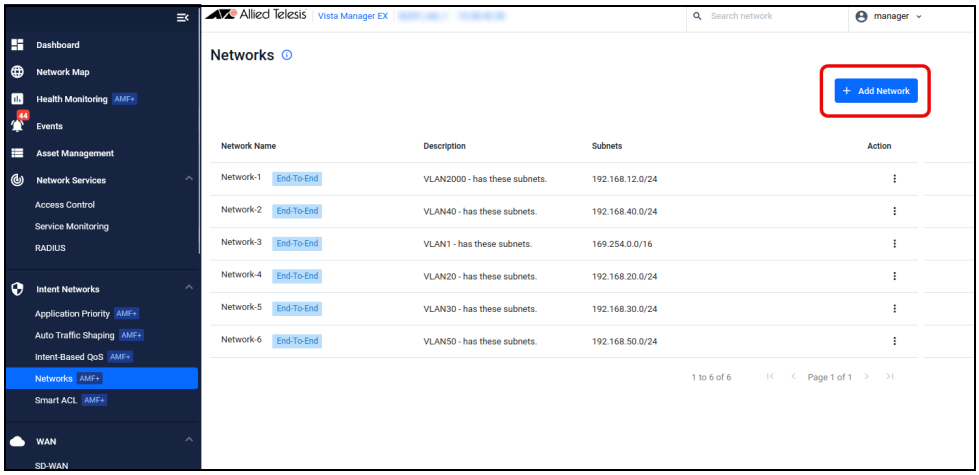
```
show access-list counters
```

Applying policies to all devices or networks

From version 3.13.1 onwards, four new enhancements have been added to the Intent-based Access Control List feature.

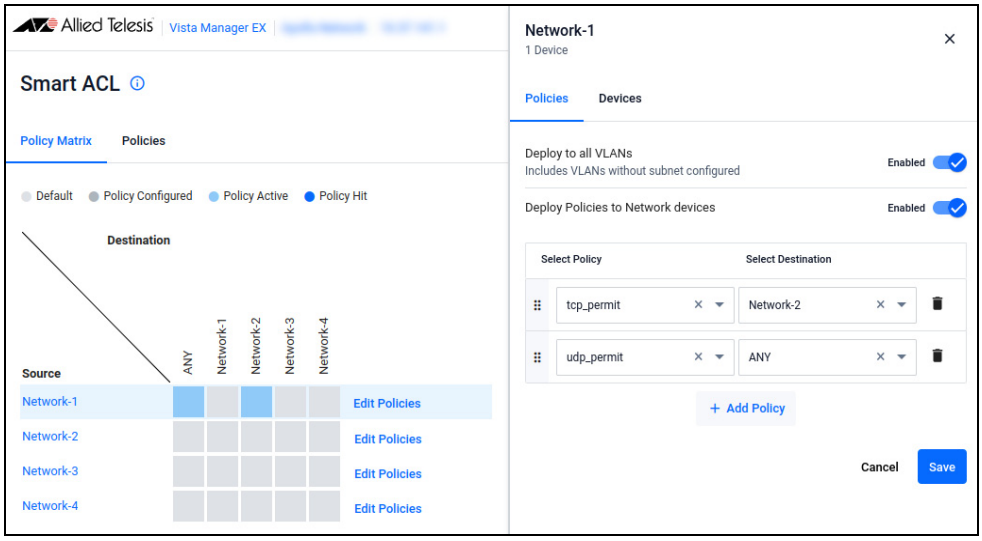
1. Use **destination networks** when creating ACLs to permit or deny traffic to these destinations. These destination networks can include networks outside of ones Vista Manager knows about.

You can add a new network by clicking the **+ Add Network** button from the **Intent Networks** > **Networks** menu.



2. A new **ANY** destination has been added, which allows you to to block or permit user access to all external networks. You can filter traffic through a list of rules, with ANY as a catch-all final rule.

3. When using **IP filtering** for managing which traffic types (protocols) an ACL will block or permit, a new ANY option will select all IP protocols (e.g. TCP, UDP, ICMP, etc). This makes configuration simpler, and saves needing a separate IP filter for each individual IP protocol.



4. You can apply **Smart ACL policies** to all network devices if desired (although this is not often necessary for ACL operation in the network). When choosing to deploy to all switches, a toggle has been added to allow you to exclude edge switches with a low ACL limit to avoid oversubscribing capacity if you expect to need a large number of ACLs (see below).

Switches with a low ACL limit

A low limit of ACLs refers to devices with less than 512 ACL entries.

You can confirm the number of ACL entries on a device with the **show platform classifier statistics utilization brief** CLI command.

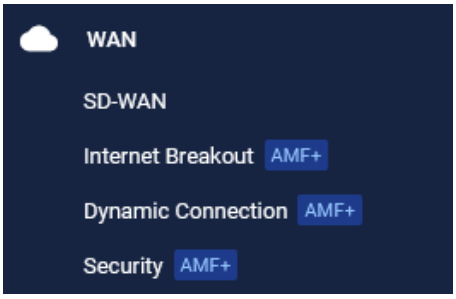
Edge devices with a low limit of ACLs include the following devices:

Device Series	ACL Entries
FS980M	496/408
GS900MX	119
IE200	496
IE210L	119
IE220	247
IE300	247
IE340, IE340L	119
IE510	247
x230, GS970M, x230L	119
x310	119
GS970EMX, x330	247
x510, x510L, x510DP, IX5	247
XS900MX	248

WAN

Introduction

The WAN menu hosts a variety of features related to wide area network configuration. The Software Defined WAN (SD-WAN) feature 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 dashboard 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.

Initial configuration of devices for SD-WAN

The 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.
`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 "Configuration example" on page 276.

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
!
```

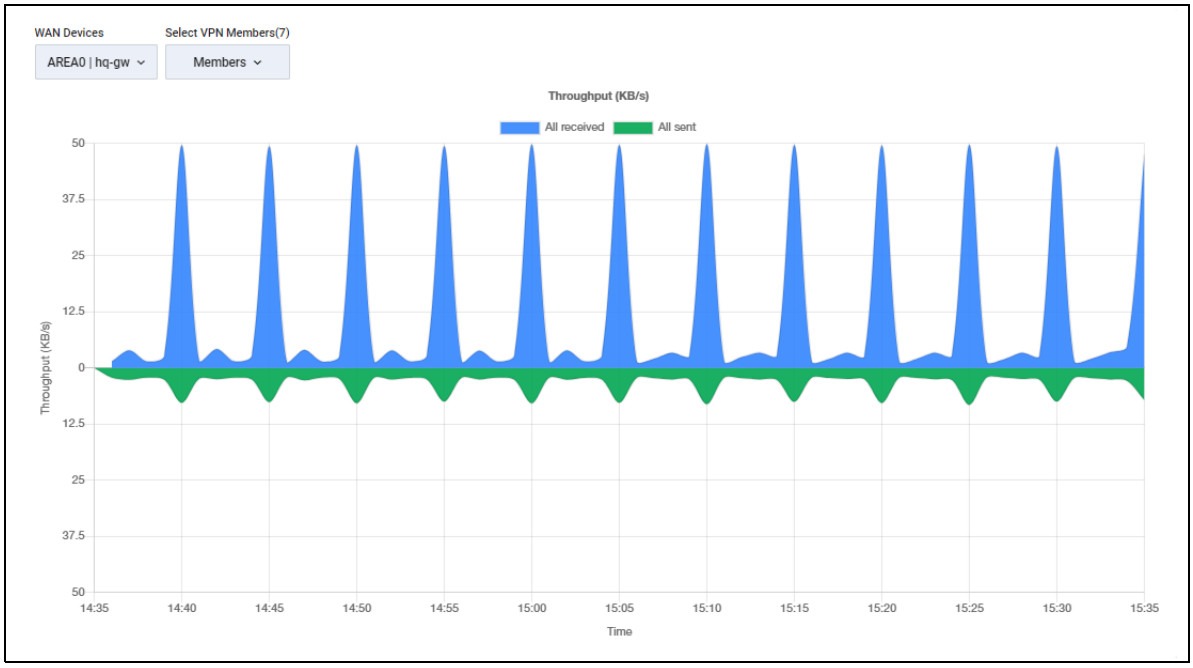
```
interface port1.0.8
switchport
switchport mode trunk
rmon collection history 4 buckets 10 interval 30 owner VISTA
switchport atmf-link
!
interface eth1
encapsulation dot1q 2
encapsulation dot1q 3
encapsulation dot1q 1000
!
interface eth1.1000
ipv6 address 2001:db9:1:1::2/64
!
interface eth1.3
ip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

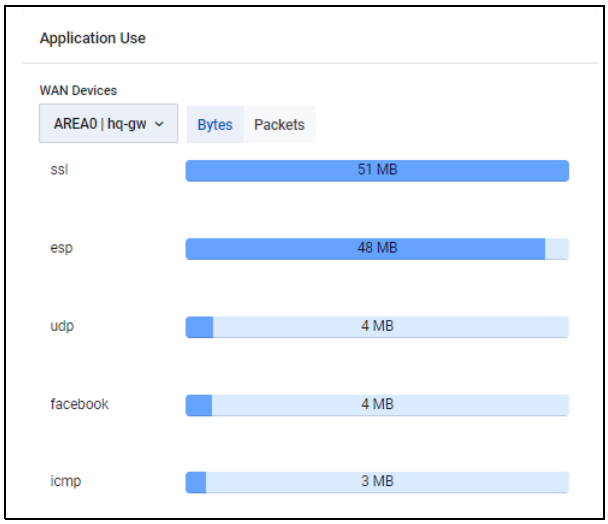
SD-WAN Dashboard

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

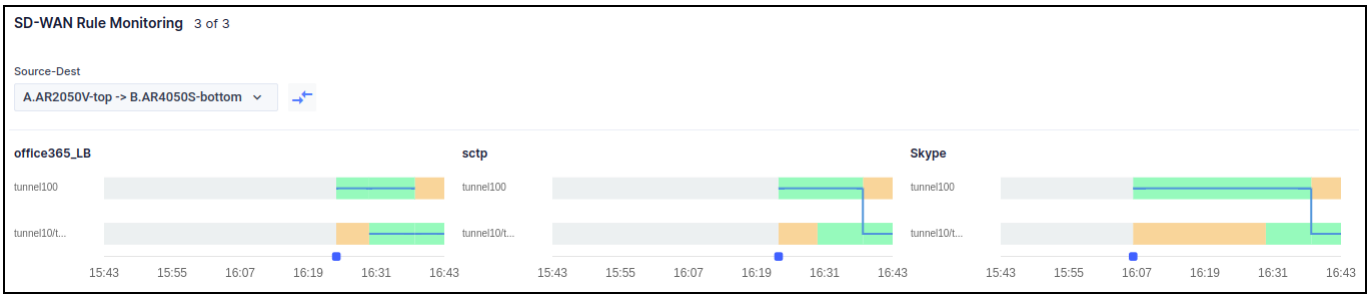
You can also choose the time-frame you wish to display; either the last 1 hour, the last 12 hours, the last 24 hours, or a custom range.



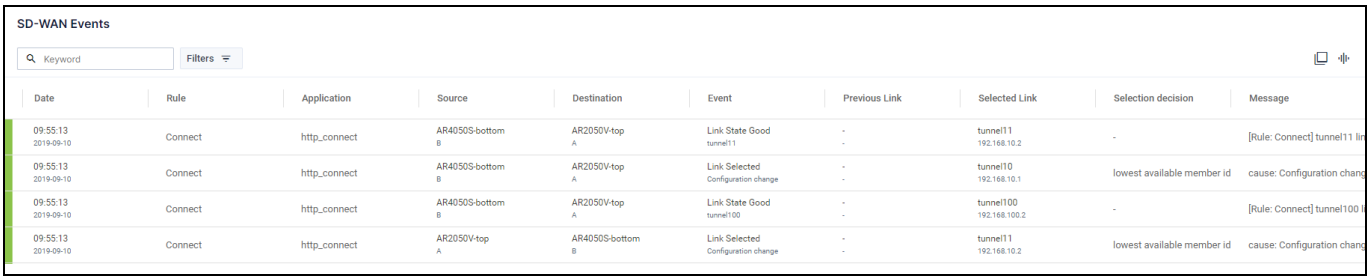
The throughput chart shows an overview of sent and received data for a device. You can select which device to view from the WAN Devices drop-down. You can also choose which members to include from the Select VPN Members drop-down.



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.



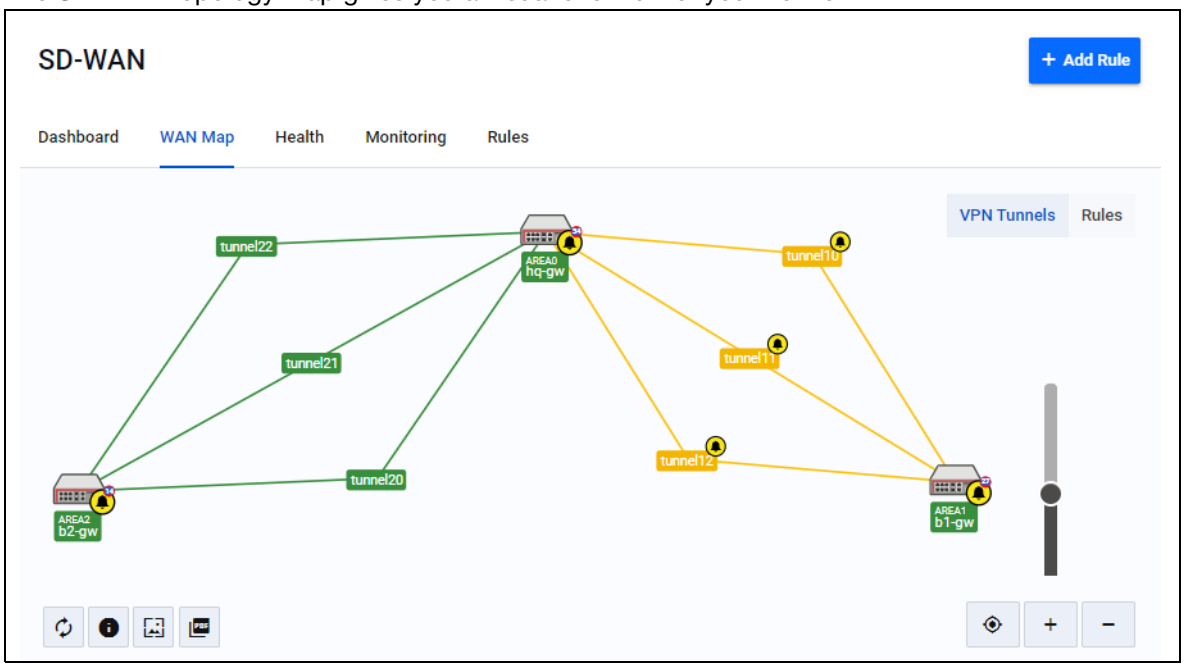
The rule monitoring chart shows the status of rules in your network. You can change which rules are shown from the Source-Destination drop-down.



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

SD-WAN Topology map

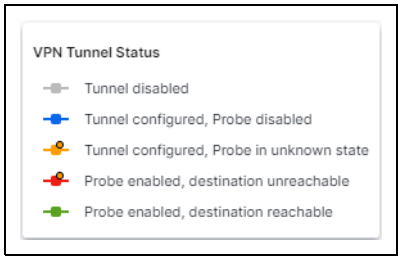
The SD-WAN topology map gives you a visual overview of your network.



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

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

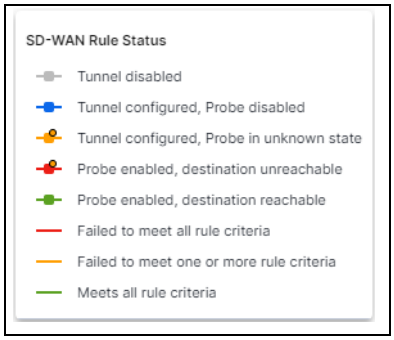
You can click on the Information button to bring up a key explaining each of the colors.



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

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

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

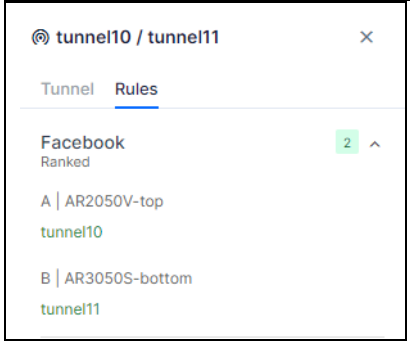


To change between showing the health of the tunnels or the rules, select either VPN Tunnels or Rules by clicking on the control in the top right corner.

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

Tunnel details tab:

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

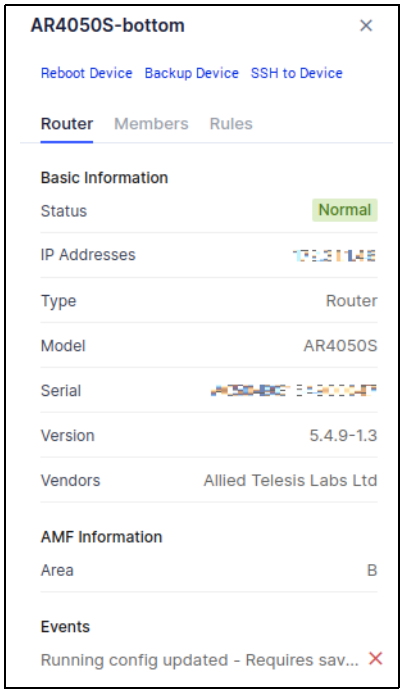


SD-WAN rules tab:

- Rule Name
- Rule Details

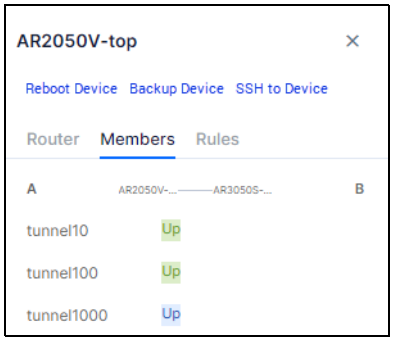
When you click on a router, the router details are displayed in the side panel. The side panel shows the following information:

Router details:

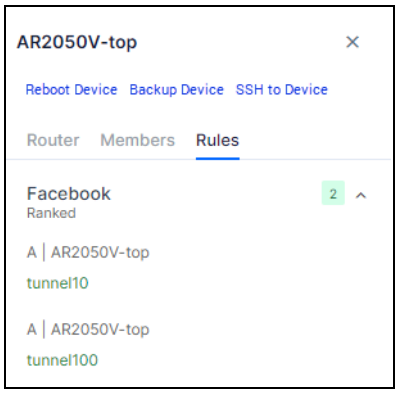


- Status
- IP Address
- Type
- Model
- Serial
- Version
- Vendors
- AMF Information

VPN members:



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



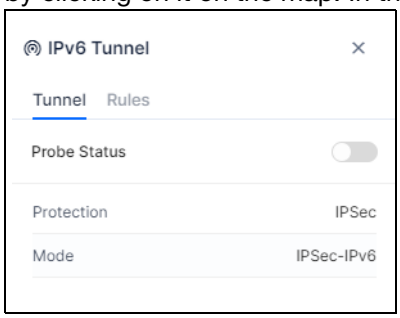
Rules:

- Rule Name
- Rule Details

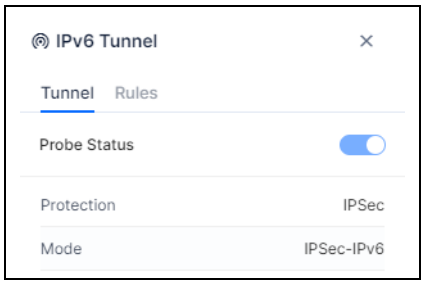
Probes on the Topology map

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

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



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



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

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

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

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

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

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

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

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.

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

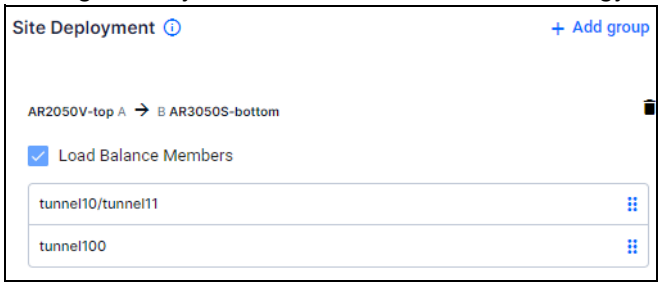
Site deployment

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

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

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

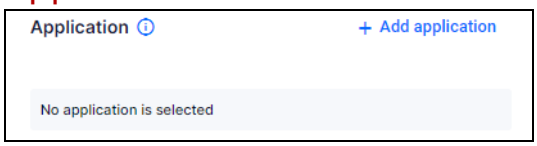
Within each router pair, links can be moved to have a higher or lower ranking within the group. This ranking is solely used for the Link Selection Strategy of 'Ranked'.



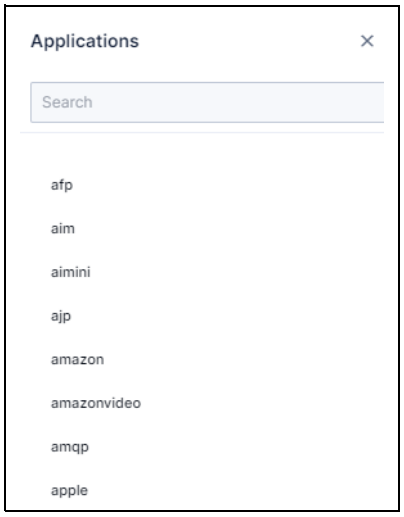
When selecting a VPN member, you will be notified how many more rules can be created on the device. Remaining rule spaces are calculated by taking the highest rule ID and subtracting it from 500. When there are 0 rules available, you cannot select the member as a source or destination.

When selecting a VPN member, you can only select links between a source and destination 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



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.



Health

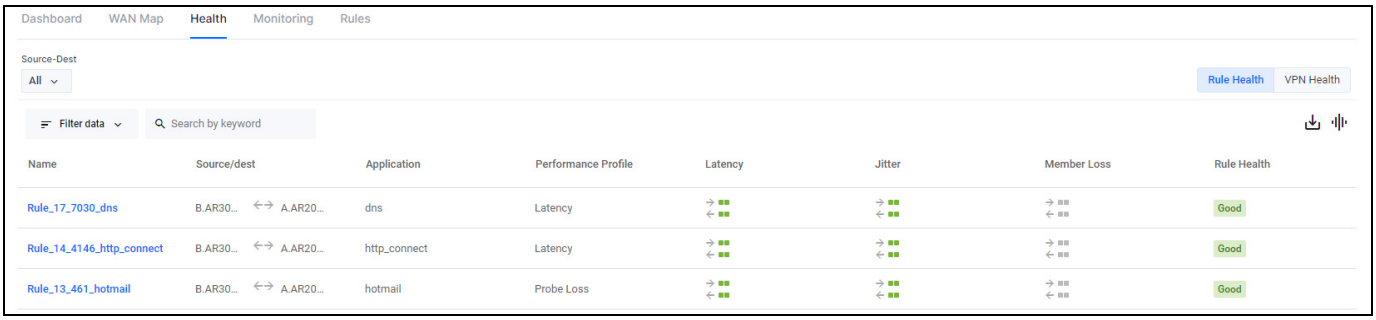
The health tab gives you an overview of the current health of your network in a single location.

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

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

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

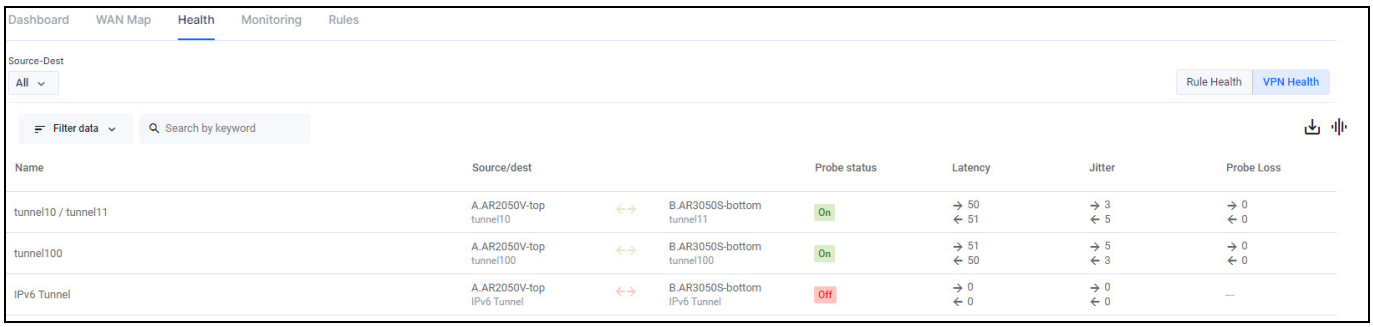
Rule health



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

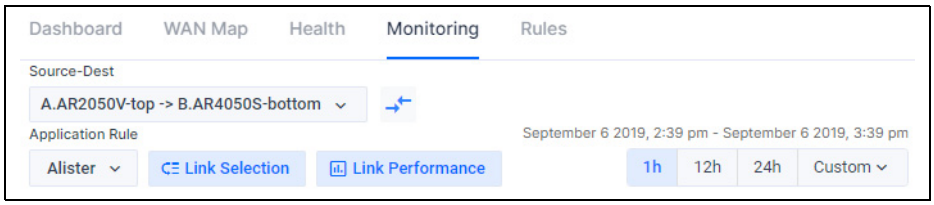
- the rule settings
- the rule status
- the current settings for:
  - latency
  - jitter
  - probe loss

VPN health



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

Monitoring



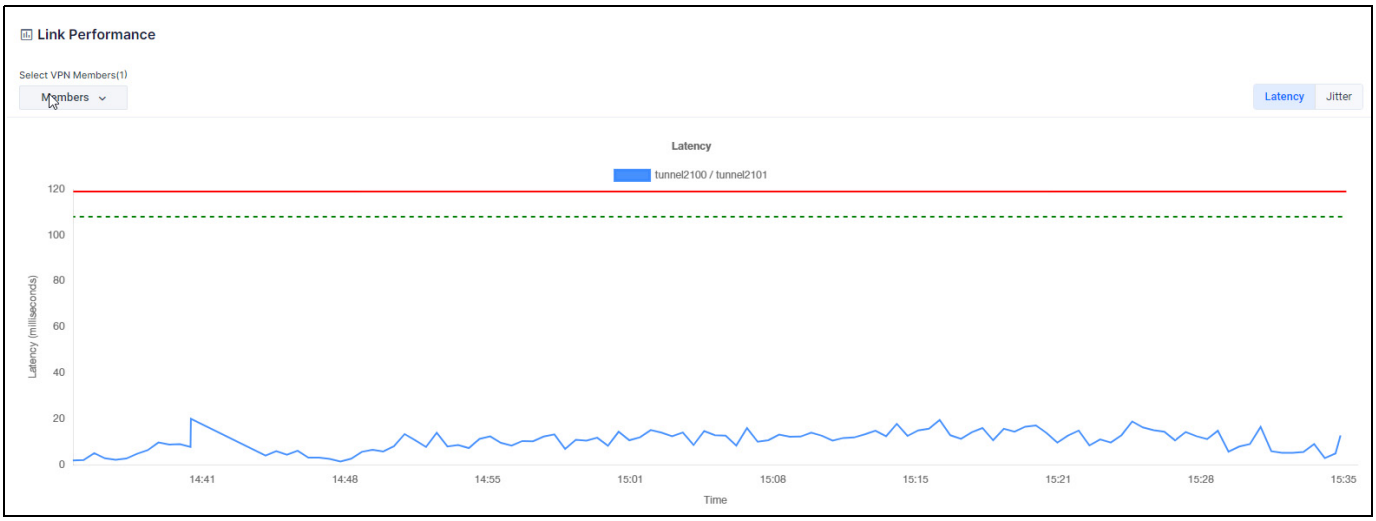
The monitoring tab displays historic link and rule information. Vista Manager EX allows you to view up to 7 days of historic data.

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

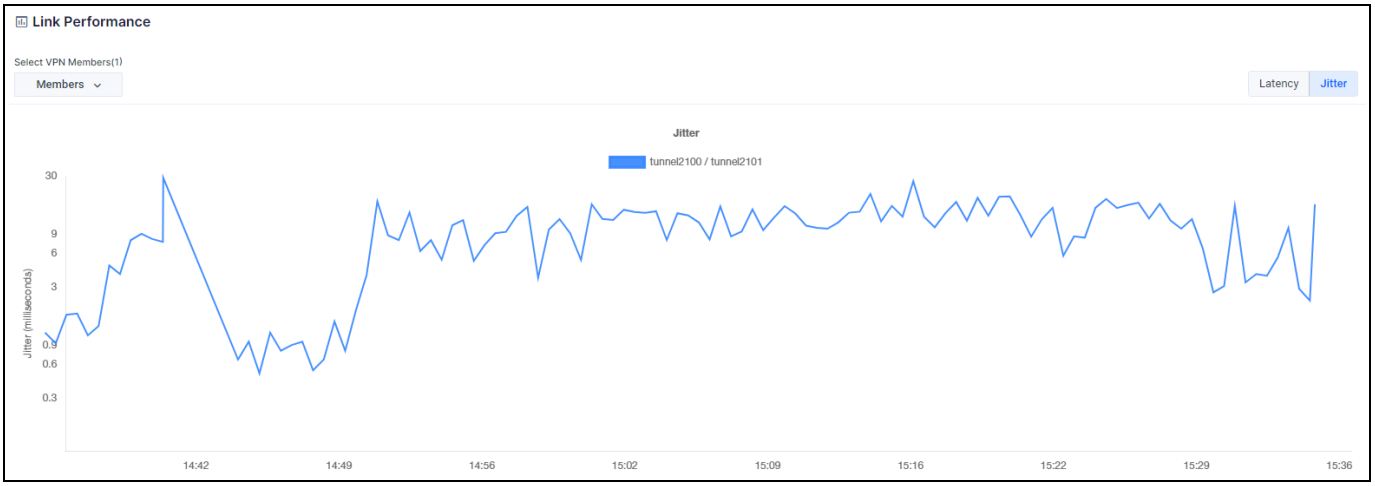
You can toggle which charts are shown. The Performance Routing Events chart is always available. The Link Selection Path and Link Performance charts are only available after a source and destination have been selected.

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

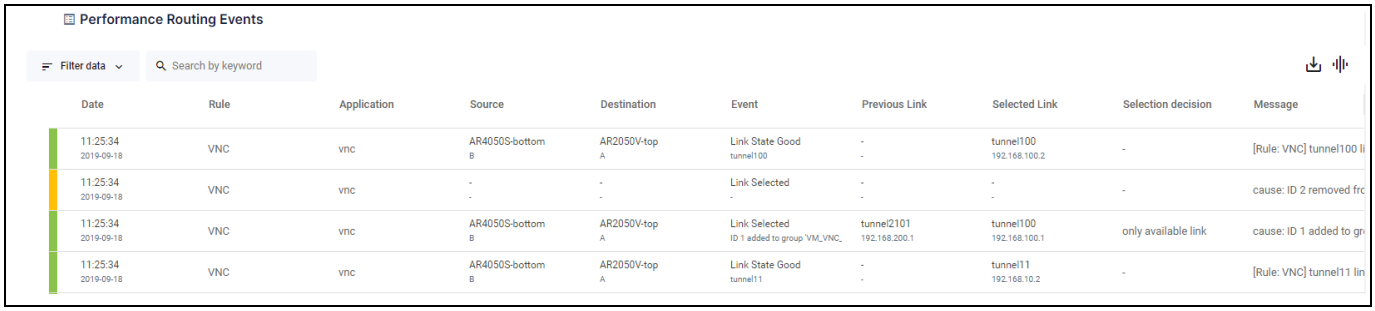
The Link Performance charts show the performance history of a link for either latency or jitter. You can select which member you would like to see from the Members drop-down, or select multiple members to compare them.



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



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



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

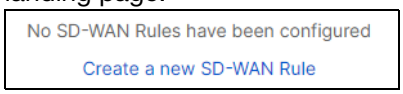
User permissions

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

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:

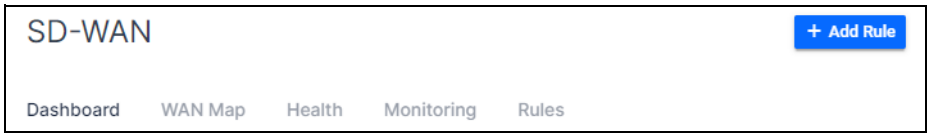


From version 3.14.0 onwards, support has been added for an 'any' option for applications from the **SD-WAN** > **Rules** page.

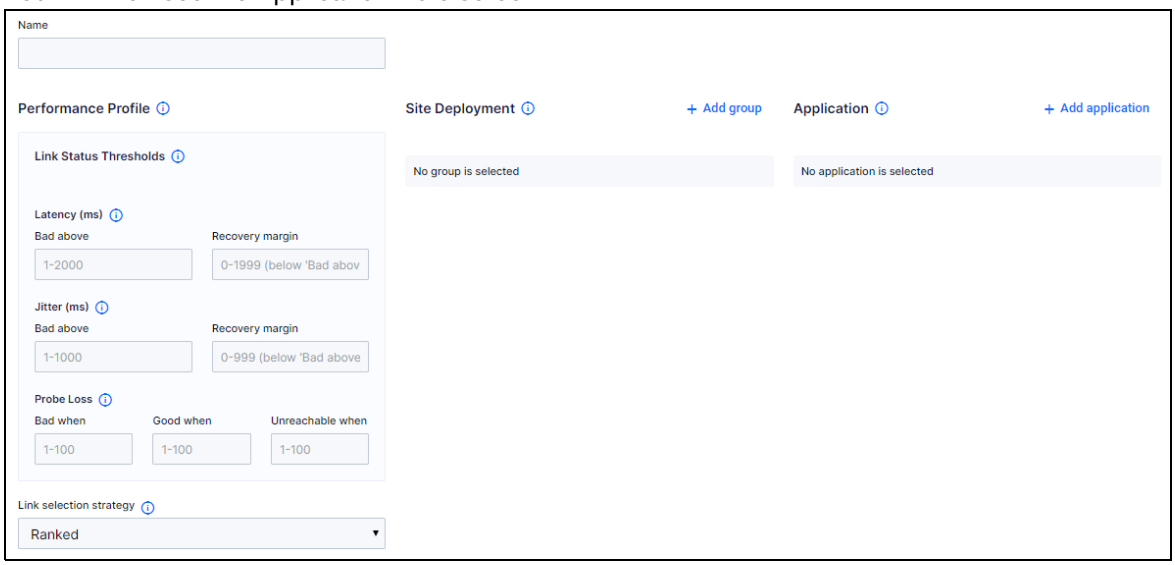
You can now create an SD-WAN rule that applies to any application. This support helps you to deploy SD-WAN across multiple sites easily, by using rules that apply to all applications instead of making individual rules for each application.

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

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

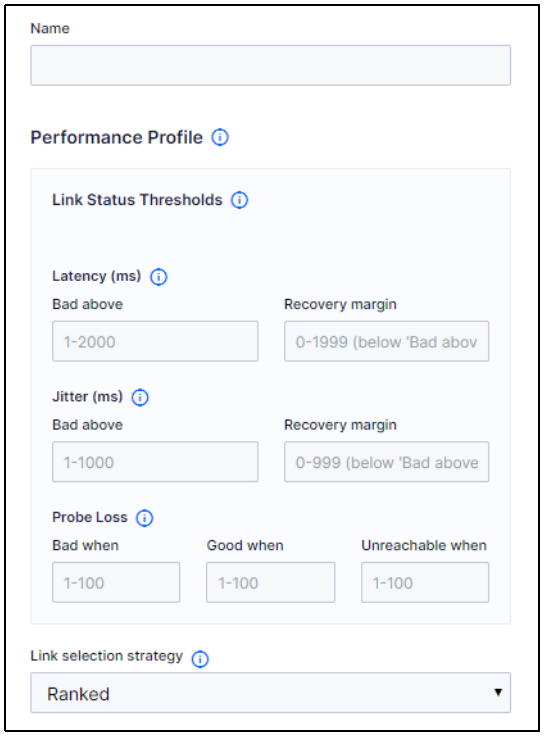


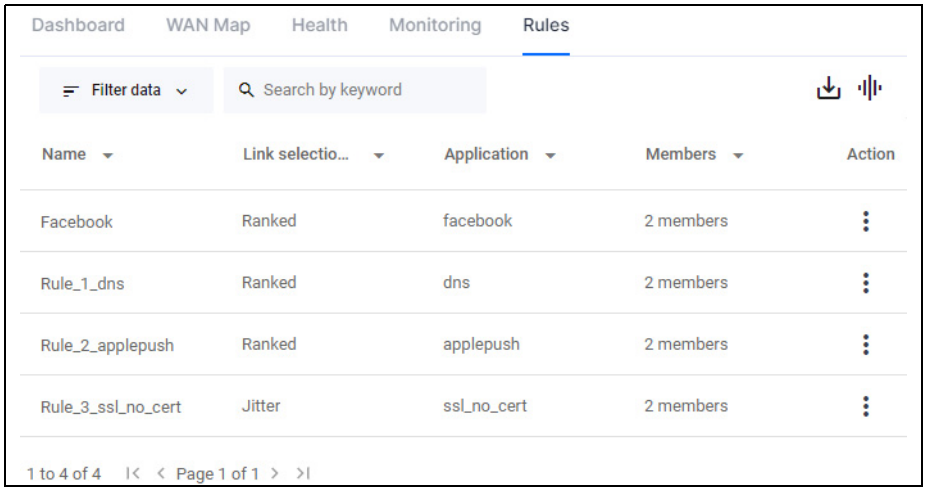
You will then see the Application Rule screen:



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

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





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

The table of existing rules contains link state history. History information is polled and stored, so there may be a delay in the rule table.

Note: 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.

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.

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.

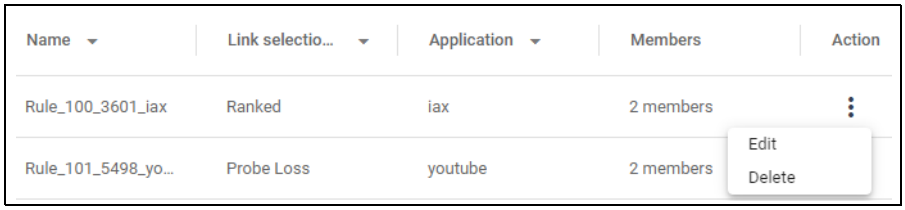
When Vista Manager detects a configuration mismatch, it will generate one event for the device that has the mismatch:

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.

Editing and deleting an SD-WAN rule



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

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

User permissions for SD-WAN 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.

Applying SD-WAN rules to all applications

From version 3.14.0 onwards, support has been added for an 'any' option for applications from the SD-WAN > Rules page.

You can now create an SD-WAN rule that applies to any application. This support helps you to deploy SD-WAN across multiple sites easily, by using rules that apply to all applications instead of making individual rules for each application.

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:

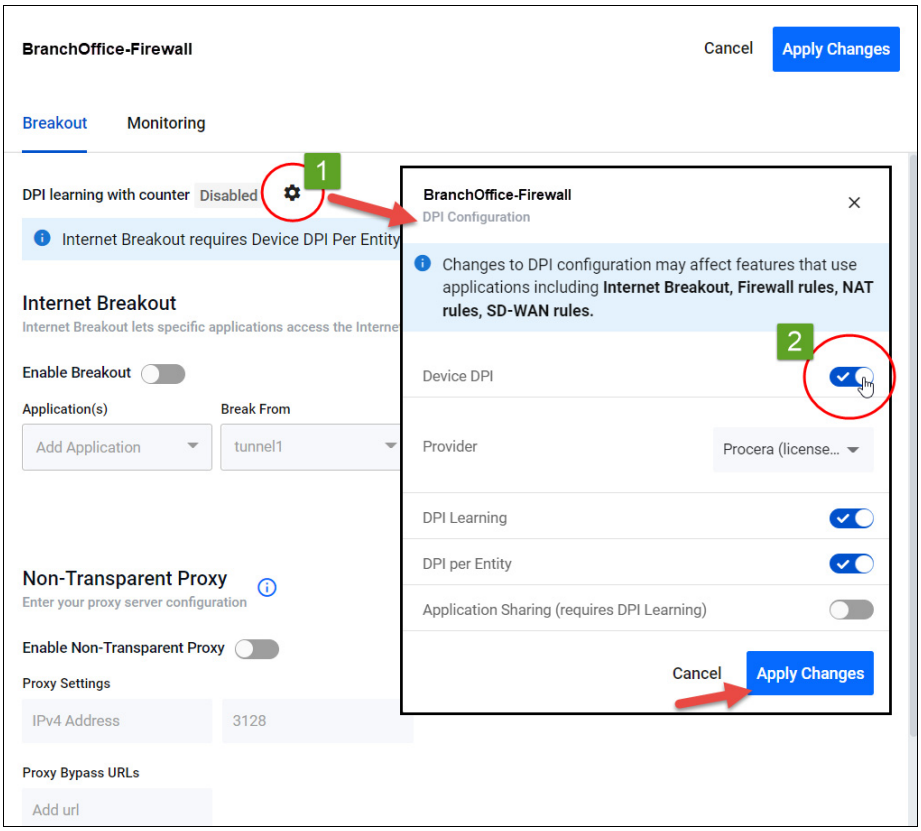
```
enable
conf t
tunnel security-reprocessing
```

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

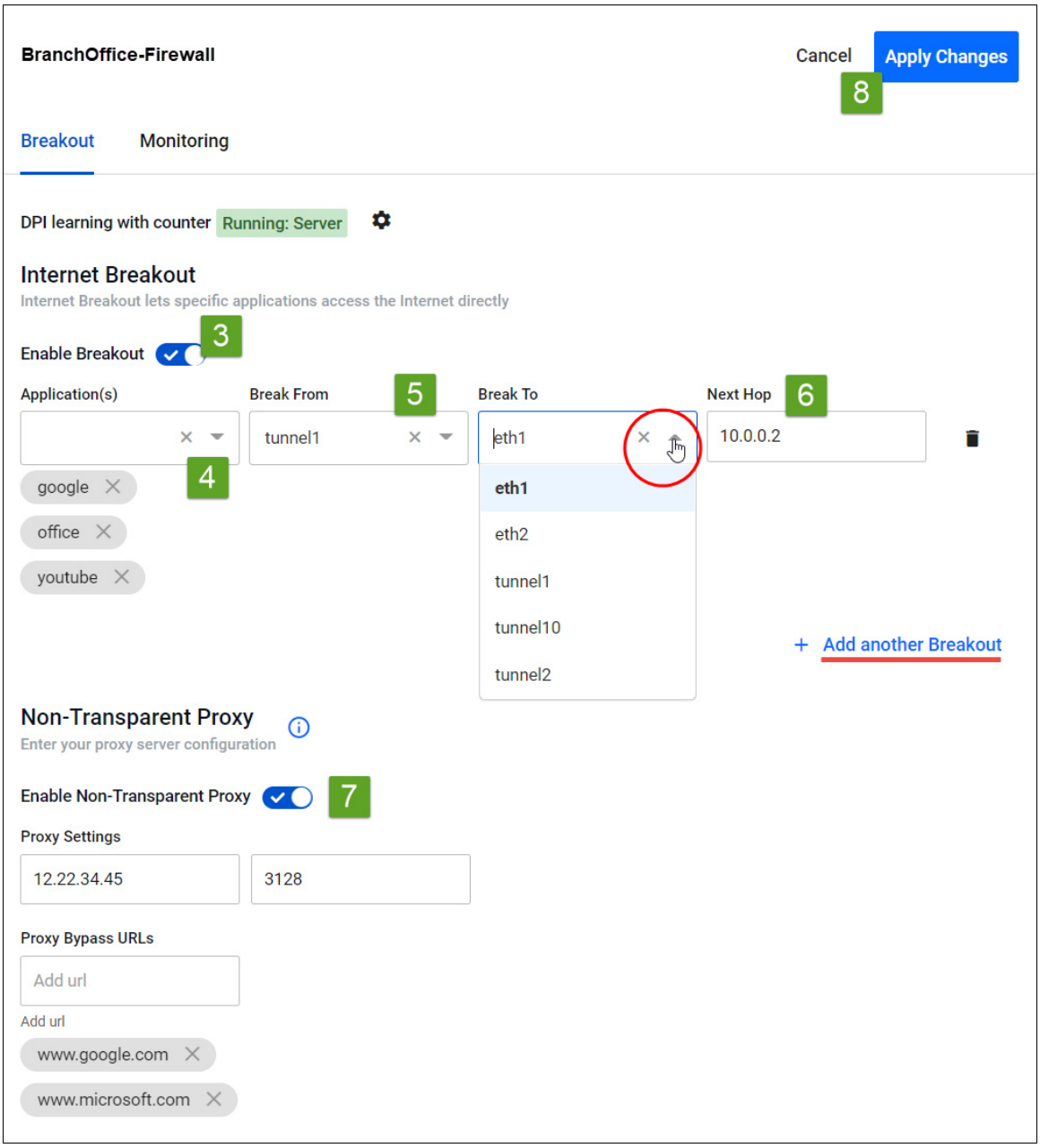
By default, Internet Breakout inputs are disabled until **Breakout** or **Non-Transparent Proxy** is enabled. If invalid options are selected followed by disabling Internet Breakout, these options will be removed. This prevents saving a disabled but invalid configuration.

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

1. Click the **Settings** icon.
2. Enable **Device DPI** (save any changes).



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**.

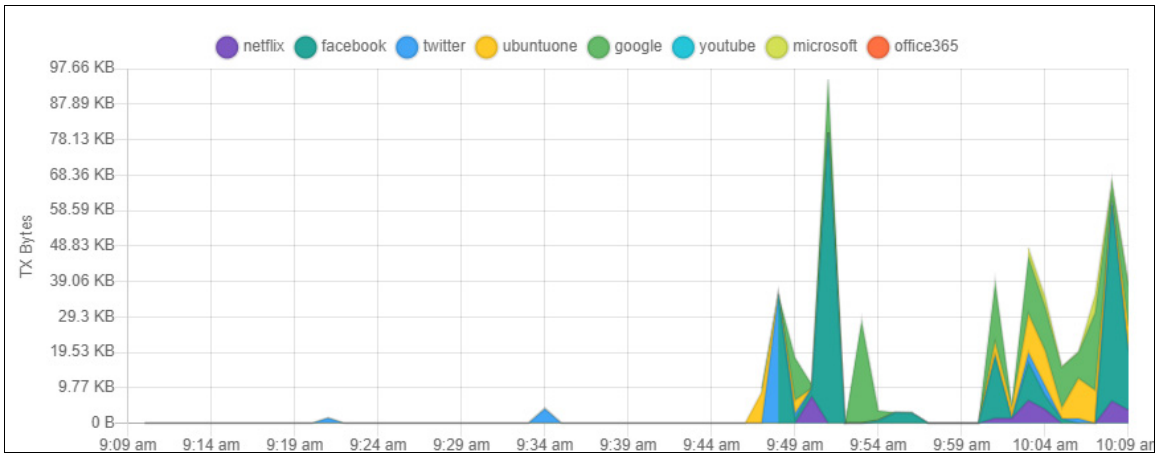

BranchOffice-Firewall
Cancel
Apply Changes
8
Breakout
Monitoring
DPI learning with counter
Running: Server
Internet Breakout
Internet Breakout lets specific applications access the Internet directly
Enable Breakout
3
Application(s)
Break From
5
Break To
Next Hop
6
tunnel1
eth1
10.0.0.2
4
google
office
youtube
eth1
eth2
tunnel1
tunnel10
tunnel2
+ Add another Breakout
Non-Transparent Proxy
Enter your proxy server configuration
Enable Non-Transparent Proxy
7
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.



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.

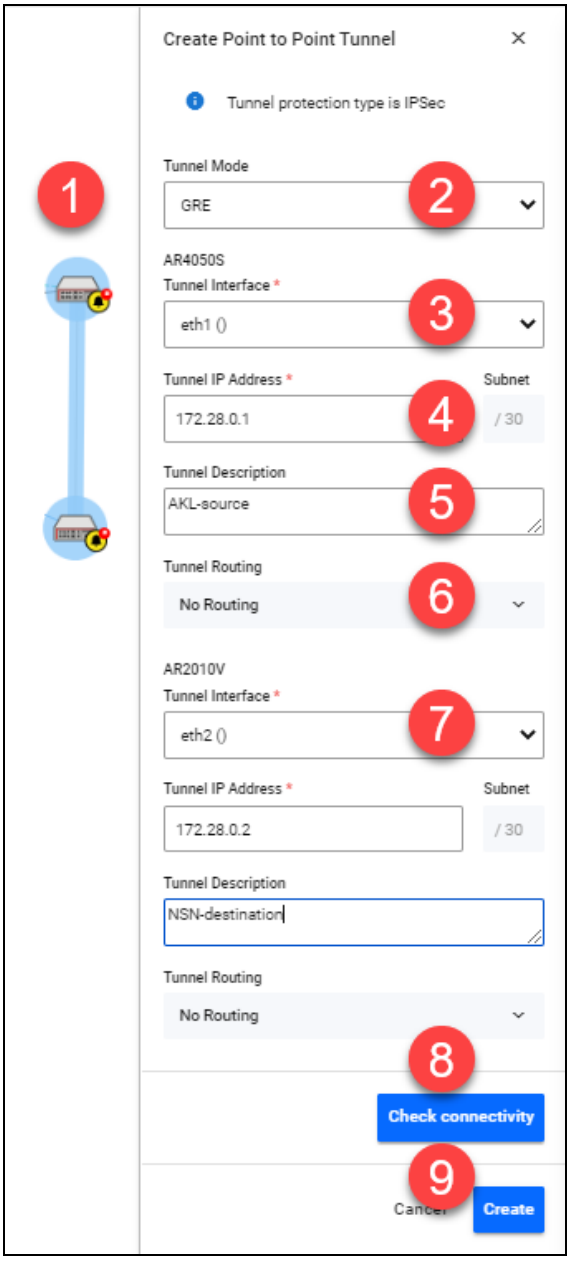
To create a tunnel, both devices must be part of the AMF network, support GRE tunnels and be running firmware version AlliedWare Plus 5.5.0-2.x or later.

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



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.

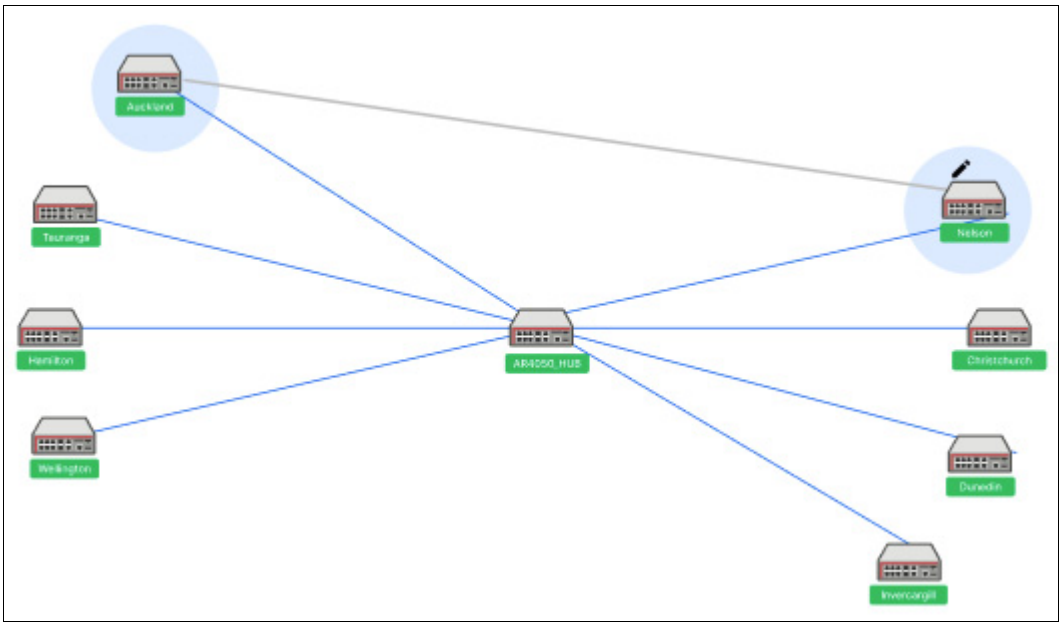
Note: If you choose your own IP address, it must be in the same subnet and must not be used on another interface on those devices.

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.

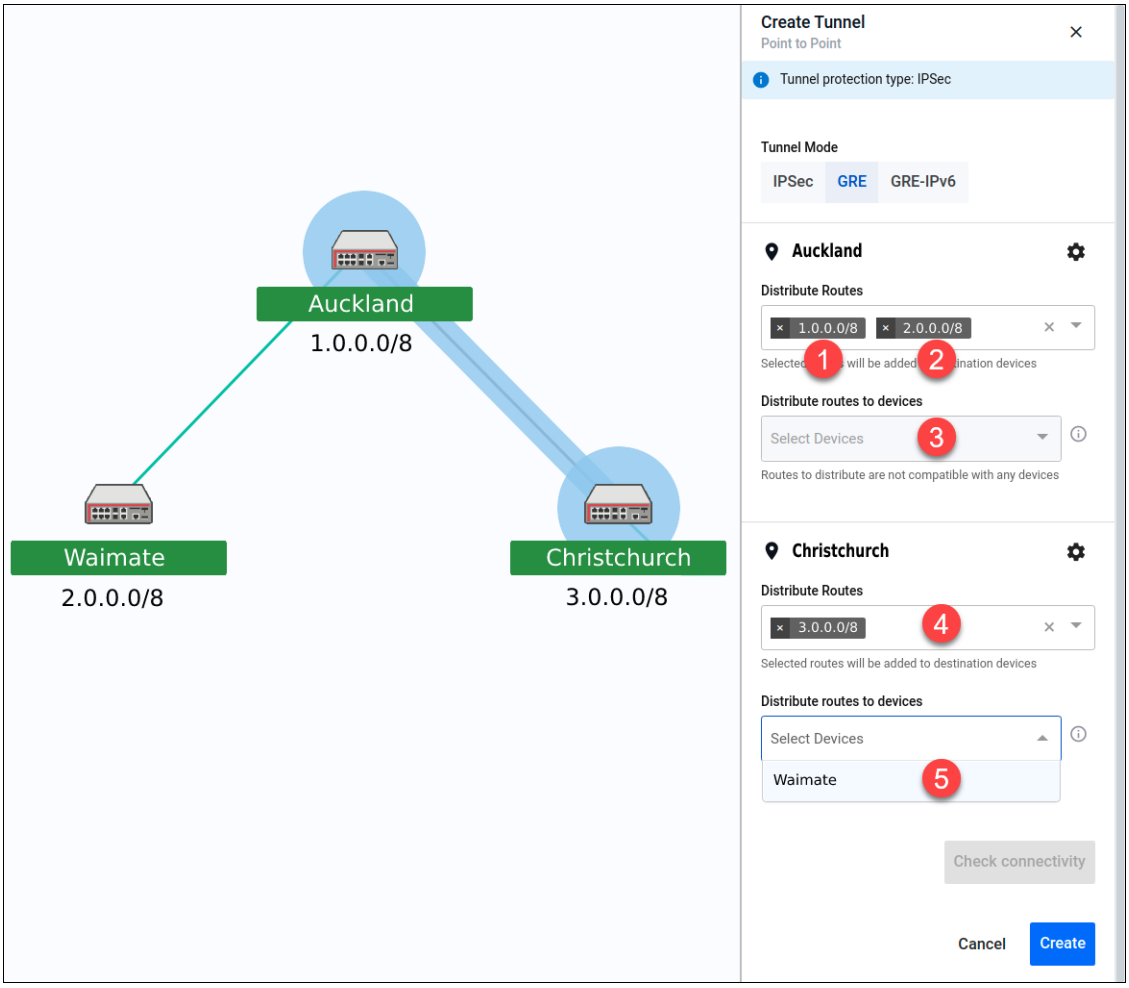
For this feature to be fully supported, AlliedWare Plus version 5.5.1-2.1 or later is required.

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.



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.

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.

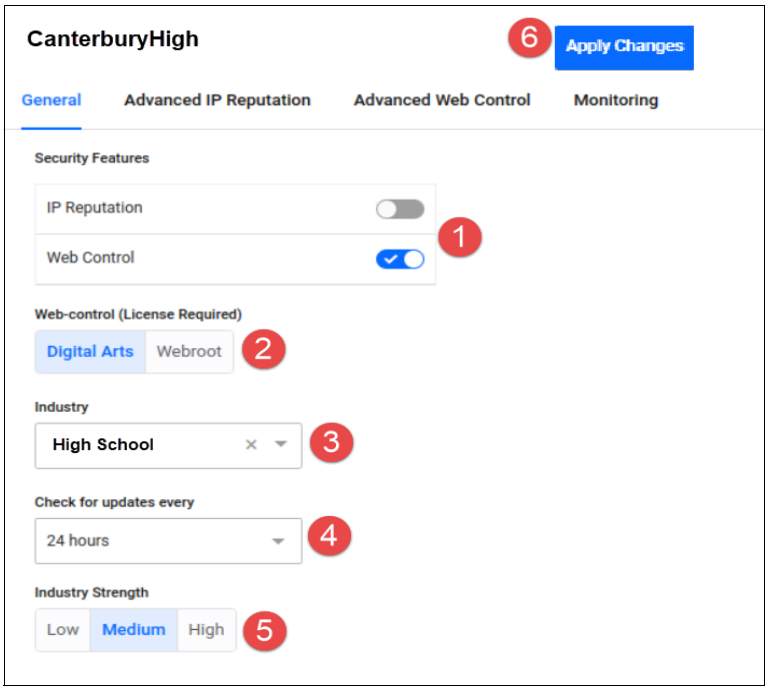
The overall security feature allows you to enable recommended security settings for a group of UTM firewall devices based on an industry type and security strength. This simplifies the process as there is no need to manually choose website or reputation categories for each device.

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

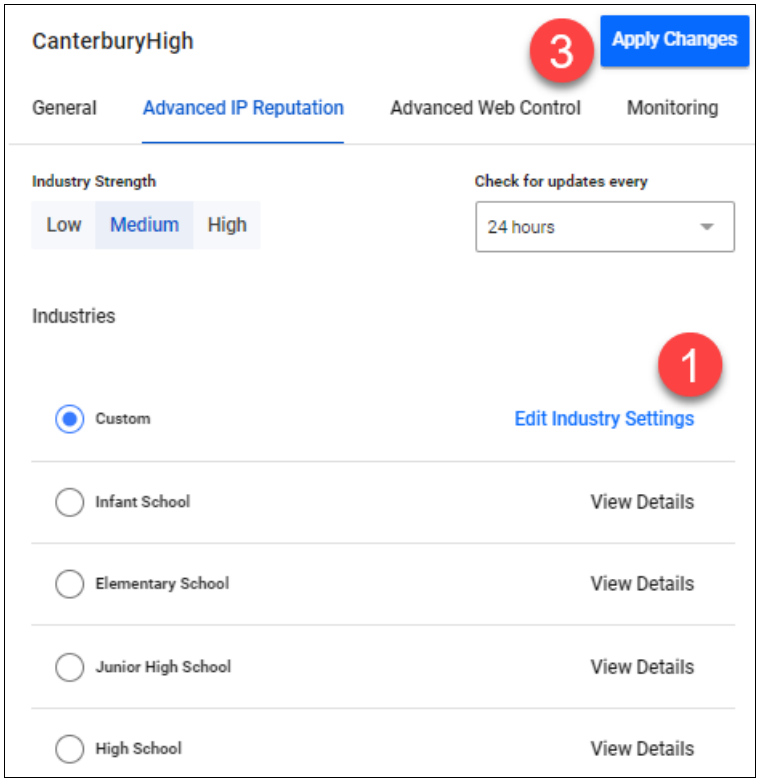
1. Enable **IP Reputation** and **Web Control** for the desired device group(s).
2. Select a Security provider (e.g. Digital Arts).
3. Select the industry type (e.g. High School).
4. Set a time to check for updates.
5. Select the desired security strength for the industry (e.g. Medium).
6. Click **Apply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



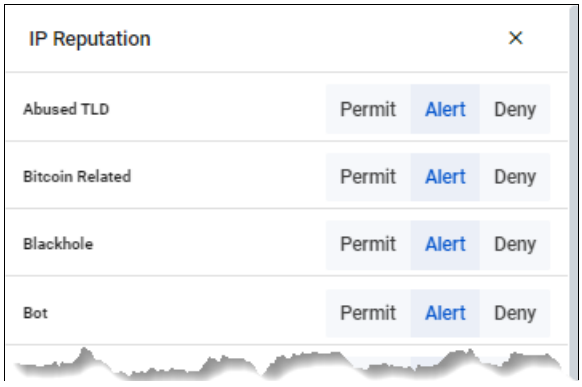
Step 2: Edit advanced IP reputation settings if required.

Use the Security > Advanced IP Reputation tab

1. Click **Edit Industry Settings**.



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.



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

Step 3: Edit advanced Web Control settings if required.

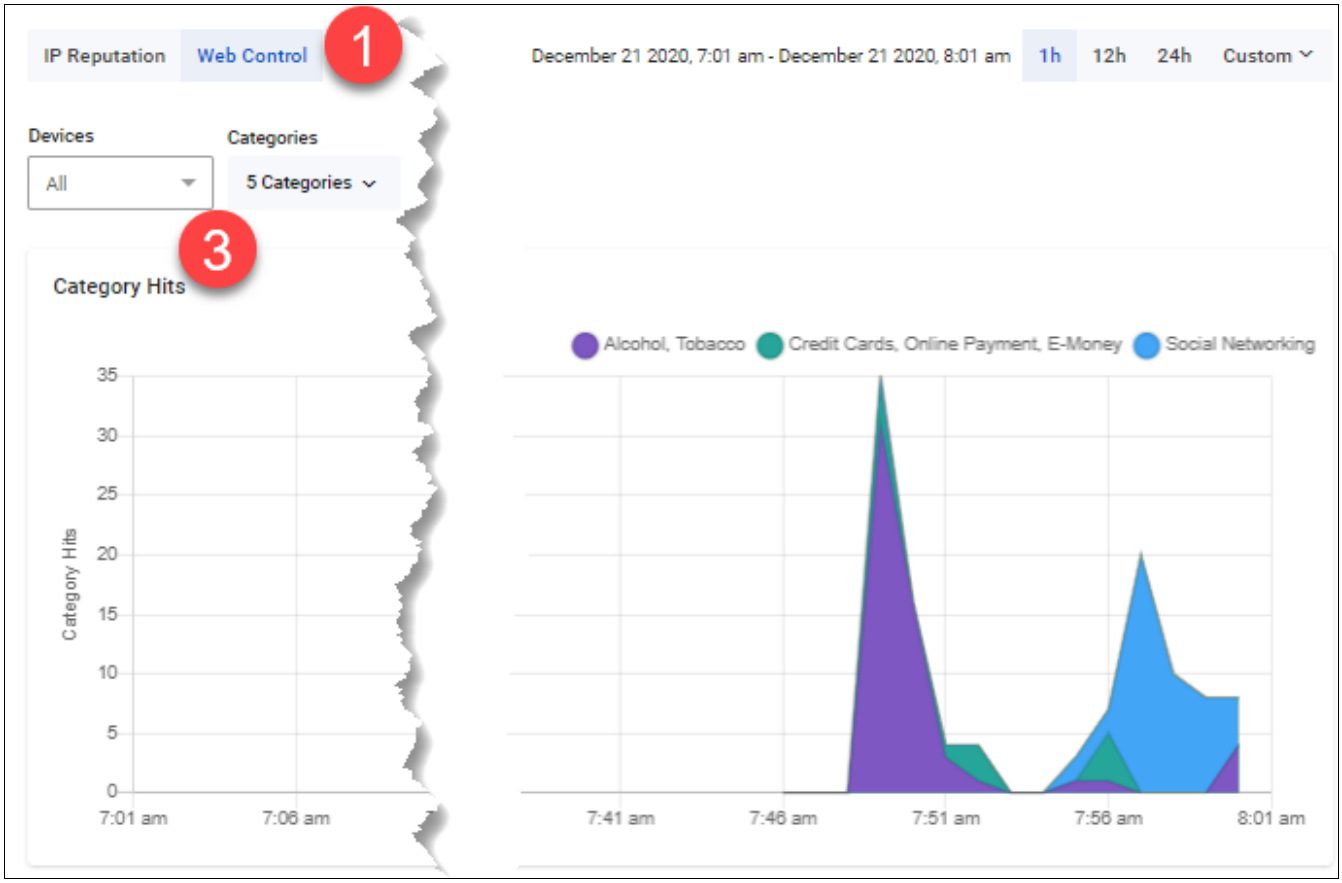
Use the Security > Advanced Web Control tab

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

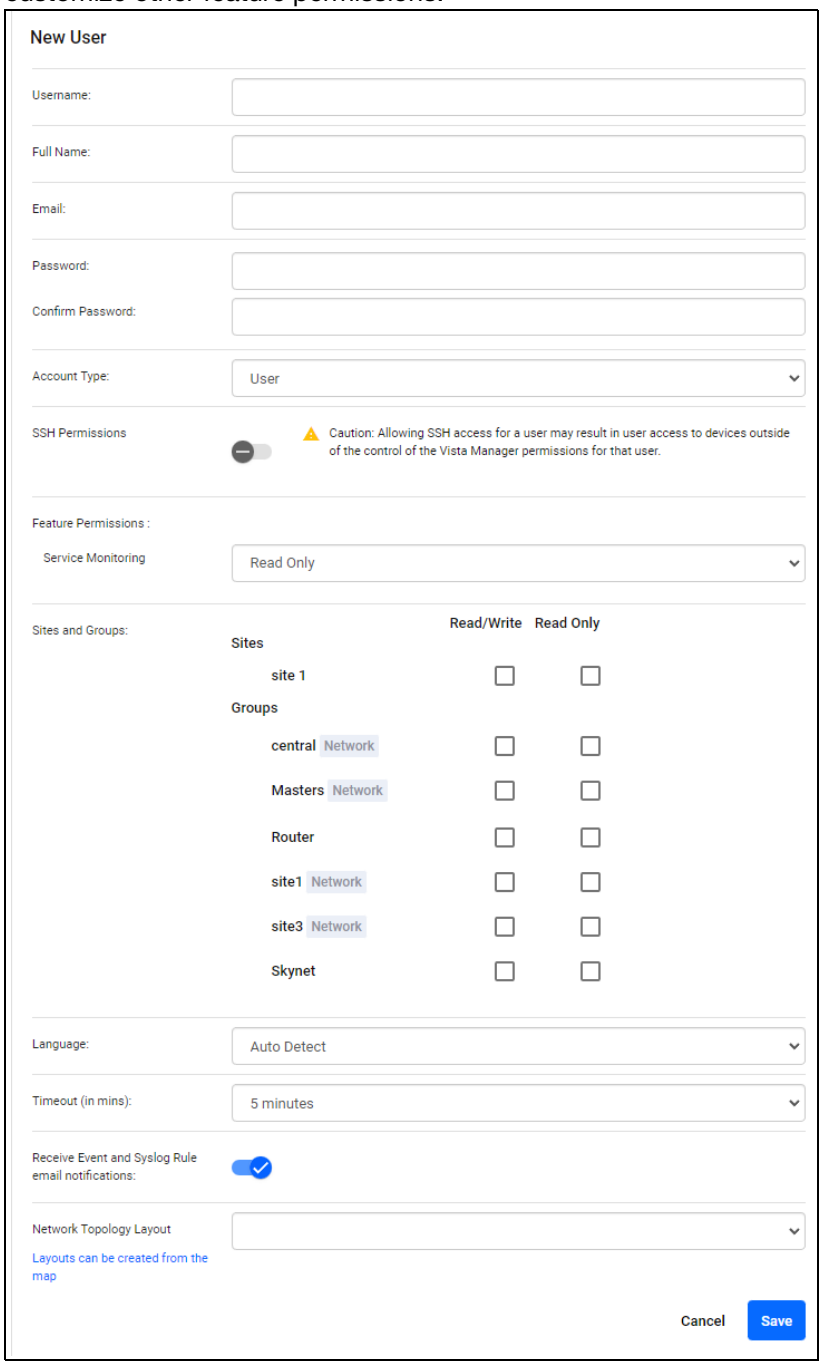
1. Click on the **IP Reputation** and **Web Control** buttons to view respective graphs.
2. For IP Reputation, click the drop-down list to select the UTM firewall device from a specific location to view.
3. For Web Control, click the drop-down list to select the UTM firewall device from a specific location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



User Management

From the User Management menu, you can create new users and manage your account. There are two types of user account, **Admin** and **User**. The User Management page is only accessible to Admin users. Any other account types do not have access.

Admin accounts have read/write access across all AMF areas. An Admin can create other user accounts and give them specific access to read/write permissions for sites and groups, as well as customize other feature permissions.



Create an account

1. Log in with an Administrator account type and select **User Management** from the menu item.
2. Click the **+Create New** button in the upper right hand corner of the screen.

3. In the **New User** dialog boxes enter the relevant user details.
4. 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

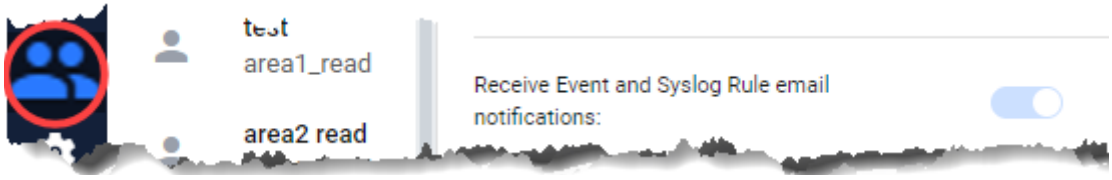
1. Log in with an Administrator account type.
2. Select **User Management** from the menu item.
3. Select the account you want to delete from the account list.
4. Click the **Delete** button.
5. From the Delete User dialog box click the **Delete** button again.

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

Event and Syslog Notifications

Event and syslog notifications are enabled by default for all users. This setting determines whether a user will receive an email when a syslog matches a syslog rule configured with email notification. Admin users can enable/disable email notification for all users.

As a non-admin user, you can change this setting only for yourself.



Permissions

Service Monitoring Permissions

Service monitoring permissions can be changed to be user-specific. This affects what a user can see on the Service Monitoring page. You can change permissions between Read Only, or Read/ Write.

Syslog Permissions

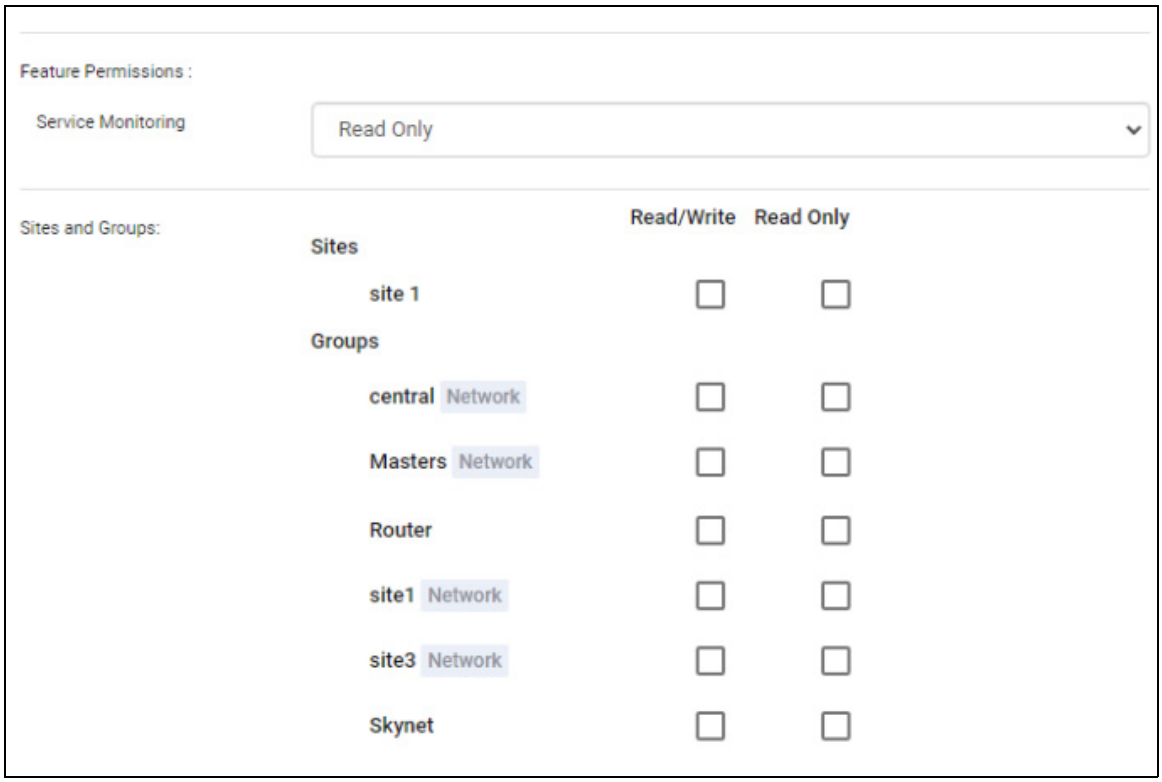
- Only an admin user can view all syslog messages received from an IP address that Vista Manager has not discovered in the network.
- Any device can send syslog messages. If the source IP address does not correspond with a Vista device, only an admin user can view the message.
- A user can only view 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.

Sites and Groups Permissions

Groups that correspond to a network have a gray badge next to them.

As an administrator, you can edit both feature permissions and specific sites and groups permissions from Read Only or Read/Write for each user.

In the event the user would like to restrict permissions to specific users for different sites or groups, the permissions can be changed in the **Sites and Groups** menu. Groups corresponding to specific networks have a gray badge next to their names.

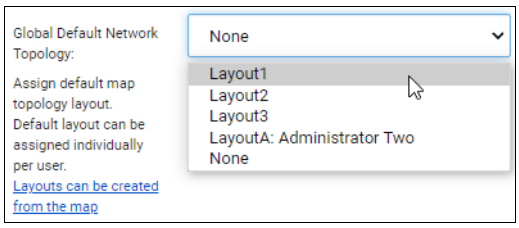


Setting the default network topology layout for all users

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.



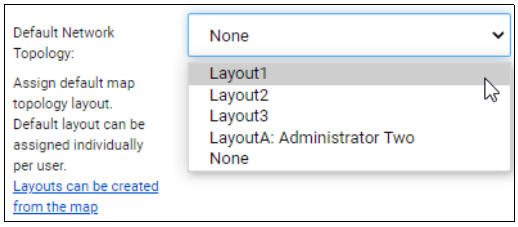
4. Click on the **Save** button.

Setting the default network topology layout for a specific user

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.



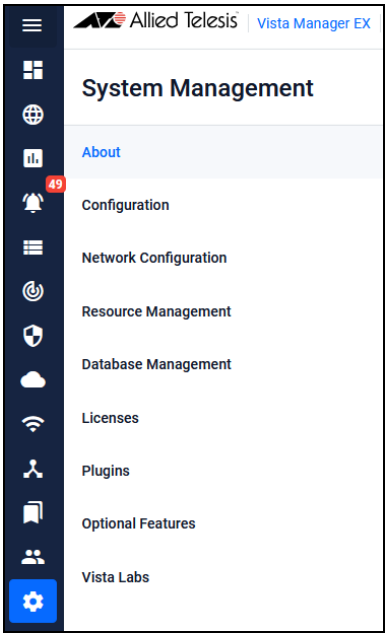
4. Click on the **Save** button.

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.

System Management

Navigating the System Management menu

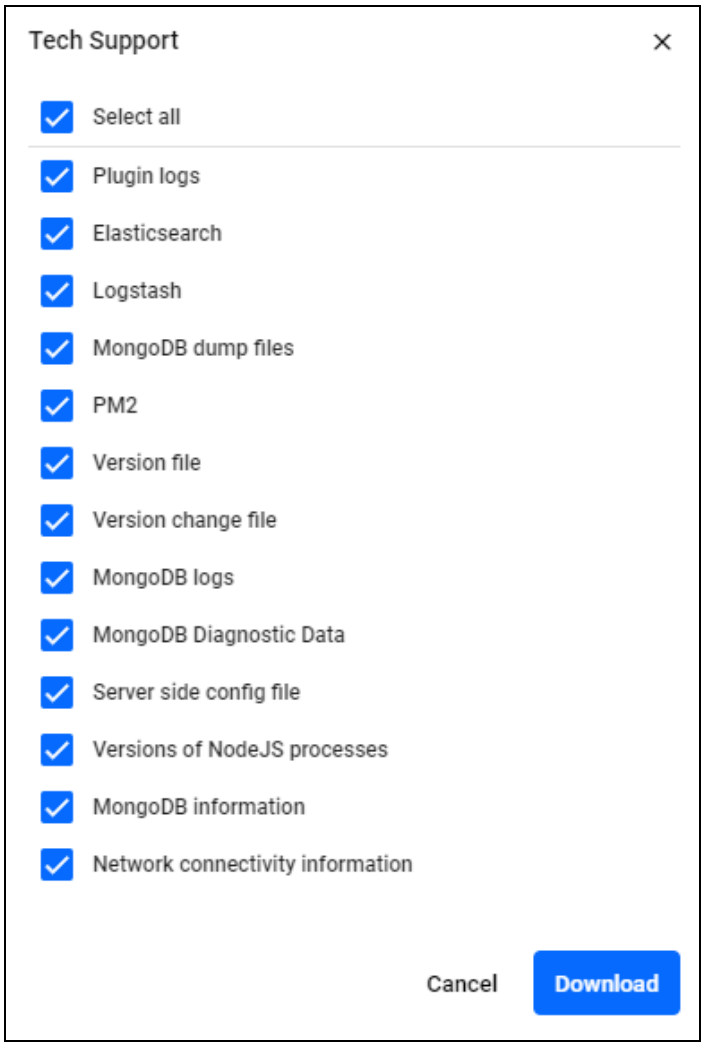
The Vista Manager EX system itself can be managed in the System Management menu. At a glance. the menu contains the following features:



Generating Tech Support Information

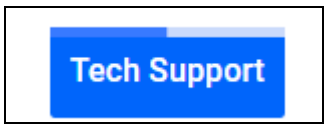
In the event that you encounter any issues, tech support information can be generated from the System management menu on any page by clicking on the **Tech Support** button in the top left.

You can to select different categories of information and logs which can be used by an Allied Telesis Customer Support representative to help with any problems you may be experiencing and diagnose any network problems.



You can click on the **Download** button to generate a Tech Support zip file. Clicking on this button will download a zip file named **vista_tech_support.zip** with the information you have selected to your local PC.

When the files are downloading, a bar above the Tech Support button will move to signify the download is running.



If the Tech Support fails, Vista Manager will notify you in the bottom left with a notification. You can retry the download.

You can contact technical support from the Contact page on the Allied Telesis website.

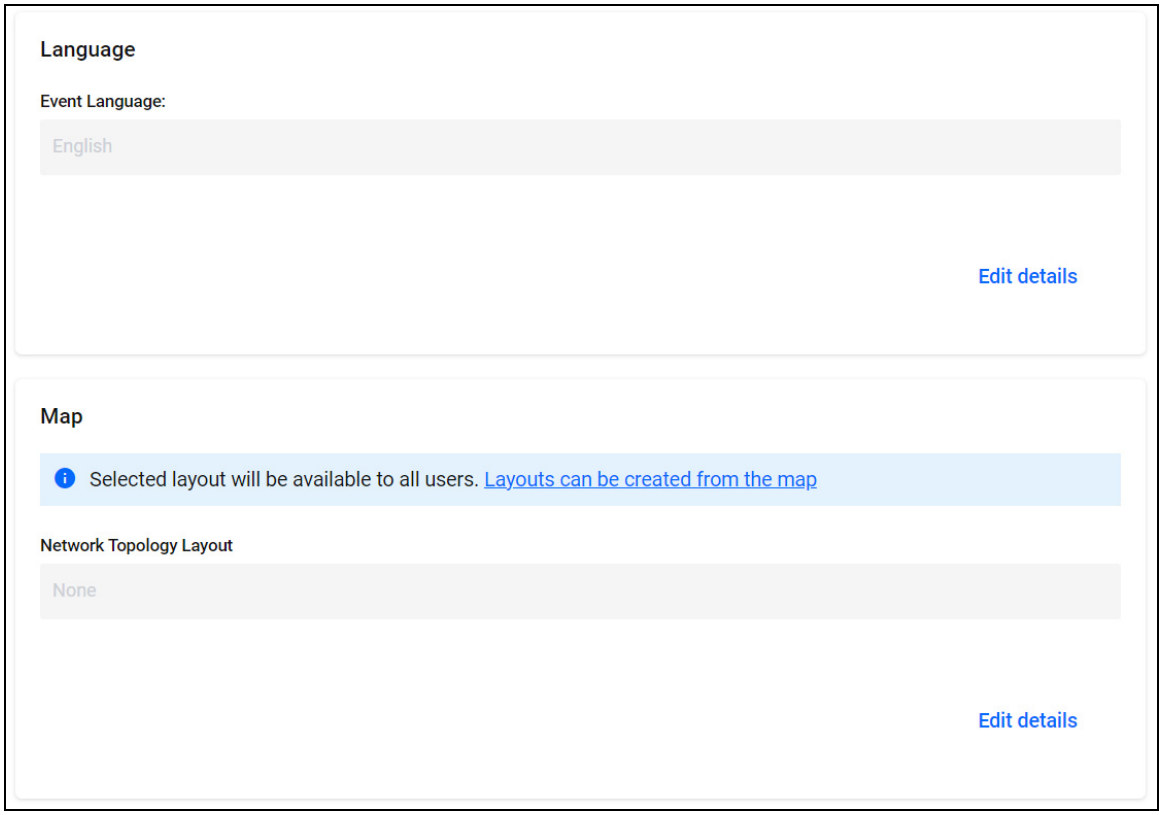
About

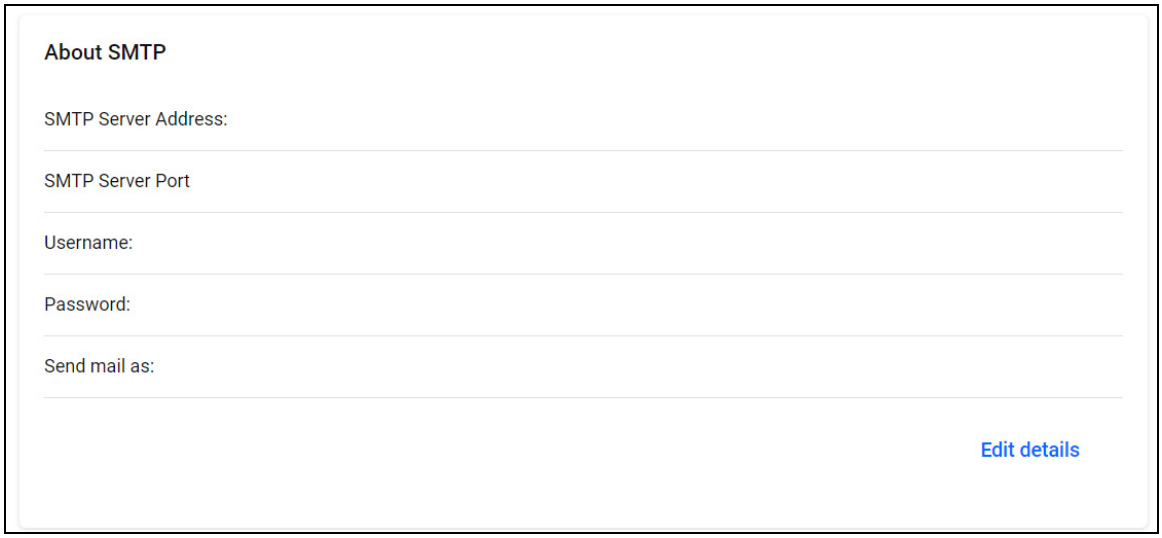
The **About** section shows key information about the current release of Vista Manager EX such as:

- Vista Manager EX version, build, serial number and base license expiry date.
- Device GUI version and build.
- Language information for events.
- Default Map layout for all users.
- About SMTP section

You can edit the details of the following sections:

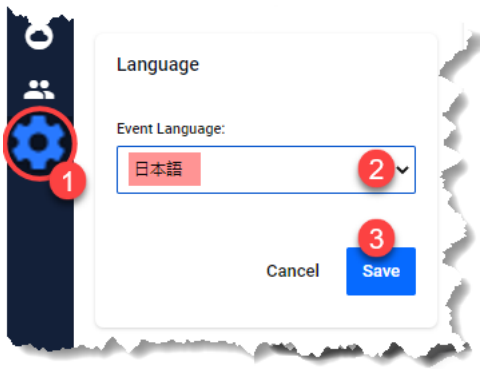
- Language - Change the event language
- Map - Change the default network topology layout used for all users
- About SMTP - Change various SMTP settings





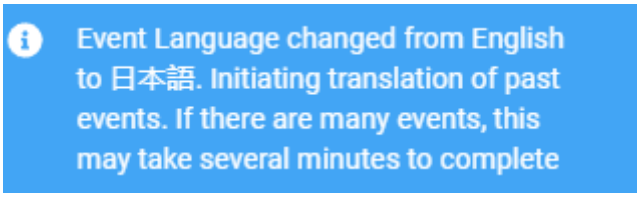
Event Language Support

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



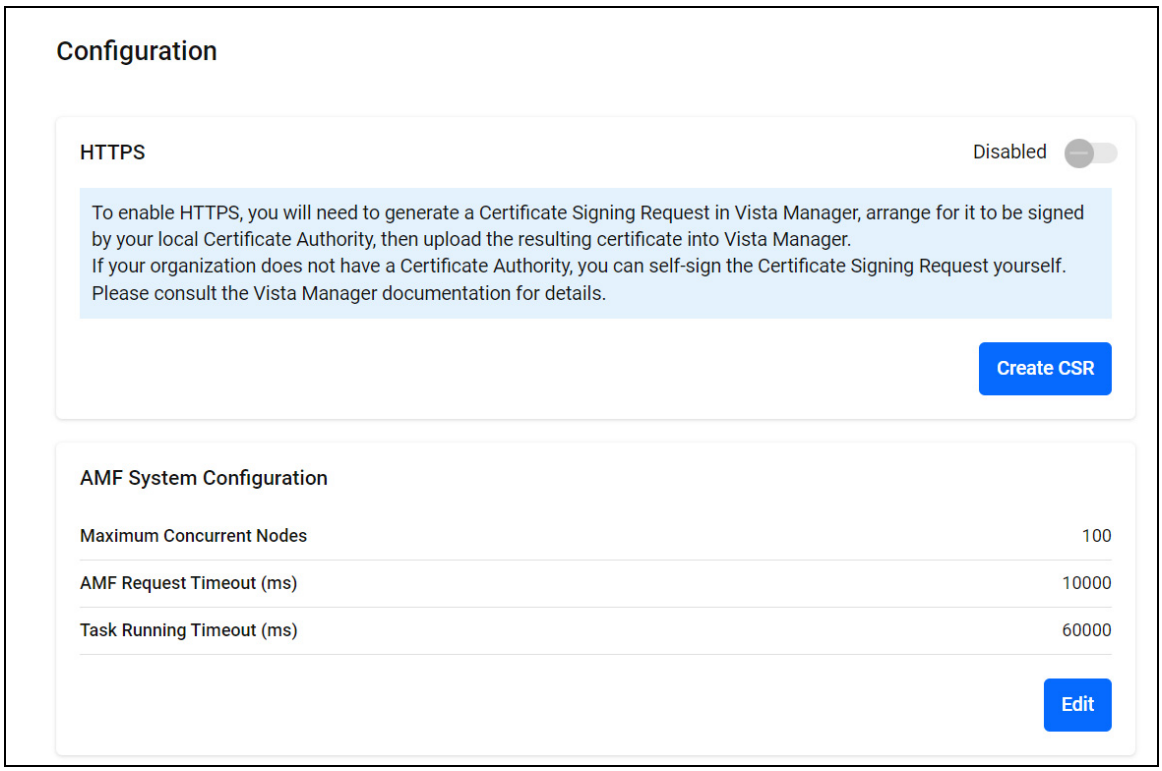
Click **Edit Details** under the Language section to do so.

When changing an Event language, a confirmation will display.



Configuration

The **Configuration** section displays the status of HTTPS and AMF System Configuration settings. Here you can enable HTTPS and edit the AMF system configuration settings.



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.

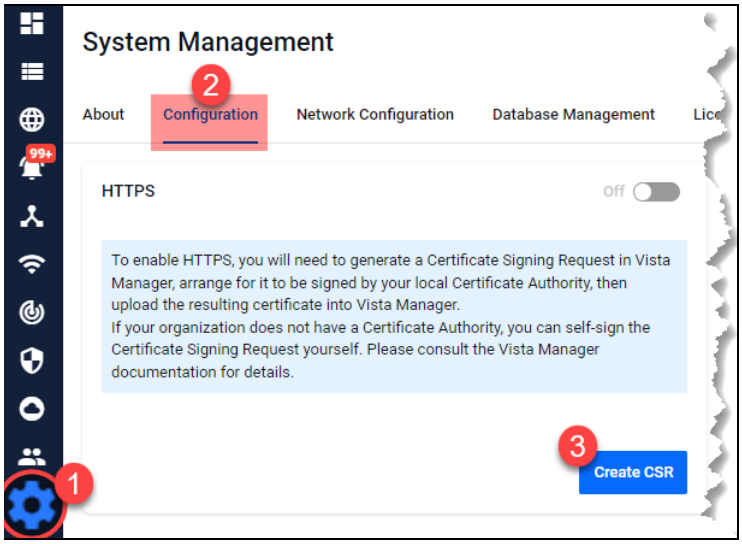
Vista Manager EX can generate a Certificate Signing Request (CSR) which you can then submit to a Certificate Authority (CA). The CA will then give you a signed certificate which you can import back into Vista Manager EX. Note that both the application's and CA's private key are never transmitted; this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

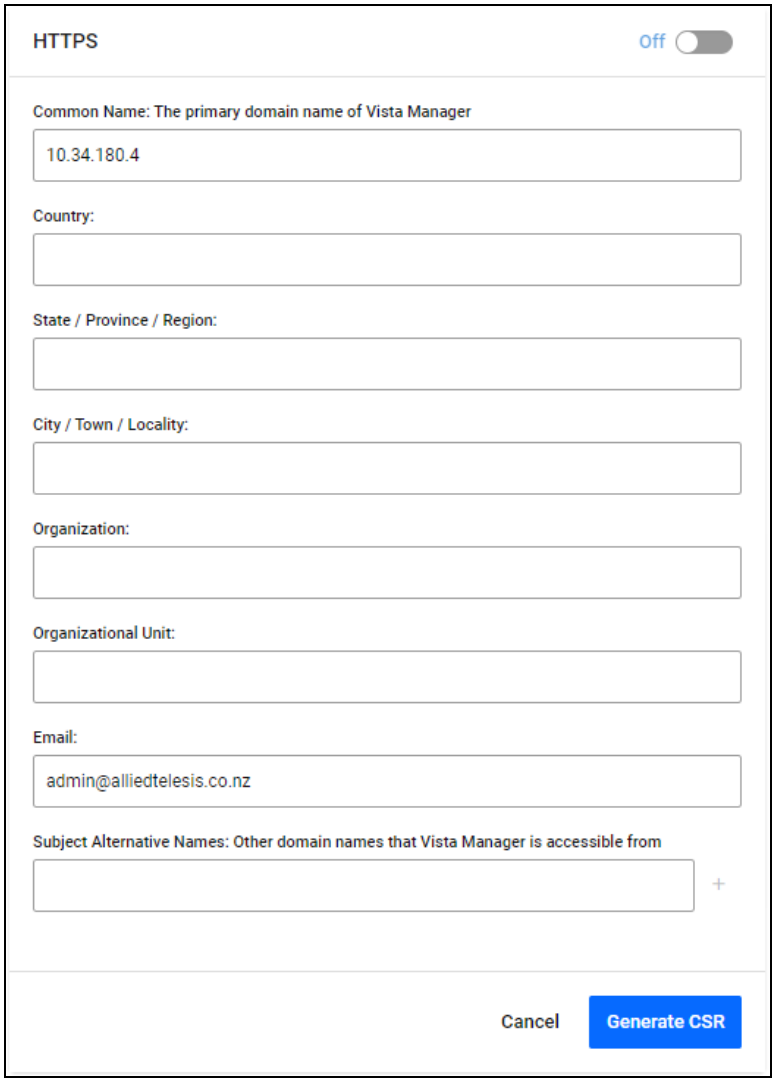
Alternatively, you can use OpenSSL to self-sign the CSR. For more information, visit https://www.openssl.org/.

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

To enable HTTPS:

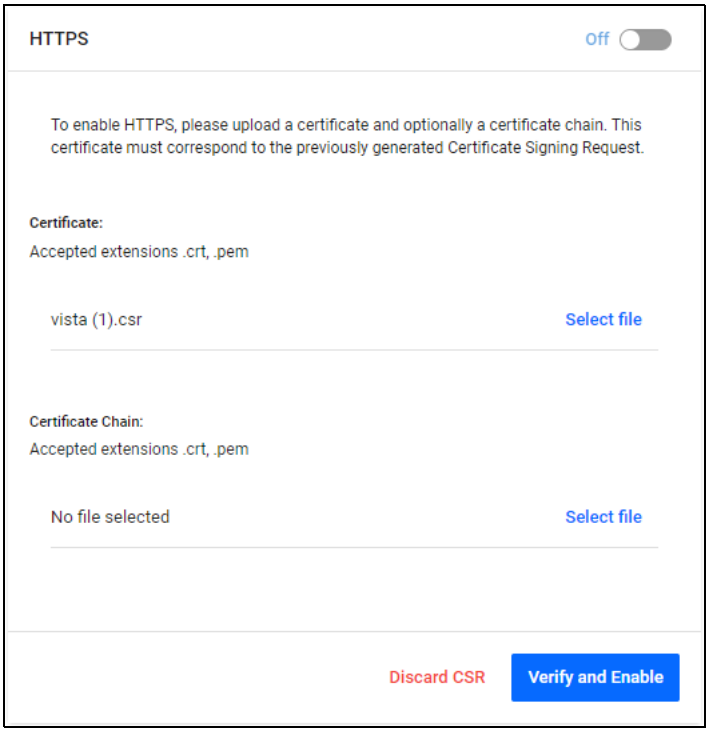
1. In Vista Manager, open the System Management menu item.
2. Then go to the Configuration tab.
3. Click on **Create CSR**.





- Make sure the primary domain name and email are correct. You can also add other domain names if required.
- Once the CSR has been generated, save it somewhere safe. Send this CSR to your CA to be signed.
- Once the CA has returned to you with a certificate, click the **Next** button. Then upload the

certificate to Vista Manager. You can also optionally upload a certificate chain.



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

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

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

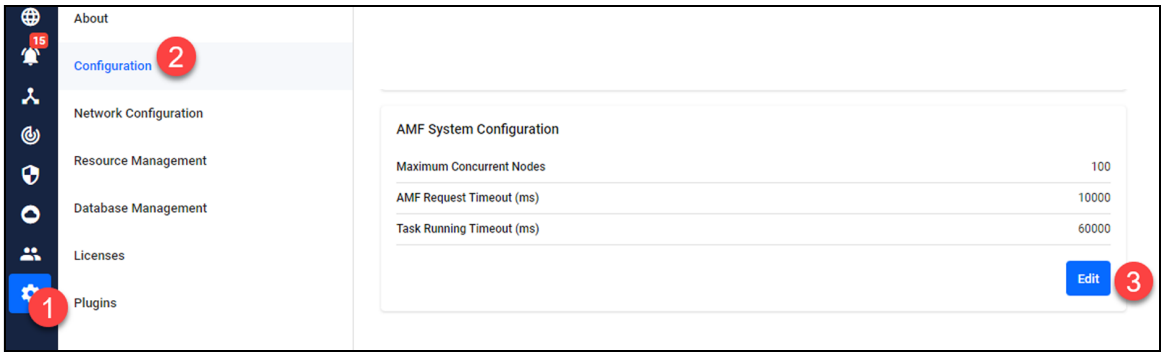
Changing the AMF system configuration settings

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.

Click **Save** when complete.



Note: No restarting is required.

Support for SMTP OAuth Configuration

From version 3.15.0 onwards, you can use OAuth as an SMTP authorization method by configuring OAuth for SMTP.

OAuth allows Vista Manager to securely request permission to send emails on your behalf without storing your password.

Support for SMTP OAuth is supported with the following email providers:

- Google
- Microsoft

Note: You must access Vista Manager from the same hostname as specified in your redirect URI for security reasons. We recommend using the most public hostname of your Vista Manager EX server or a DNS-allocated host address.
Your redirect URI must use HTTPS.

How to configure OAuth with Microsoft

You will need the following prior to setup:

- an Azure subscription,
- a Microsoft Entra Subscription,
- and an Outlook Online subscription with at least 1 user set up.
  Vista Manager will send emails from this account.

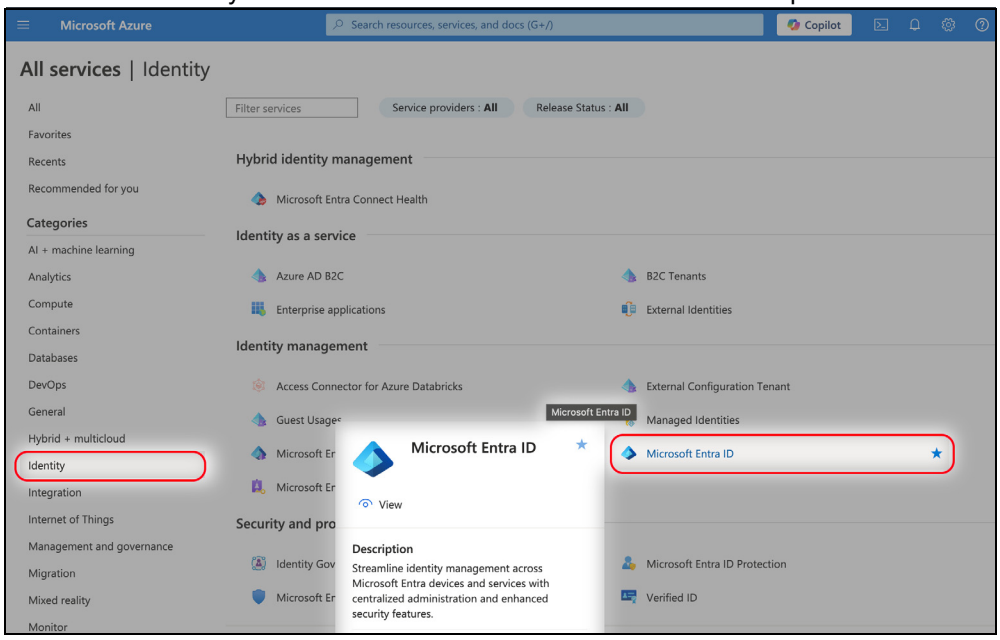
1. **Access the Azure Portal**

   Access the Azure Portal from https://portal.azure.com/#home and log in using your Microsoft Azure credentials.

2. Navigate to Microsoft Entra ID

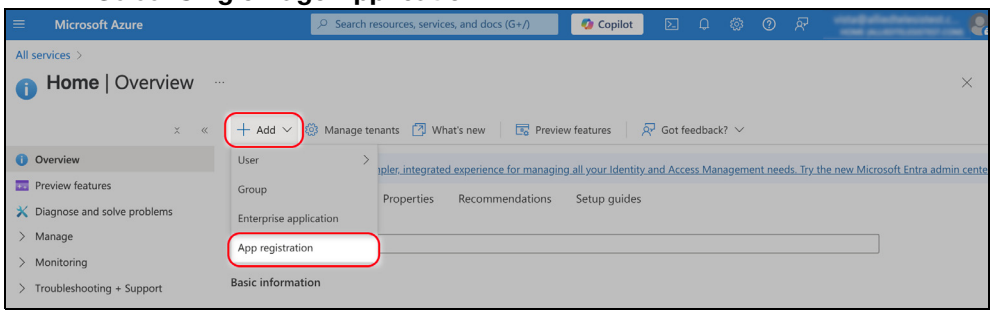
   Go to **All Services** > **Identity** > **Microsoft Entra ID**.

   - Alternatively search for Microsoft Entra ID and move to step 3.



3. Register a New Application

   - Click **Add** > **App Registration**
   - Select **Single Page Application**.



4. **Register an Application in Azure**

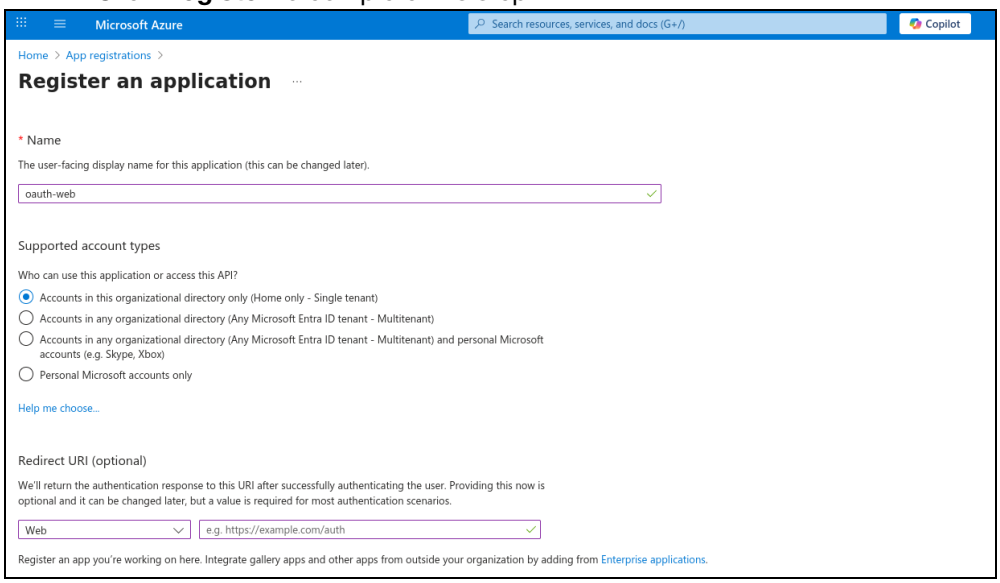
   Fill out the Application registration form with the required details:

   - For Web Application Type select **Single Tenant**
   - **Paste** the redirect URI from **Vista Manager**

This is auto-generated by Vista Manager in the "Redirect URI" form field.

Copy this from Vista Manager and paste it into the Redirect URI field in the Azure App Registration form. You can see how to get the Redirect URI from "Support for SMTP OAuth Configuration" on page 319.

- Click **Register** to complete this step.

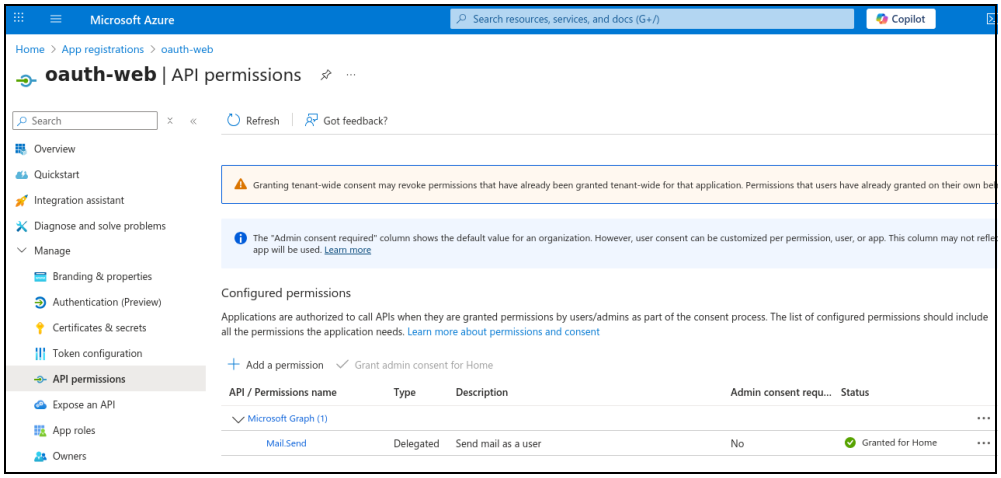


5. Assign Email-Sending Permissions to Azure for Vista Manager

In the Azure Portal, go to the App Registration for Vista Manager.

Under API Permissions, add a new permission for Microsoft Graph:

- Type - **Delegated**
- Permission - **Mail.Send**



- Click **Register**
- The Application Overview page will open where you can find the Tenant ID and Client ID

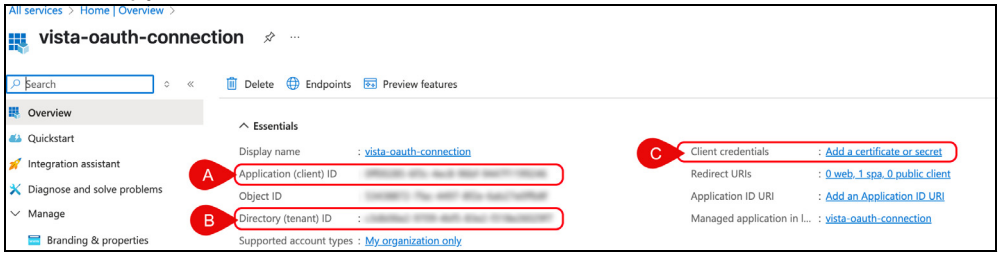
6. Complete Registration and Collect IDs from the Application Overview page

a. Copy the Client ID

b. Copy the Tenant ID

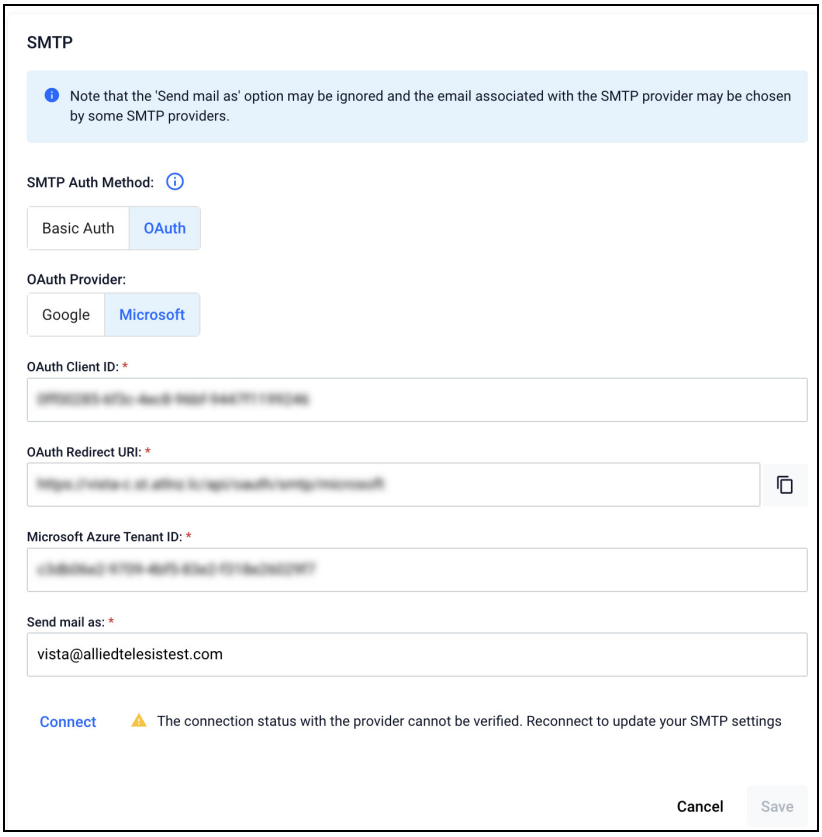
c. Click the 'Client Credentials' link and create a new Client Secret

- Copy the Client Secret



7. Set up the OAuth in Vista Manager

- Go to the **System Management** > **Configuration** page.
- Scroll down to the SMTP settings and click **Edit**.
- Under the SMTP Auth Method, select the OAuth tab.
- Select from Microsoft as a provider and enter the previously copied Client ID, Tenant ID, and Client Secret



8. Connect your Microsoft Entra account with Vista Manager

- Click **Connect and Save** to go to the Microsoft landing page.
- Sign in with your Microsoft Entra credentials, and you will be sent back to Vista Manager.
- You will see a **Green Tick** when the connection is successful.
- If verification takes longer than 30 seconds a warning message is shown.

Configuration of an Application with Google

You will need the following prior to setup:

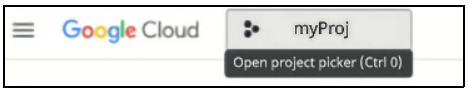
- a Google Workspace account
- access to the Google Cloud Platform

1. Access the Google Cloud platform

   Navigate to https://console.cloud.google.com/ and log in using your Google account credentials.

2. Create a new OAuth project

   - Click on the Project button in the top navigation bar



   - Select New Project

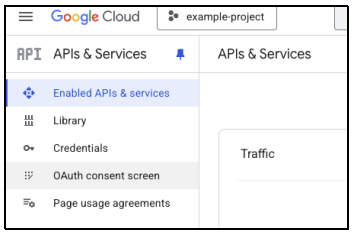
   - Enter a name (such as myProj) for your project and click **Create**.

3. Create a new OAuth Client

   - Click on the name of the existing project to go to the Overview screen.
   - On the Overview page, click the **Create OAuth client**
   - Enter Application information for your project

4. Configure OAuth Consent Screen

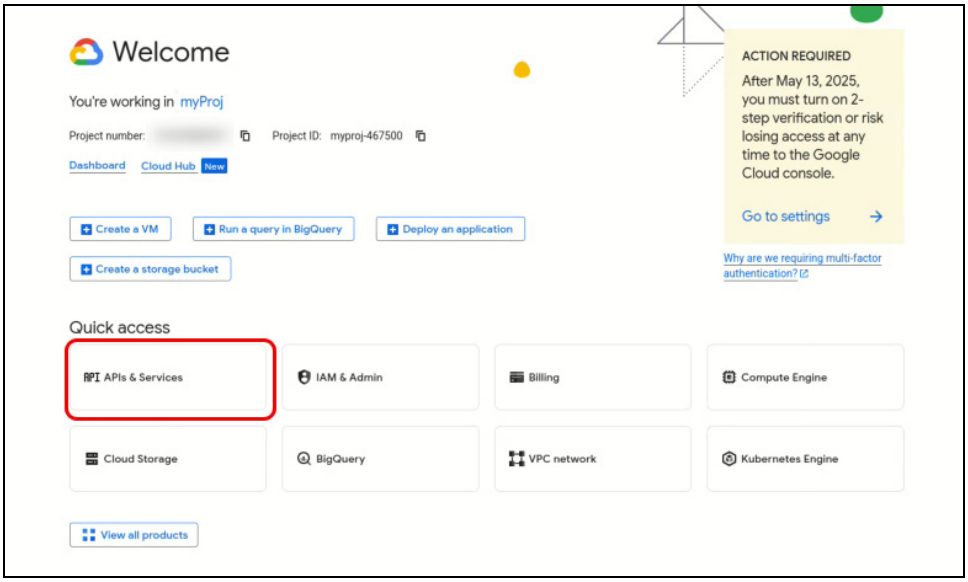
   - In the left menu, select OAuth consent screen.



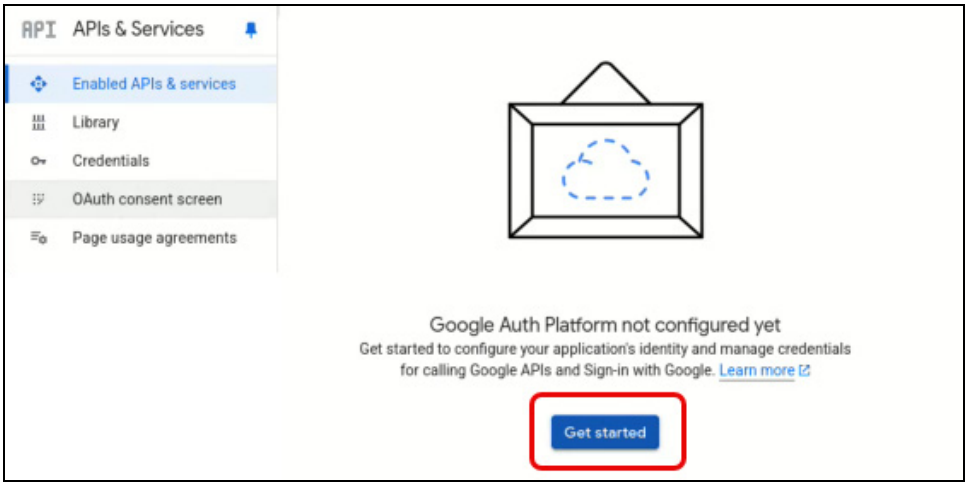
   - We recommend selecting **Internal** as Google Workspaces will restrict access to 'send emails as' to emails within your organization.
   - Fill in the required fields (App name, User support email, Developer contact information)
   - Save and continue

5. Configure the Google Auth Platform

   - On your newly created project's dashboard, click **APIs & Services** button



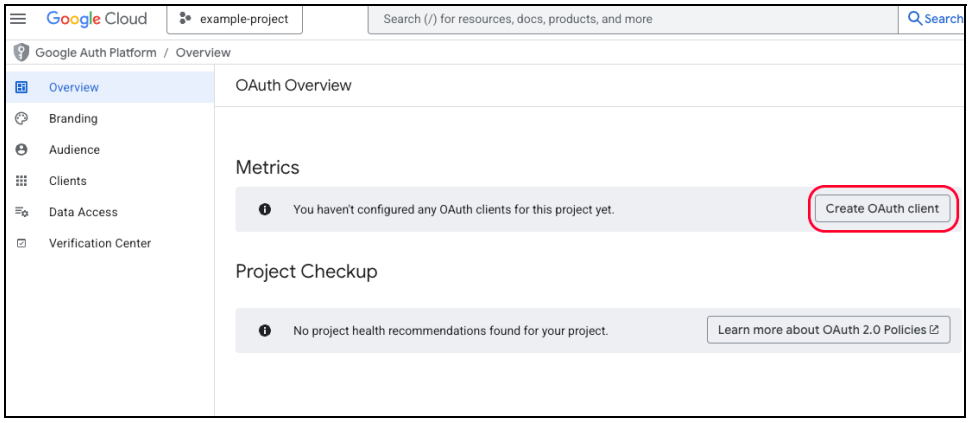
- Click **Get Started**



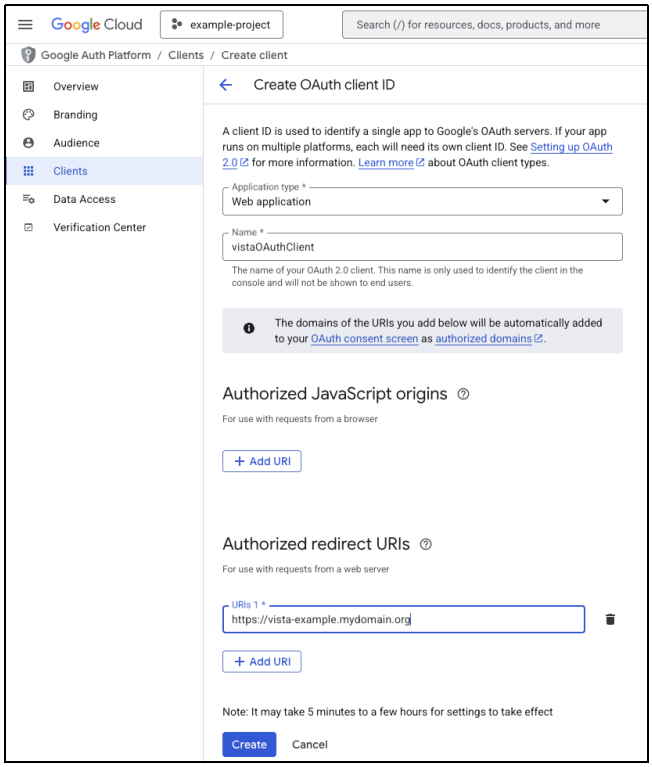
- Enter the project configuration information, and click **Create** when done.
- This will take you to the OAuth Overview page.

6. Create OAuth Client ID Credentials

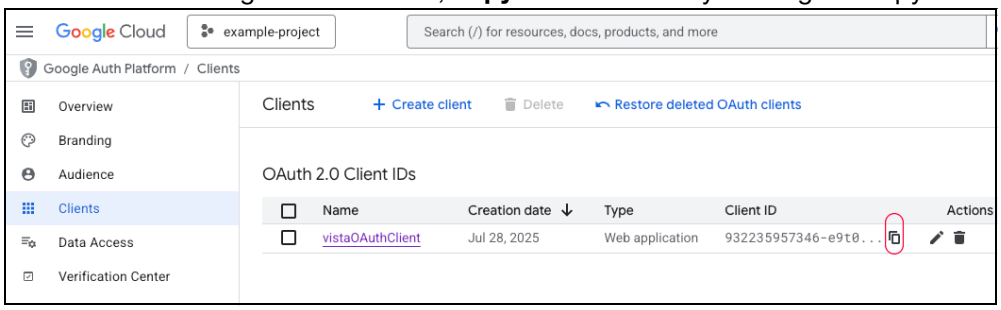
- From the OAuth Overview page, click **Create OAuth Client**



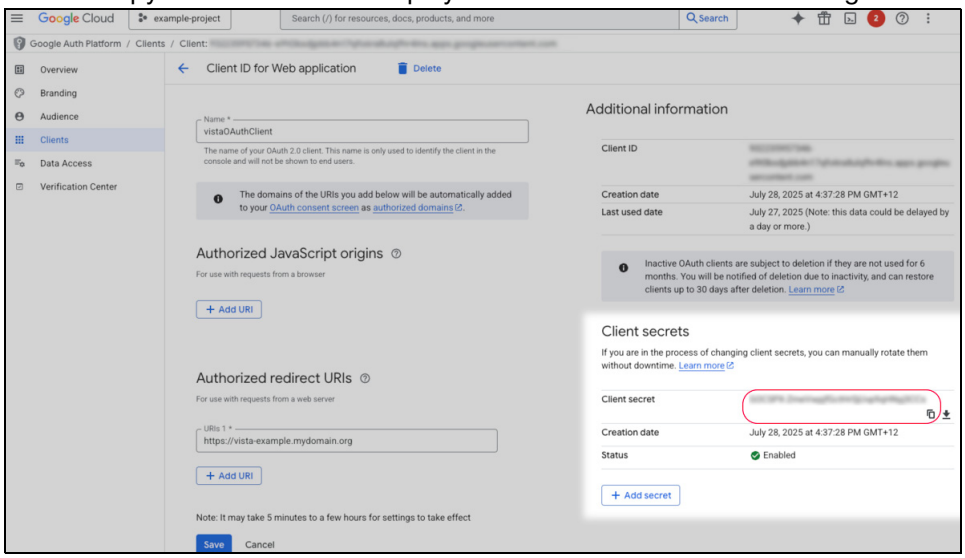
- In the **Authorized redirect URIs** section, add the redirect URI provided by Vista Manager.



- Click **Create**
- After creating the credentials, **copy the Client ID** by clicking the copy icon

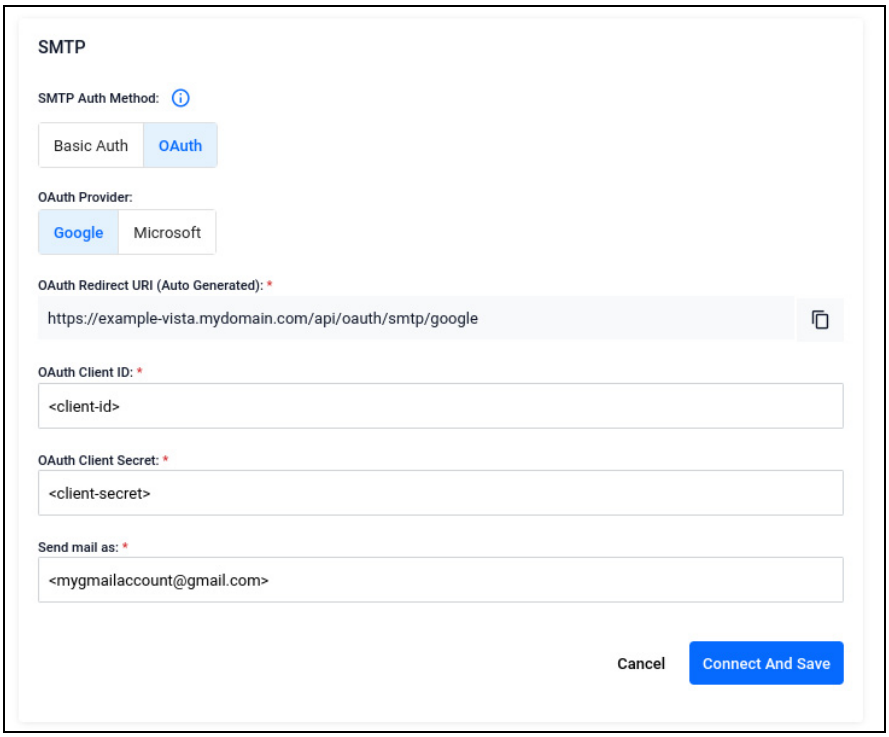


- Click on the **name of the new Client ID** to go to the Client ID for Web application page.
- Copy the Client Secret displayed on the screen in the bottom right.



7. Set up the OAuth in Vista Manager

   - Go to the **System Management** > **Configuration** page.
   - Scroll down to the SMTP settings and click **Edit**.
   - Under the SMTP Auth Method, select the OAuth tab.
   - Select from Google as a provider and enter the previously copied OAuth Client ID and OAuth Client Secret
   - Enter the email account you would like to send emails as
   - Click **Connect** and **Save**



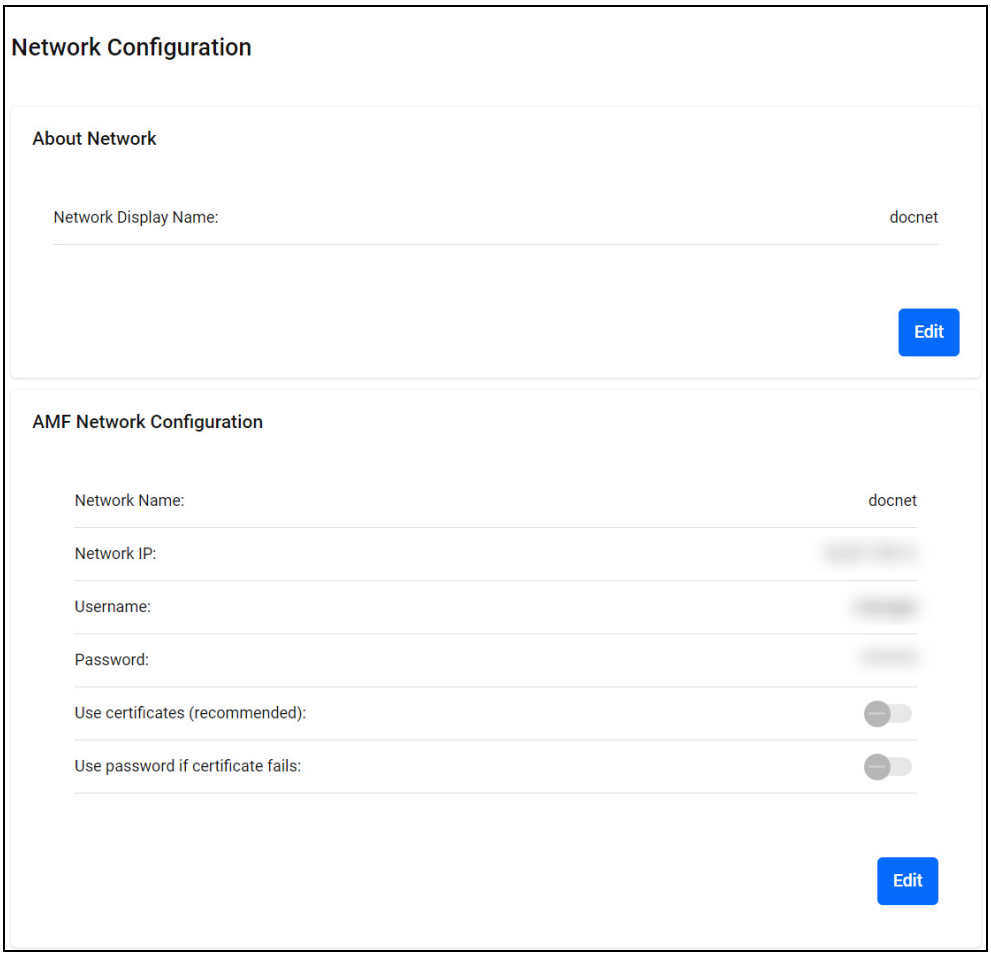
   - If verification takes longer than 30 seconds a warning message is shown.

8. Connect your Google account with Vista Manager

   - Click **Connect and Save** to go to the Google landing page.
   - Sign in with your Google account, and you will be sent back to Vista Manager.
   - You will see a **Green Tick** when the connection is successful.

Network Configuration

The **Network Configuration** section shows the Network Display Name and AMF Network Configuration settings. You are able to edit the network display name and AMF Network Configuration details from this page.

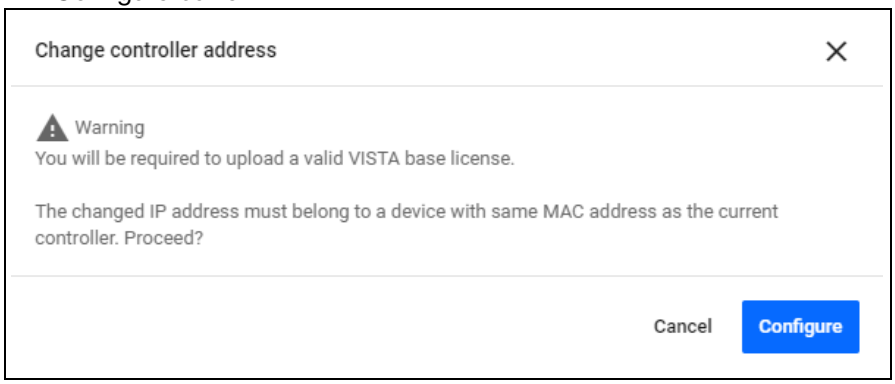


Changing the Vista Manager EX controller IP address

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

1. Click on System Management, and select the Network Configuration tab.
2. Under AMF Network Configuration, click on the Edit button.
3. Click on the Change controller address button. Once you have confirmed that the changed IP address belongs to a device with the same MAC address as the current controller, click on the

Configure button.



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

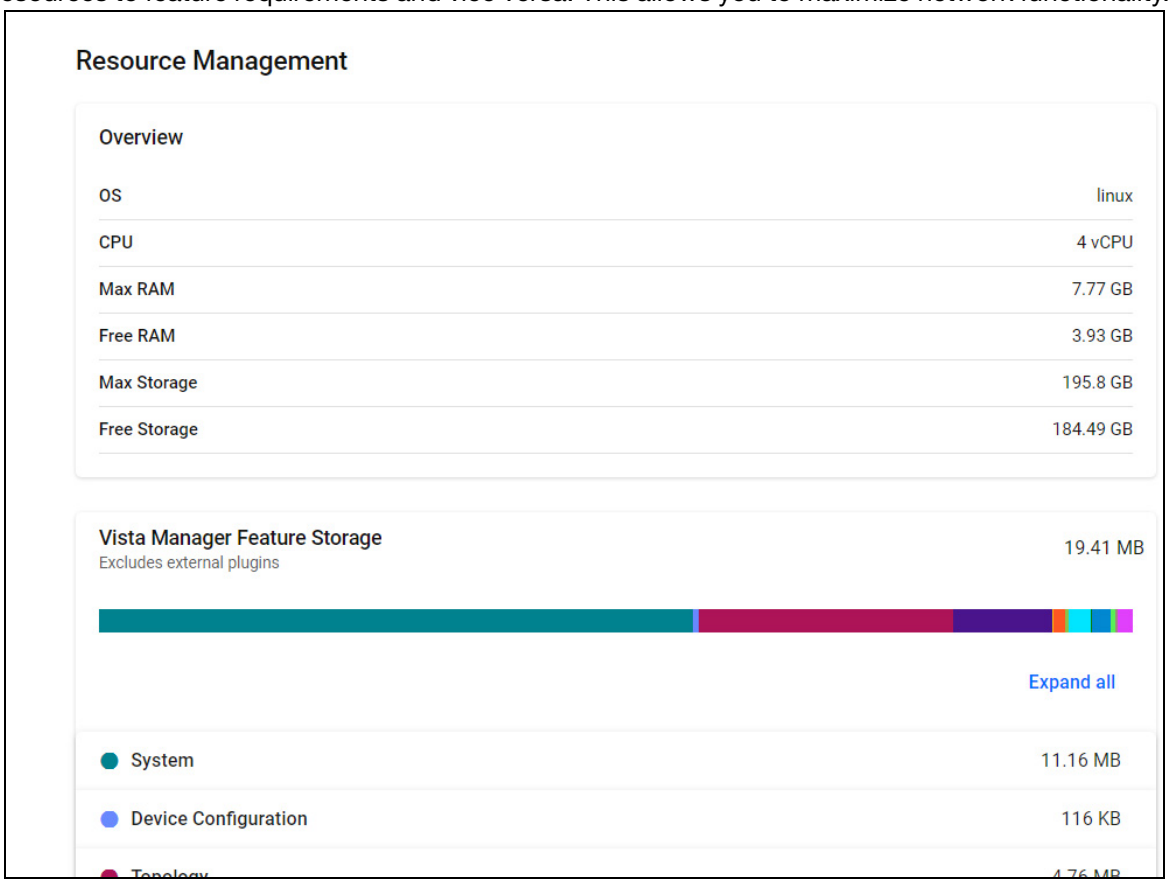
Note: The changed IP address must belong to a device with the same MAC address as the current controller.

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

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

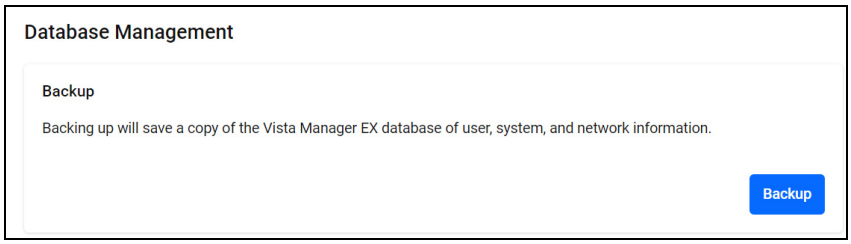
Resource Management

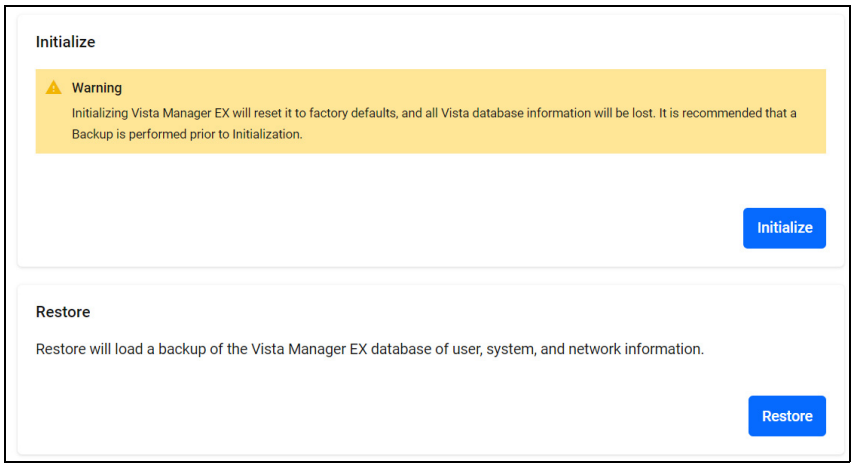
From the **Resource Management** page, you can see information about your system storage and specifications. From this page, you can manage what features are running and the amount of resources to use from the environment given (RAM/disk space/CPU). You can also match the resources to feature requirements and vice versa. This allows you to maximize network functionality.



Database Management: Backup and Restore

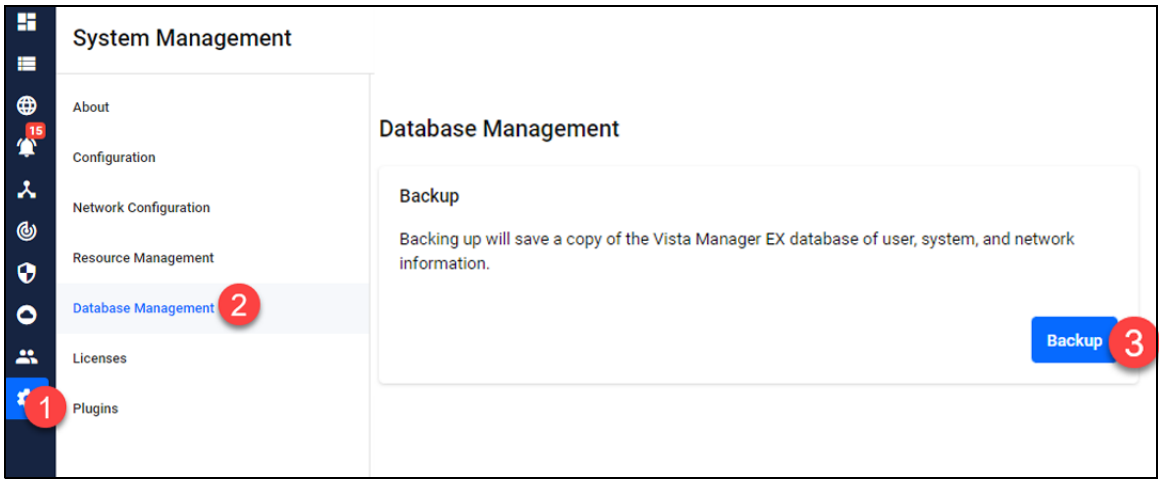
The **Database Management** page displays the Backup, Initialize, and Restore settings.





To backup your Vista Manager database, follow these steps:

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.

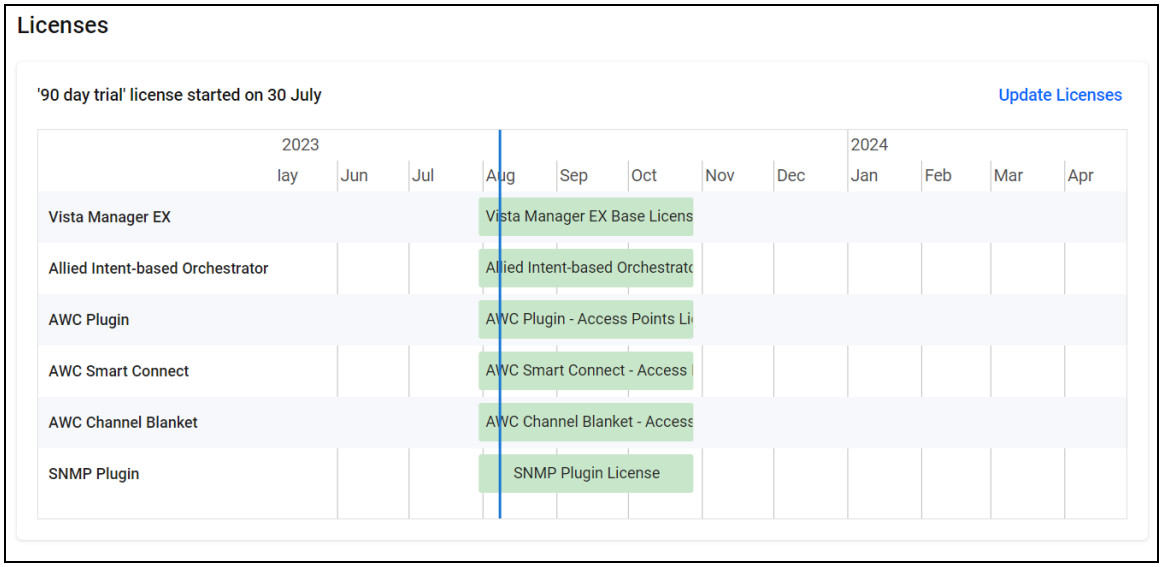


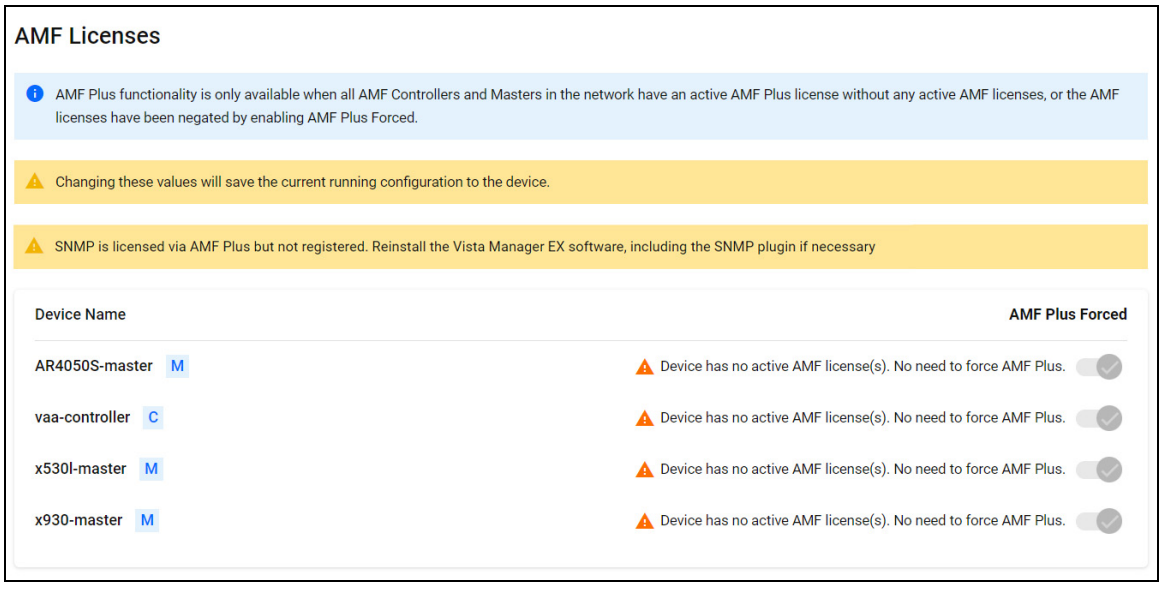
This automatically downloads a **tar** file backup to your default download location.
Keep this **tar** file in a safe location.

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.

Licenses

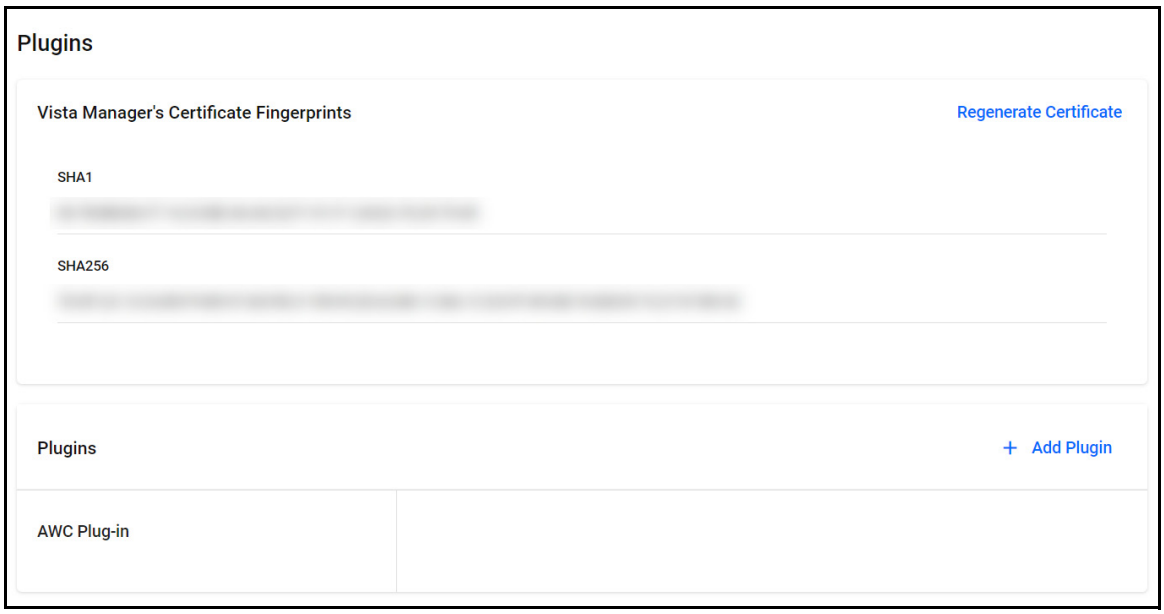
The **Licenses** page shows various licenses running on Vista Manager EX. You can update licenses from this menu. Note that this is different from device-specific licenses. For information on managing device-specific licenses see "Asset Management" on page 144.





Plugins

The **Plugins** section shows Vista Manager's certificate fingerprints (SHA1 and SHA256) and installed plugins on your network.

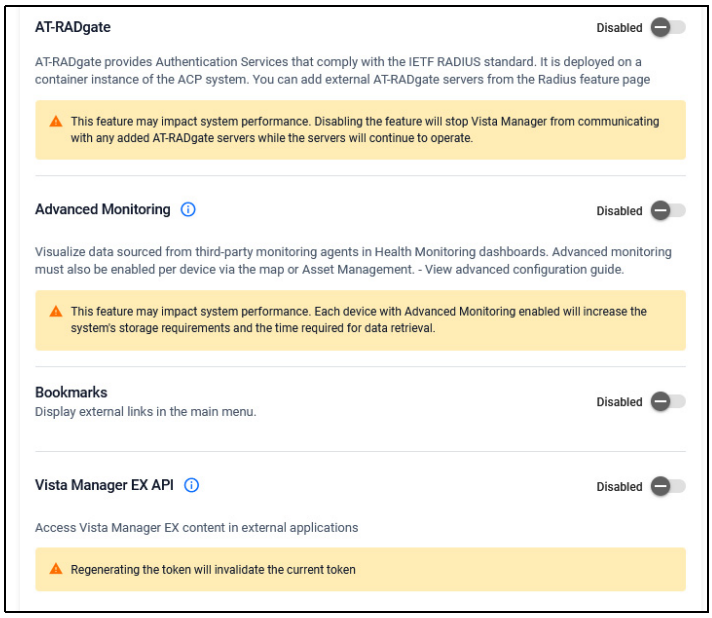


You are able to regenerate certificate fingerprints by clicking **Regenerate Certificate**. You can also register plugins from a server URL by clicking **+ Add Plugin**.

Optional Features

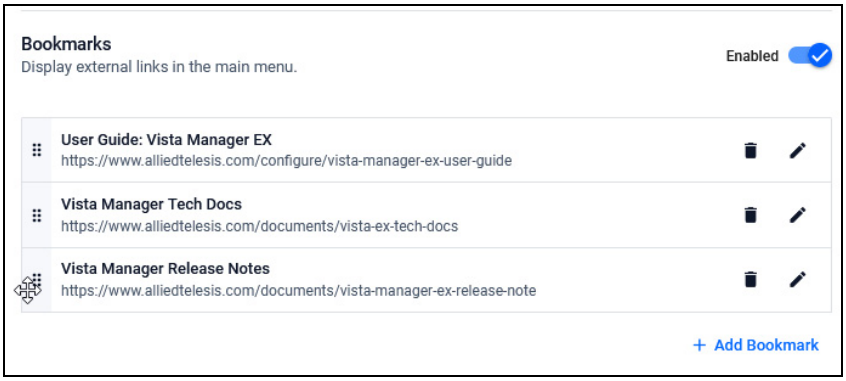
From the **Optional Features** tab, you can turn some features on and off from the System Management page. Turning off features can reduce the amount of memory Vista Manager uses.

Features you can turn on or off include AT-RADgate, Advanced Monitoring, Bookmarks, and the Vista Manager EX API access.



When you restore a backup, any features that were enabled at the time of the backup will remain enabled in when you restore that backup.

To see information on how to enable Bookmarks for easy access, see "Adding bookmarks" on page 34.



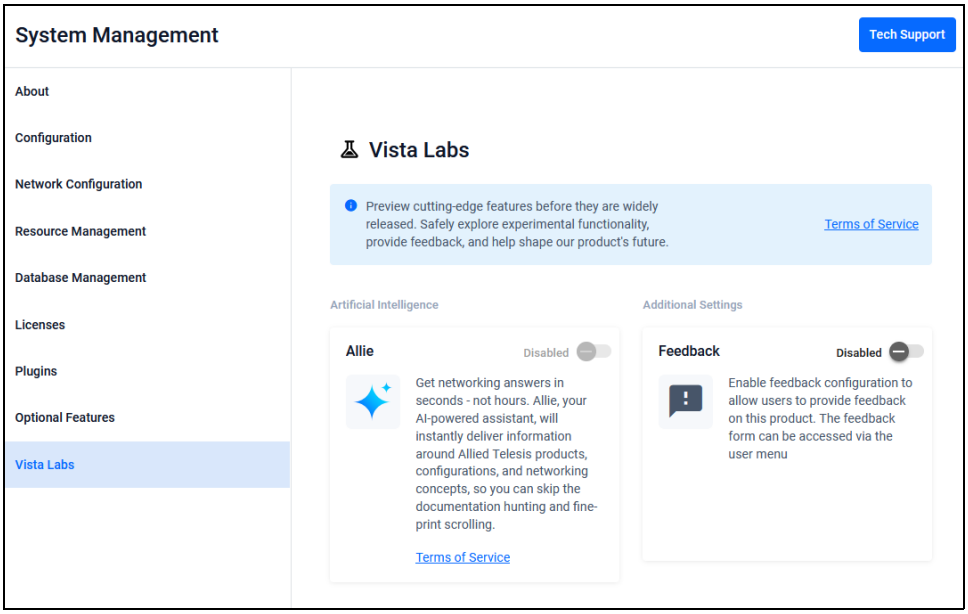
Vista Labs

From version 3.15.0 onwards, you can trial new or experimental features from the new Vista Labs menu.

A Terms of Service popup will appear when you click on the Vista Labs tab. Please read it prior to agreeing to use Vista Labs features. It can be viewed again from the Terms of Service link on the info-card above the features.

You will then have access to the Vista Labs features, and you can toggle on features you would like to use.

Currently, these new features include Allie, our AI assistant, and feedback for Vista Manager.

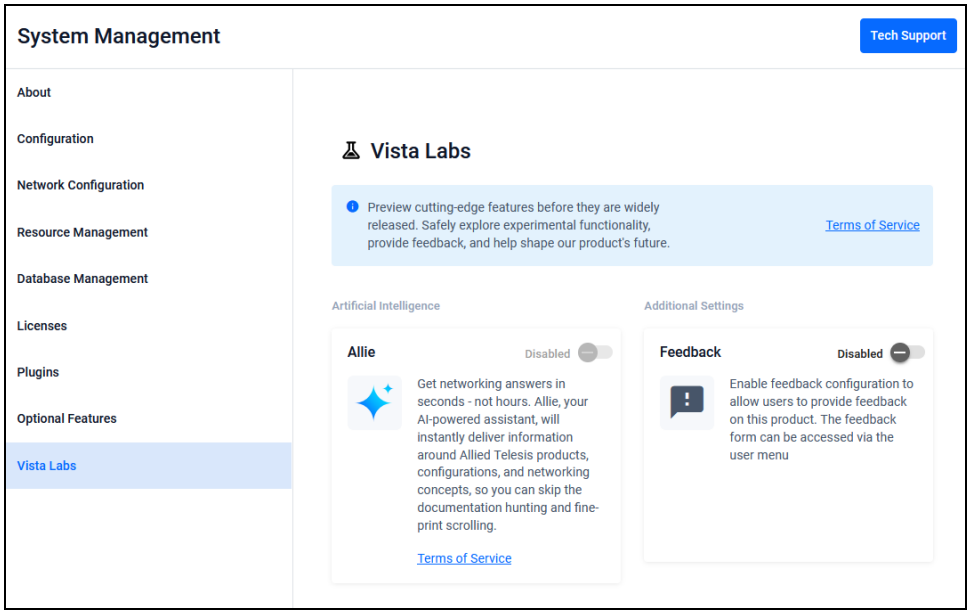


Toggle feedback to allow all users to provide feedback on Vista Manager. After toggling this, you can access the Feedback form from the User Management menu.

If you have any feedback for the Vista Labs features, use this Feedback form.

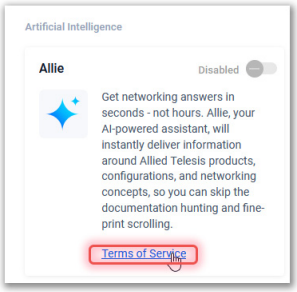
Using Allie

From version 3.15.0 onwards, you can access our AI assistant, Allie, within Vista Manager to receive assistance.

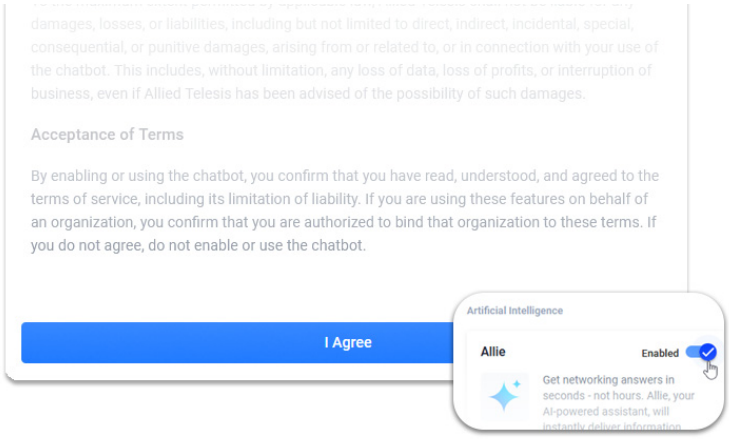


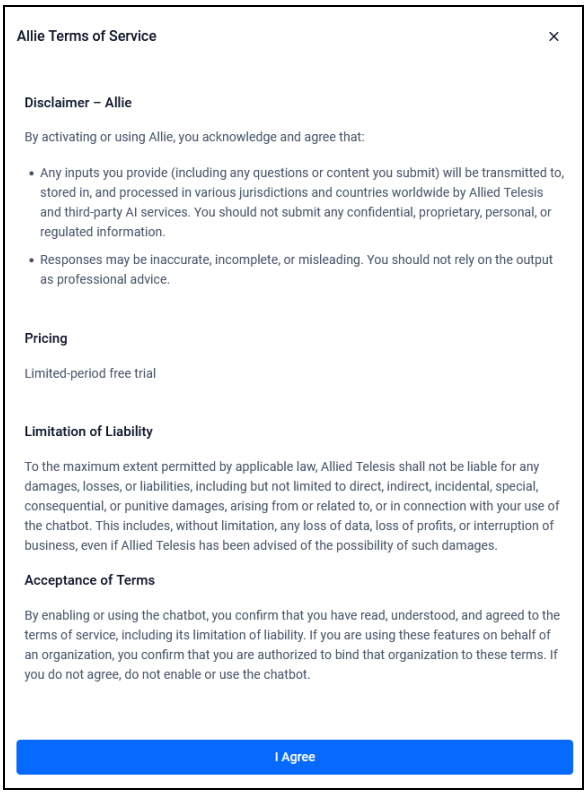
Allie can give you guidance on network configurations and features, networking concepts, and information on Allied Telesis products.

When you first see the widget, the Enable/Disable toggle will be greyed out.

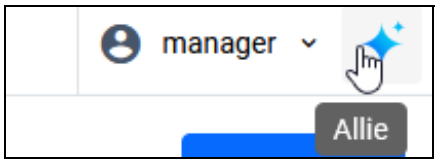


To enable Allie, you must first read Allie's Terms of Service under the widget before you can Enable the feature.





After you enable Allie, click the new icon in the top right corner to start a chat.


manager
Allie

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 plugin web interface. (This depends on which port you configured the AWC plugin to run on during installation.)
- TCP port 65437-65439, which the wireless APs use to communicate with the AWC plugin.
- TCP port 6443, which gives access to the SNMP plugin web interface.
- UDP port 162 (SNMP trap), used by SNMP devices to send traps to the SNMP plugin.
- TCP port 443 gives Vista Manager access to the Forescout API.
- TCP port 11443 gives Forescout access to CounterACT devices.

VA WIN You may need to create Windows inbound firewall rules and Virus scanning exclusions.

Upgrading versions earlier than 3.9.0

If you create a backup on a version earlier than 3.9.0, and you want to upgrade to a new version, you must first install your backup on version 3.9.0 and export the backup again.

Then you can upload the new backup to a later version of Vista Manager (such as v3.14.0).

If you upgrade directly to 3.14.0 instead (for example, from 3.7.0 to 3.14.0 without upgrading to 3.9.0 first), you may encounter data corruption or incompatibility issues. Alternatively, you can choose to perform a fresh install of the newer version and configure it from new.

Important Licensing changeover information

From version 3.14.0 onwards, we are preparing to migrate licensing systems. As of version 3.14.0, we will support both old and new licenses to prepare for the migration change.

We recommend you contact Allied Telesis Customer Support from the Support Portal in preparation to arrange new licenses for the licensed features before upgrading.

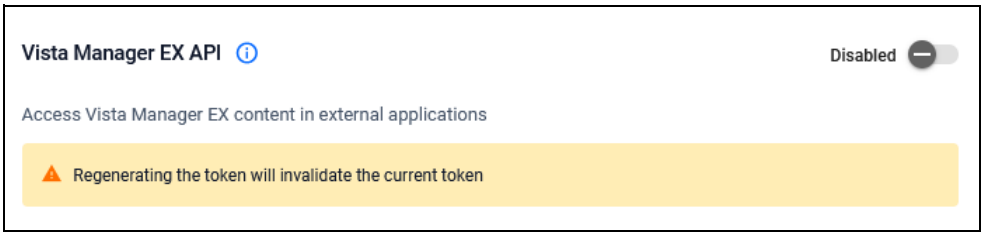
If you have not prepared licenses in advance and discover that this is an issue when upgrading, Vista Manager 3.14.0 continues to support older licenses. You can arrange new licenses and apply these before upgrading to a later version.

Vista Manager EX API

From version 3.14.0 onwards, you can access part of the APIs of Vista Manager to create custom applications.

You can create a token for access to the API from the **System Management** > **Configuration** page.

For more information about the Vista Manager EX API, contact Allied Telesis support.



Live Migration collections taking a long time to load

From version 3.13.1 onwards, a banner system has been implemented for live migration of collections that may take a long time. During a live migration, these collections may not display correctly and may be inaccurate during migration.

Live Migration is triggered when a database restore is performed. This is either enacted by you as a user from the **System** > **Database** screen, or automatically when AWC is upgrading the Vista Manager version.

Large collections include Health Monitoring information and history metrics, SDWAN history metrics, and pages with events, such as the Event page and Network Map.

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 plugin APIs are active using the following URLs:

- https://localhost:5443/wireless_plugin/api/plugin_registration
- {"version":"100","baseUrl":"http:\/\/localhost:8080\/wireless_plugin\/api","product":{"name":"AT-Vista Mana
plugin","type":"awc","version":{"major":"1","minor":"2","revision":"0","build":"B06"},"capabilities":["node
- https://localhost:6443/NetManager/api/plugin_registration

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

Note 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 17).

Problems adding plugins

If you are having difficulty adding the plugins in Vista Manager EX, make sure that you have done the following:

VRT APL WIN

- Check that you have the correct URL for each plugin as described in "Registering/Installing plugins" on page 26, 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 plugin. If you are upgrading from an earlier version, or porting to a different platform, you should re-register the SNMP plugin using the mixed-case URL.

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

where <ip-address> is the IP address of the SNMP plugin.

WIN
- Make sure that you have imported the plugin server certificates as described in the “Initial Login” section in the Vista Manager EX™ Installation Guide.

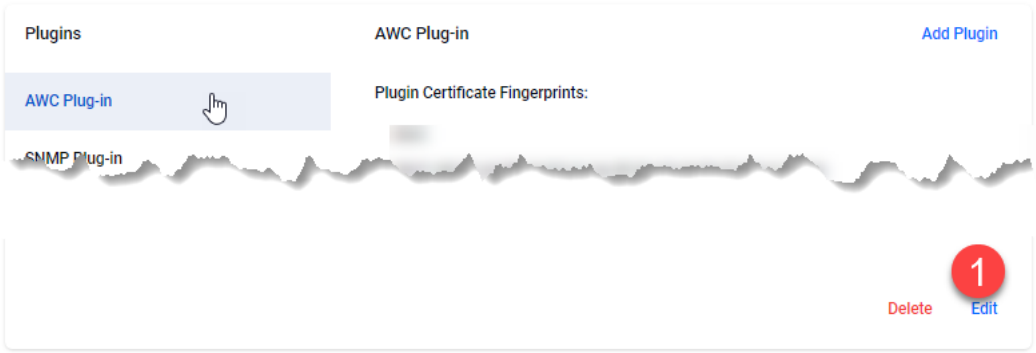
WIN
- Add the Vista Manager EX server address to your trusted sites as described in the Vista Manager EX™ Installation Guide.

WIN
- Add an exception for the server to your web proxy as described in the Vista Manager EX™ Installation Guide.

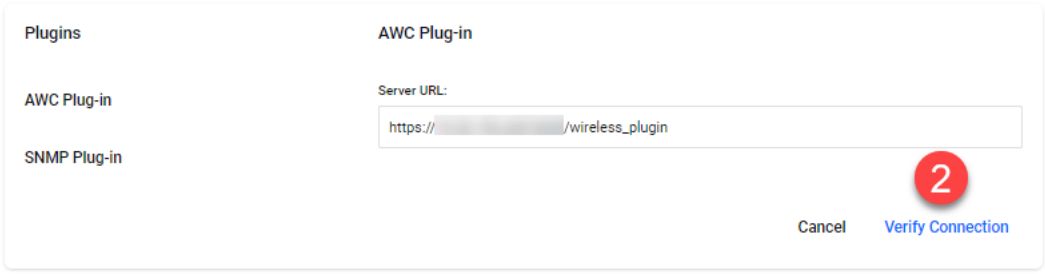
Updating plugins

If you are having issues with plugins, you can update a plugin without deleting it.

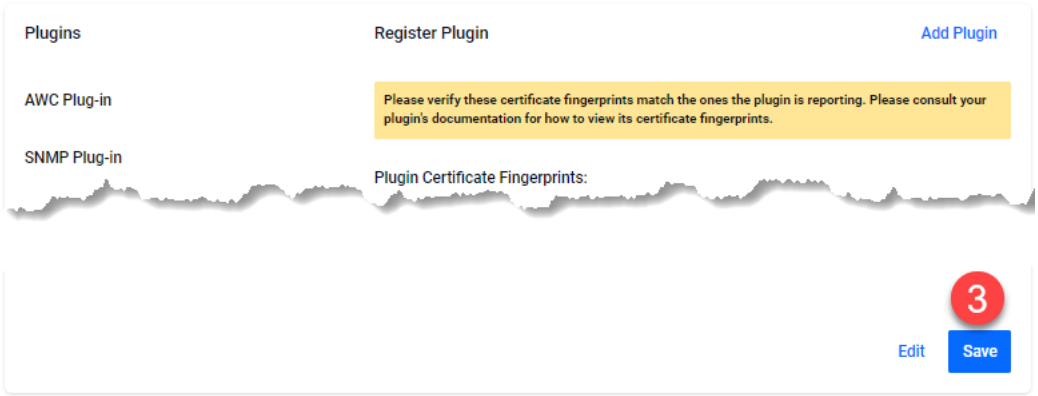
1. From the System Management menu, go to the **Plugins** tab. Select the plugin to update. Click **Edit**.



2. Click **Verify Connection**.



3. Click **Save**.

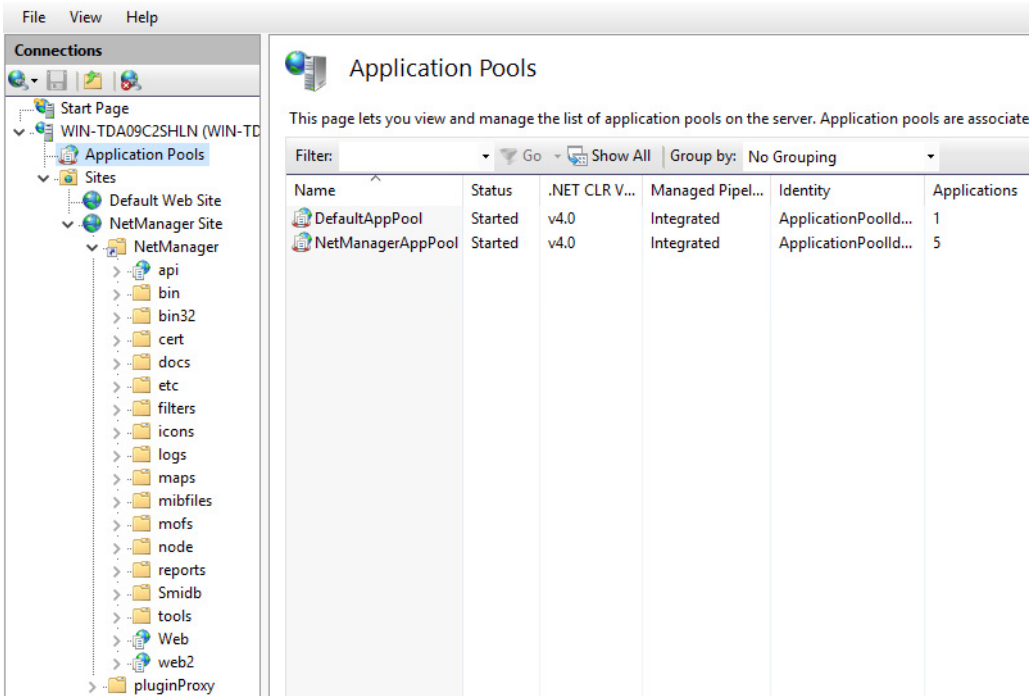


WIN SNMP plugin application pool settings

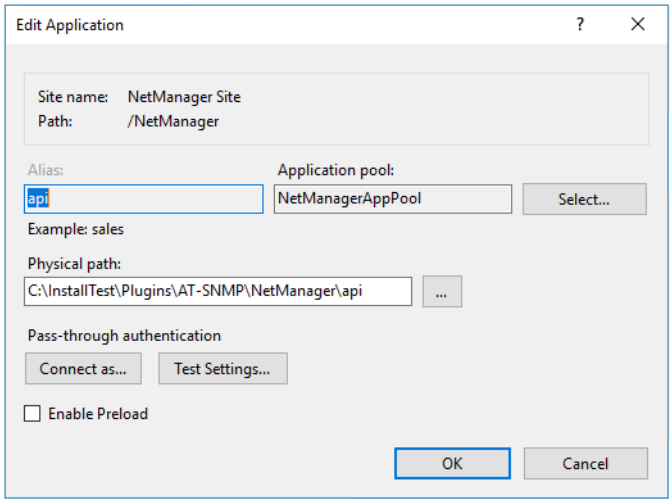
If you are having issues with the SNMP plugin, you can check the IIS settings are correct.

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.

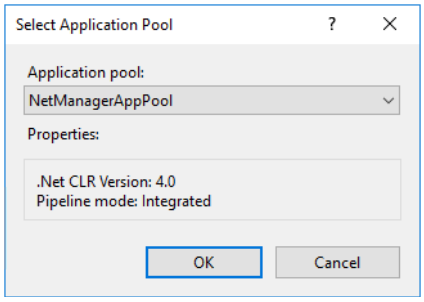


4. Select **api** in the Connections pane and then select Basic Settings in the Actions pane.

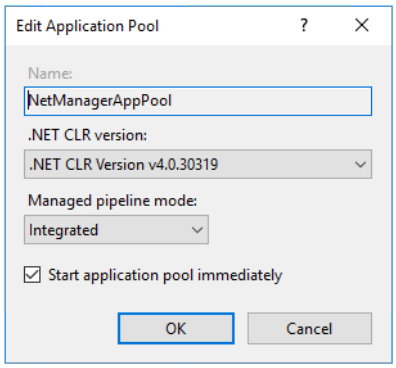


5. Click the select button and check that the Select Application Pool settings have the following properties:

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



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



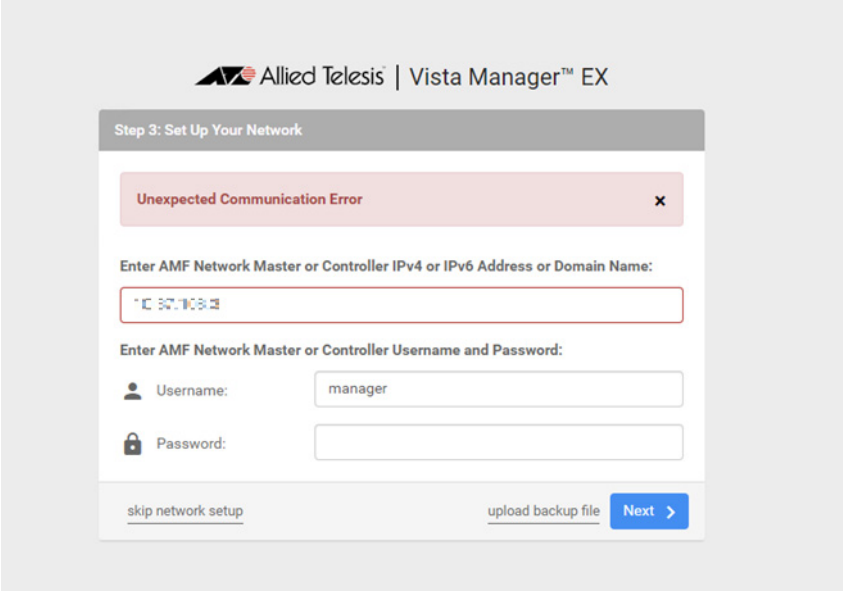
Note: The “xxxxx” portion of the **.Net CLR Version v4.0.xxxxx** version will vary depending on the Windows OS installed.

De-register the AWC plugin on large wireless networks

WIN Individual APs may disappear from the AWC plugin if the plugin is managing a large wireless network (approximately 600 APs or more). If this occurs, de-register the AWC plugin from the Vista Manager’s **System Management -> Plugin Management** page. Features such as licensing, auto-recovery, and importing an AP from a guest device will still work, even if the plugin 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:



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 340.

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:

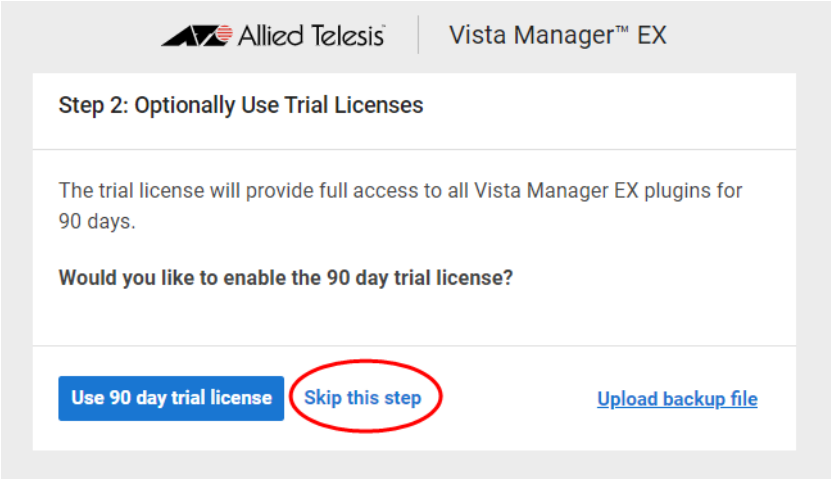
- Network name
- Area name
- Port number
- Model type
- MAC address
- IP address

Information from these log messages are intended to help facilitate easy deployment and replacement of APs.

APL

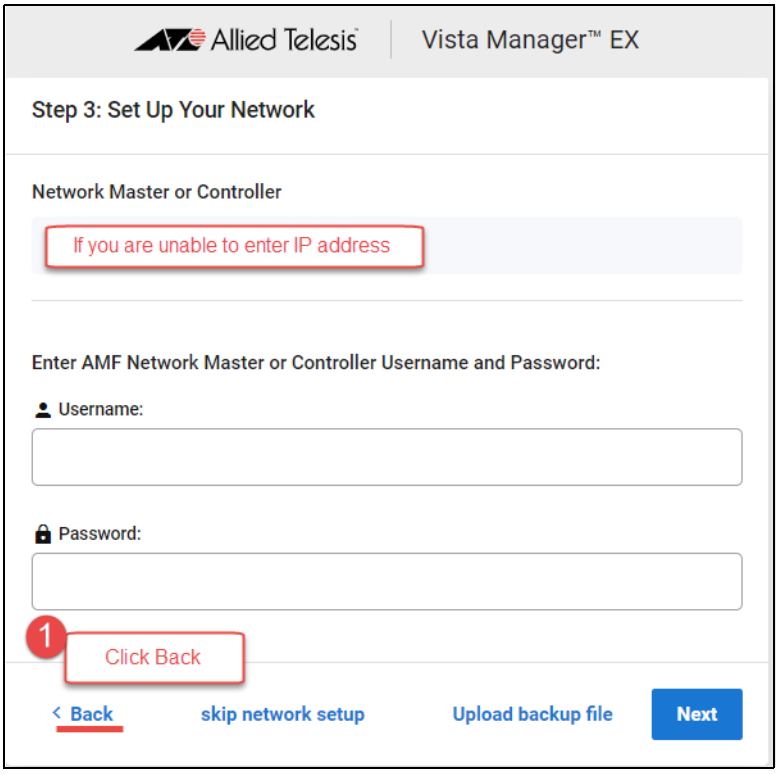
Unable to enter Master/Controller IP address after skipping license page

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.

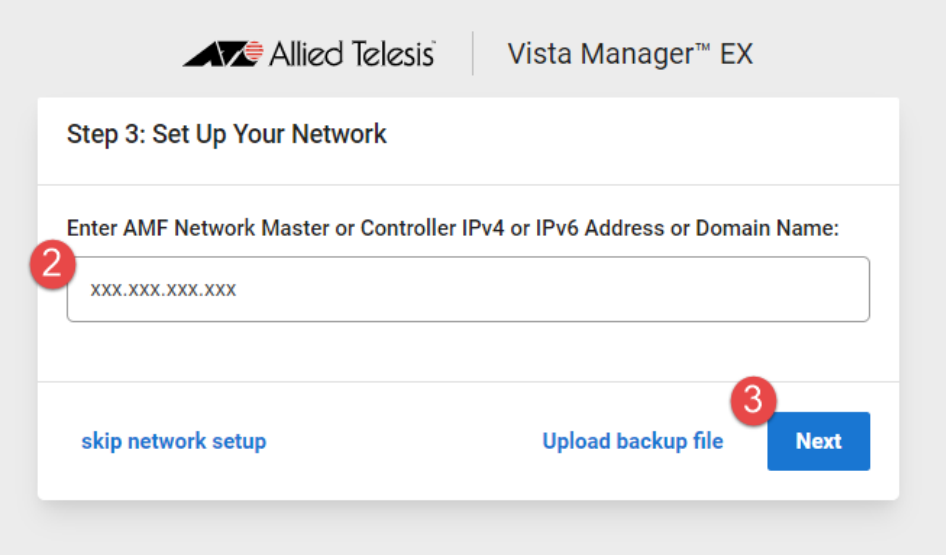


To work-around this issue, perform the following steps:

1. Click **Back**:



2. This takes you to **Set Up Your Network**, and you can then enter the IP address of your AMF Master or Controller...



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 3.15.0 are available. To use all the new features, the devices must run AlliedWare Plus version 5.5.5-1.x or later.

Vista Manager 3.15.0 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 3: Model 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
x540L-28XTm x540L-28XS	x540L
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L
x330-10GTX x330-20GTX x330-28GTX	x330
x320-10GH x320-11GPT	x320
x220-28GS x220-52GT x220-52GP	x220

Table 3: Model names (continued)

Models	Family
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L
x240-10GTXm x240-10GHXm x240-26GHXm	x240
x250-18XS x250-28XS x250-28XTm	x250
IE360-12GTX IE360-12GHX	IE360
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340
IE220-6GHX IE220-10GHX	IE220
IE210L-10GP IE210L-18GP	IE210L
SE240-10GTXm SE240-10GHXm	SE240
SE250-18XTm SE250-28XTm SE250-28XS	SE250
SE540L-28XTm SE540L-28XS	SE540L
SE240-10GTXm SE240-10GHXm	SE240
XS916MXT XS916MXS	XS900MX
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX
GS980EM/10H GS980EM/11PT	GS980EM
GS980M/52 GS980M/52PS	GS980M
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
ARX200S-GTX	AR-Series UTM firewalls

Table 3: Model names (continued)

Models	Family
10GbE UTM Firewall	
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls
AR1050V	AR-series VPN routers
TQ6702 GEN2-R TQ7403-R	Wireless AP Router

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.

C613-04199-00 REV A

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