Technical Guide

Getting Started with the Device GUI on Switches

Feature Overview and Configuration Guide

Introduction

The Allied Telesis Device GUI is used on switches, firewalls, and routers running the AlliedWare Plus™ operating system. The Graphical User Interface (GUI) allows you to easily monitor and manage your device, and includes access to the Command Line Interface (CLI) when more complex configuration is required.

What information will you find in this document?

This guide describes how to use the GUI to manage an Allied Telesis switch.

Topics include:

- Connecting to the Device GUI
- Finding your way around the Dashboard
- Understanding the menu features

What does the Device GUI do?

The Device GUI allows you to:

- Observe and monitor ports and traffic throughput
- Manage interfaces, VLANs, ACLs, logs, and files
- Use the in-built DHCP server and network testing tools
- Manage and update feature licenses
- Access the complete AlliedWare Plus feature-set via the industry-standard CLI
- On some switches, use Vista Manager mini. Vista Manager mini enables you to control wireless APs and monitor devices attached to the switch.

For guides to using the Device GUI on other platforms, see "Related documents" on page 3

Contents

Products and software version that apply to this guide

This guide applies to switches running AlliedWare Plus software version **5.4.8-0.2** or later.

Feature support may change in later software versions. For the latest information, see the following documents:

- The product's Datasheet
- The AlliedWare Plus Datasheet
- The product's Command Reference

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

Related documents

To configure an Allied Telesis UTM firewall or VPN router using the Device GUI, see the following guides:

- Getting Started with the Device GUI on UTM Firewalls
- Getting Started with the Device GUI on VPN Routers

For detailed documentation on wireless configuration, see:

- User Guide: Wireless Management (AWC) with Vista Manager mini.

Accessing the Device GUI

This section describes how to connect your switch to the Device GUI. Your switch will have a GUI already loaded. If your switch has an older GUI version, you can update it using the steps outlined below.

Your switch must be running AlliedWare Plus software version **5.4.8-0.2** or later.

Supported web browsers for connecting to the Device GUI are:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge™
- Apple Safari™

Browse to the GUI

Perform the following steps to browse to the GUI.

1. If you haven't already, add an IP address to an interface. For example:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 192.168.1.1/24
```

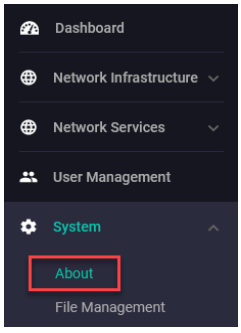
   Alternatively, on unconfigured devices you can use the default address, which is 169.254.42.42.

2. Open a web browser and browse to the IP address from step 1.

3. The GUI starts up and displays a login screen. Log in with your username and password. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the System > About page in the GUI and check the field called **GUI version**.



To see if a more recent GUI is available, check the Software Download center.

Update the GUI

Perform the following steps through the Device GUI and command-line interface if you have been running an earlier version of the GUI and need to update it.

1. Obtain the latest GUI file from our Software Download center. For example, the filename for v2.12.0 on AlliedWare Plus version 5.5.2-1.x is awplus-gui_552_27.gui.

   Make sure that the version string in the filename (e.g. 552) matches the version of AlliedWare Plus running on the switch. The file is not device-specific; the same file works on all devices.

2. Log into the GUI:

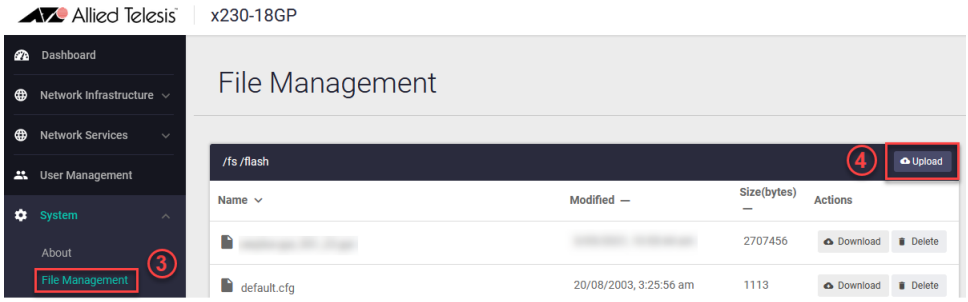
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   The GUI starts up and displays a login screen. Log in with your username and password.

   The default username is *manager* and the default password is *friend*.

3. Go to **System** > **File Management**

4. Click **Upload**.



5. Locate and select the GUI file you downloaded from our Software Download center. The new GUI file is added to the **File Management** window.

   You can delete older GUI files, but you do not have to.

6. Reboot the switch. Or alternatively, use a Serial console connection or SSH to access the CLI, then use the following commands to stop and restart the HTTP service:

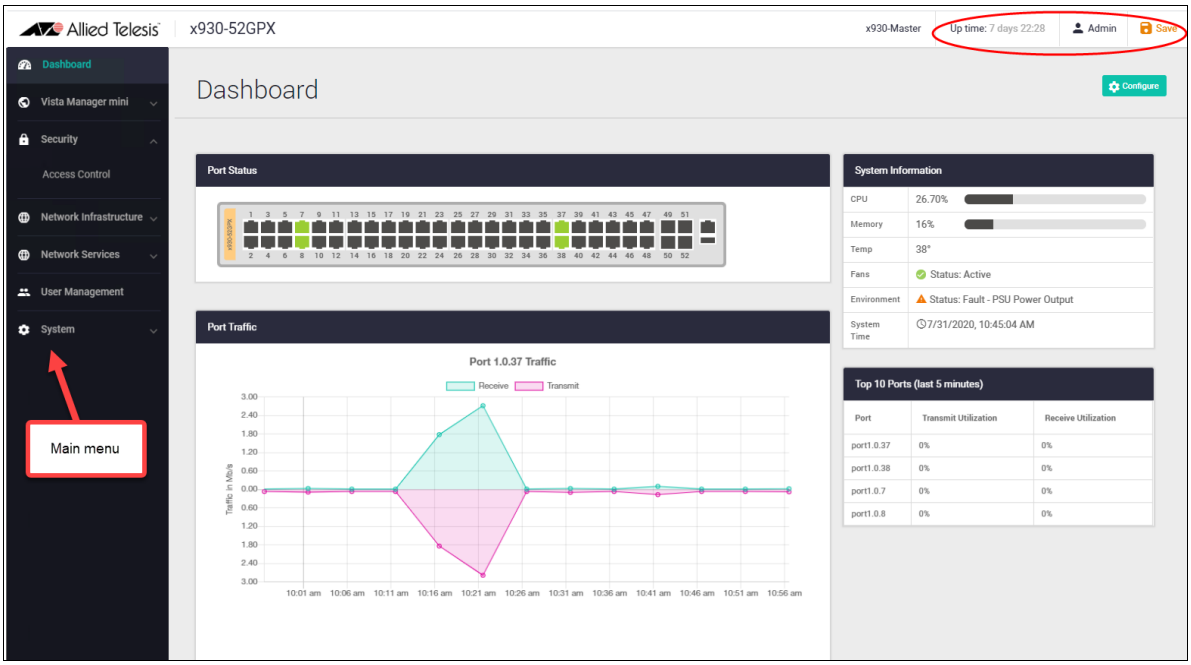
```
awplus> enable
awplus# configure terminal
awplus(config)# no service http
awplus(config)# service http
```

   To confirm that the correct file is now in use, use the commands:

```
awplus(config)# exit
awplus# show http
```

The Dashboard

Log in and you'll see the Device GUI dashboard. The dashboard provides useful information for monitoring the status and health of your switch, as well as port connectivity and traffic information.

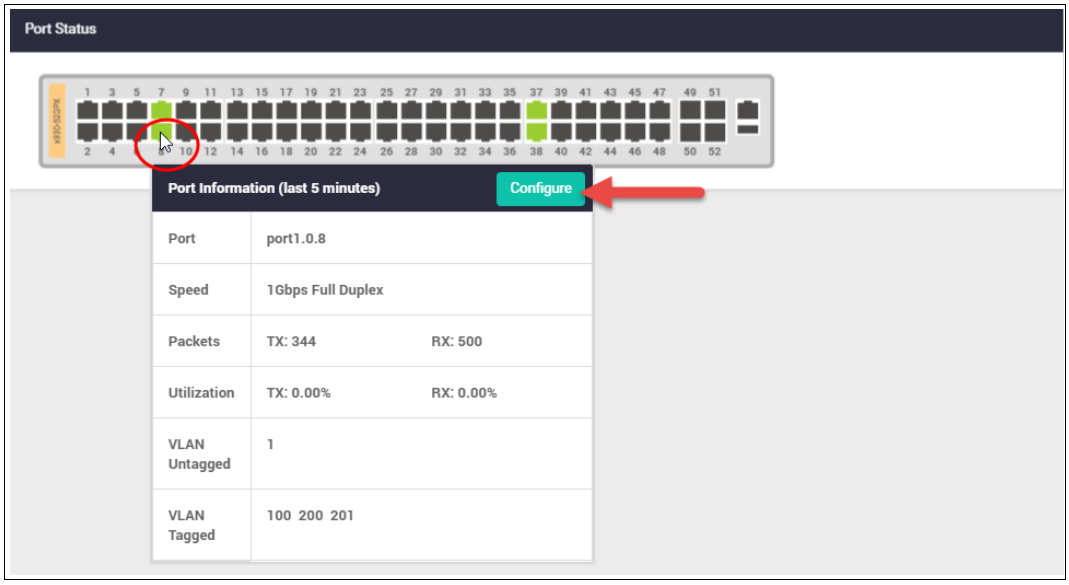


At the top right of the screen you can see the **Uptime** for the switch, as well as the **Admin** button which is used to log out. There is also a **Save** button, which will be colored orange any time there is unsaved configuration, or black if the configuration has been saved.

The main menus: **Vista Manager mini**, **Security**, **Network Infrastructure**, **Network Services**, **User Management** and **System** are located on the left of the dashboard. You can collapse or expand these menus to access the sub-menus.

The dashboard contains widgets, which are components of the interface that enable you to perform a function or access a service.

Port Status widget

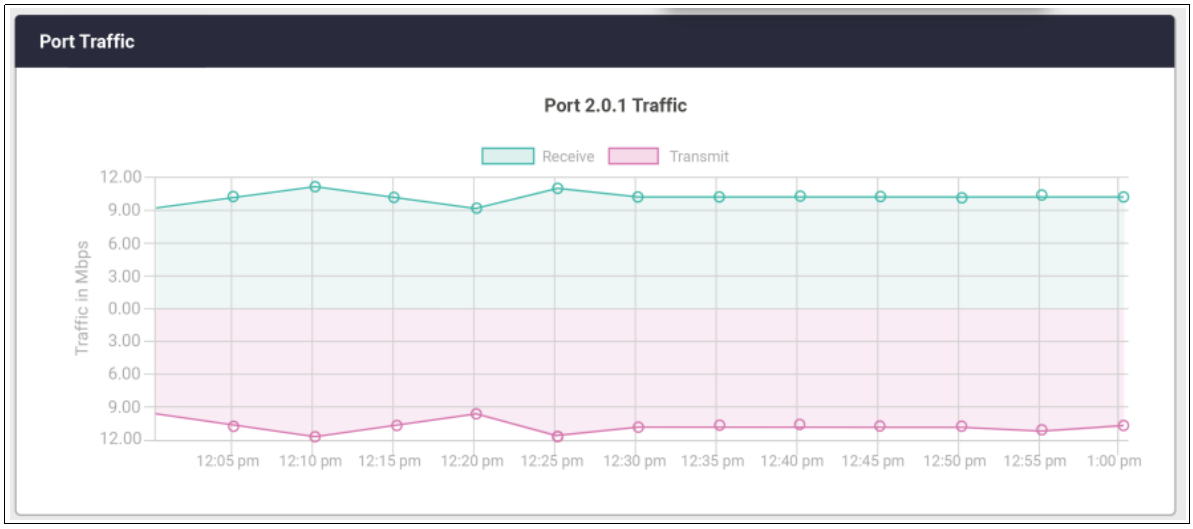


The Port Status widget displays the front panel ports of the switch, or switches if you are connected to a VCStack, with the specific model shown on each switch.

Any ports that are currently ‘up’ are shown in green. Hovering your mouse over any port that is ‘up’ displays the Port Information window, with statistics over the last 5 minutes. The window lists the port’s number, speed, packet transmit and receive counts, utilization percentages and VLAN associations.

Click on the **Configure** button to enable or disable the port. From here you can also configure the port’s speed, duplex mode, polarity, and aggregator status.

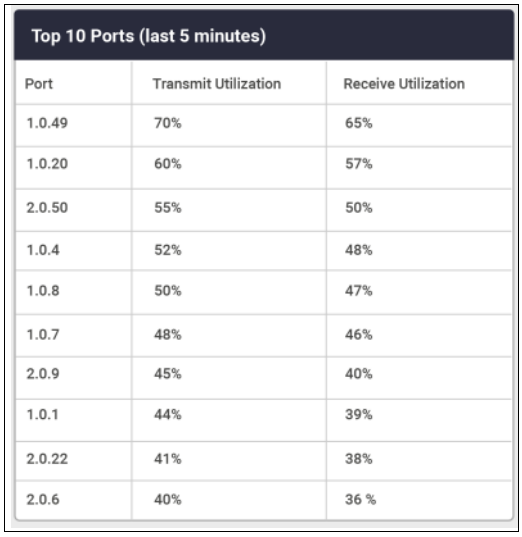
Port Traffic widget



The Port Traffic widget displays traffic sent and received on a selected port over the last hour. This is useful for analyzing traffic patterns.

By default, the Port Traffic widget displays the traffic from the highest utilized port, as shown in the Top 10 Ports widget. Clicking on any other port in the Port Status widget will display traffic for that port.

Top 10 Ports widget

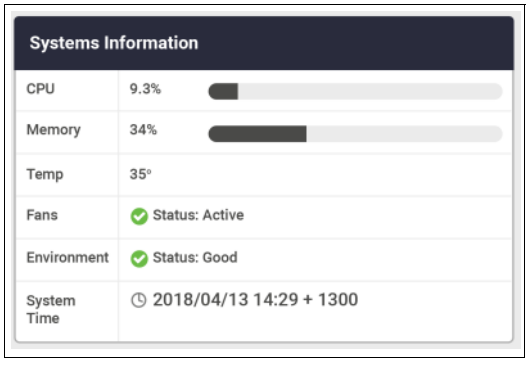


Top 10 Ports (last 5 minutes)

Port	Transmit Utilization	Receive Utilization
1.0.49	70%	65%
1.0.20	60%	57%
2.0.50	55%	50%
1.0.4	52%	48%
1.0.8	50%	47%
1.0.7	48%	46%
2.0.9	45%	40%
1.0.1	44%	39%
2.0.22	41%	38%
2.0.6	40%	36 %

The Top 10 Ports widget displays the top 10 utilized ports on the switch (or stack of switches), over the last 5 minutes. The widget is dynamic, and so ports will change position, and/or drop in and out of the top 10 ports list as utilization across the switch changes. By default, the last hours traffic from the top utilized port is shown in the Port Traffic widget.

System Information widget



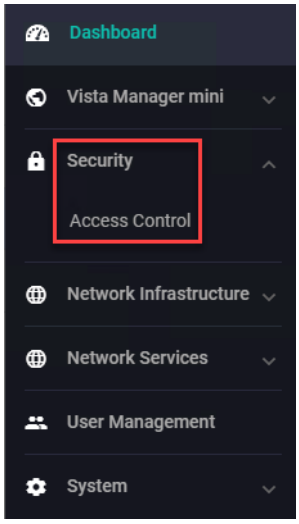
Systems Information

CPU	9.3%
Memory	34%
Temp	35°
Fans	Status: Active
Environment	Status: Good
System Time	2018/04/13 14:29 + 1300

The System Information widget displays the current CPU and memory usage, as well as temperature, fan and environmental status, and system time.

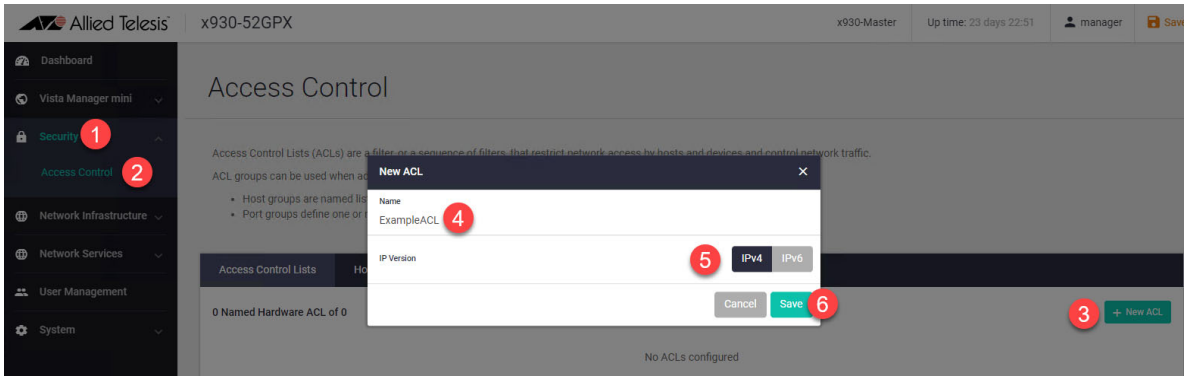
Security menu

From 2.12.0 onwards, the Device GUI makes it easy to configure Access Control Lists (ACLs), through the Security menu. ACLs let you filter traffic, so you can block or allow traffic that meets particular criteria.



Creating an ACL:

1. Open the Security menu.
2. Select **Access Control** in the menu.
3. Click **+ New ACL**.
4. Give the ACL a name.
5. Select whether the ACL will filter IPv4 or IPv6 traffic.
6. Click **Save**.:



7. The new ACL will be listed on the Access Control page. If you want to create a host group for IP addresses, click **Host Groups**. Click either **+ IPv4 Group** or **+ IPv6 Group** to create a new host group. Give your group a name. Then expand the **Entries** field, click **+ New IP Address** and create the desired address entries.

8. If you want to create a port group for TCP or UDP ports, click **Port Groups**. Click **+ New Port Group** to create a new group. Give your group a name. Then expand the **Entries** field, click **New Port Selection** and create the desired port entries.

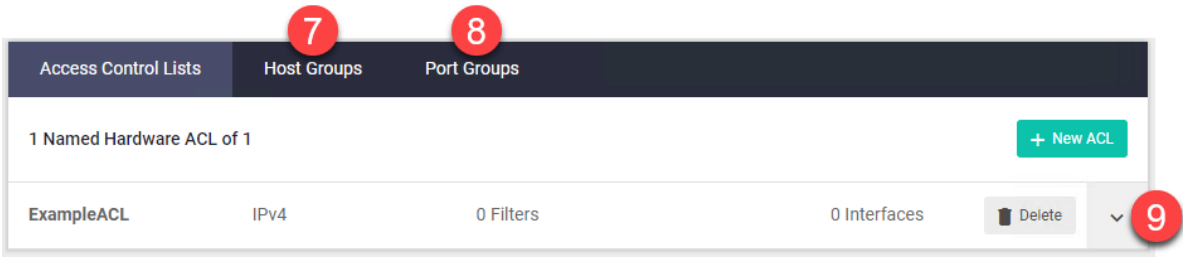
   Host and port groups are useful for the following reasons:

   - They let filters match on multiple addresses or port matching criteria. For example, you can use a port group to match all ports greater than a given port number. You can use a mix of criteria in one group, like this:

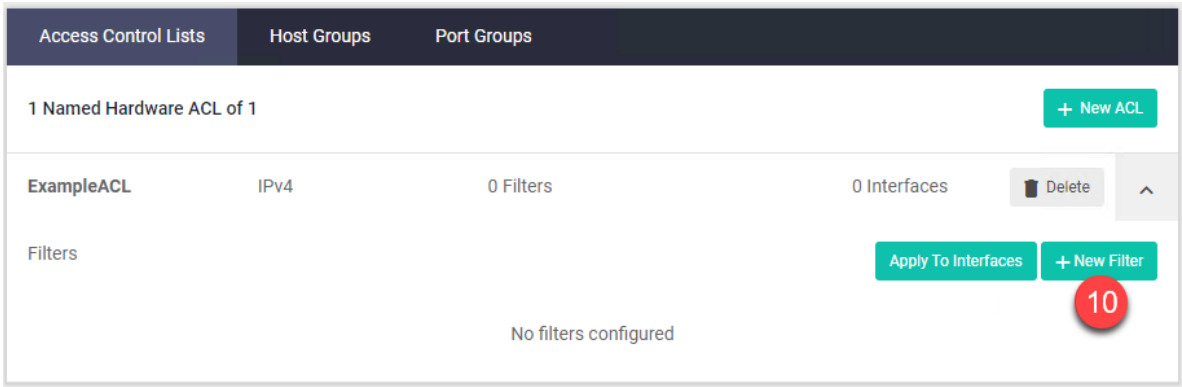
Name	Port Range				
ExampleCombinedCriteria	equal 500	greater than 1000	less than 2000	not equal 1500	3000 to 4000

   - They let you name the grouped addresses or port numbers. This makes it easy to see what each filter does. For example, you can create a host group for each team in your company.
   - If you use the same addresses or port numbers in multiple filters, and those addresses or port numbers change, then you only have to edit the group instead of each filter.

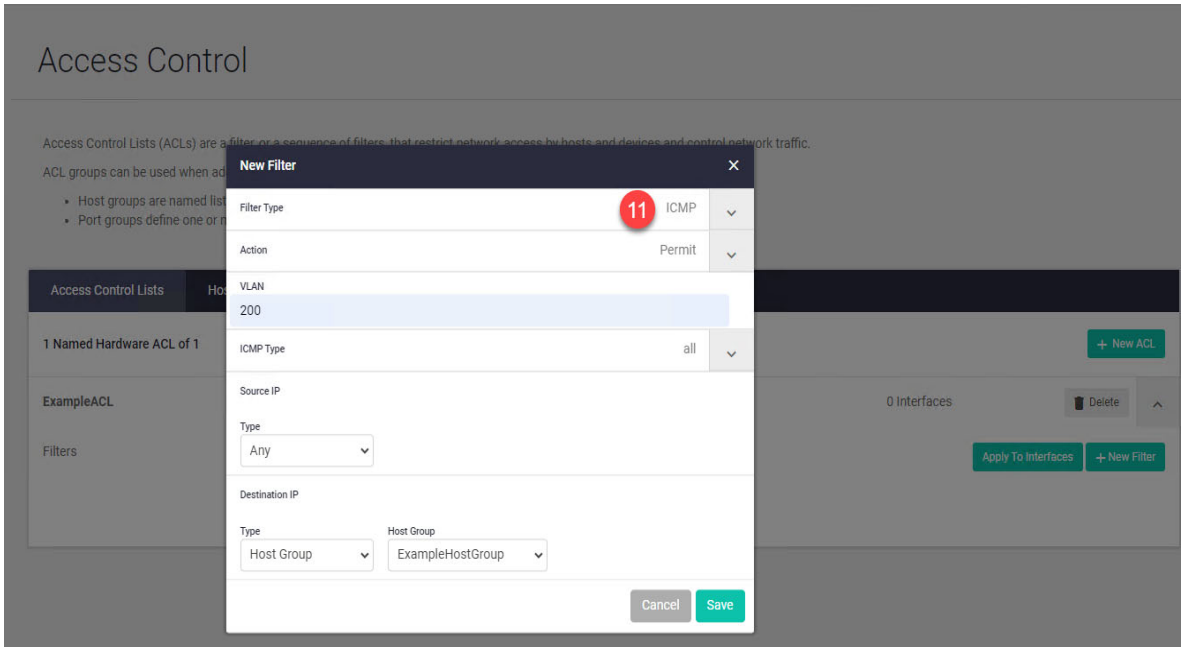
9. Return to the Access Control lists tab and select the down-arrow button at the end of your ACL's row to edit it.



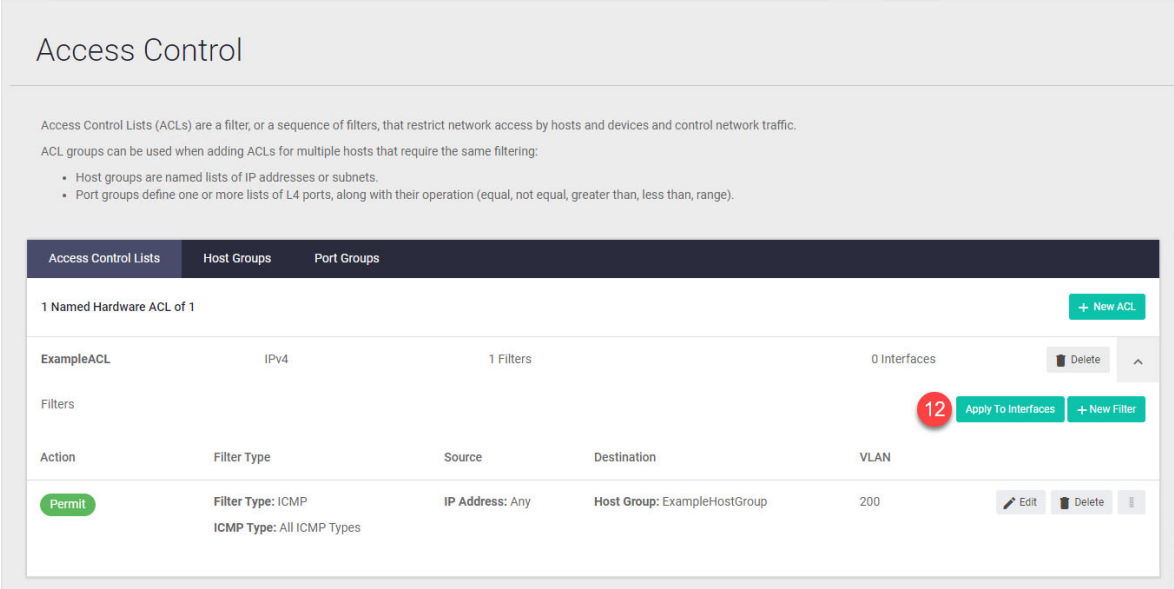
10. Click **+New Filter** to add a filter entry to the ACL.



11. Select the type of filter you want, fill out the rest of the fields, and click **Save**. Different fields are available for different filter types. If you created host groups or port groups, you can select them here.

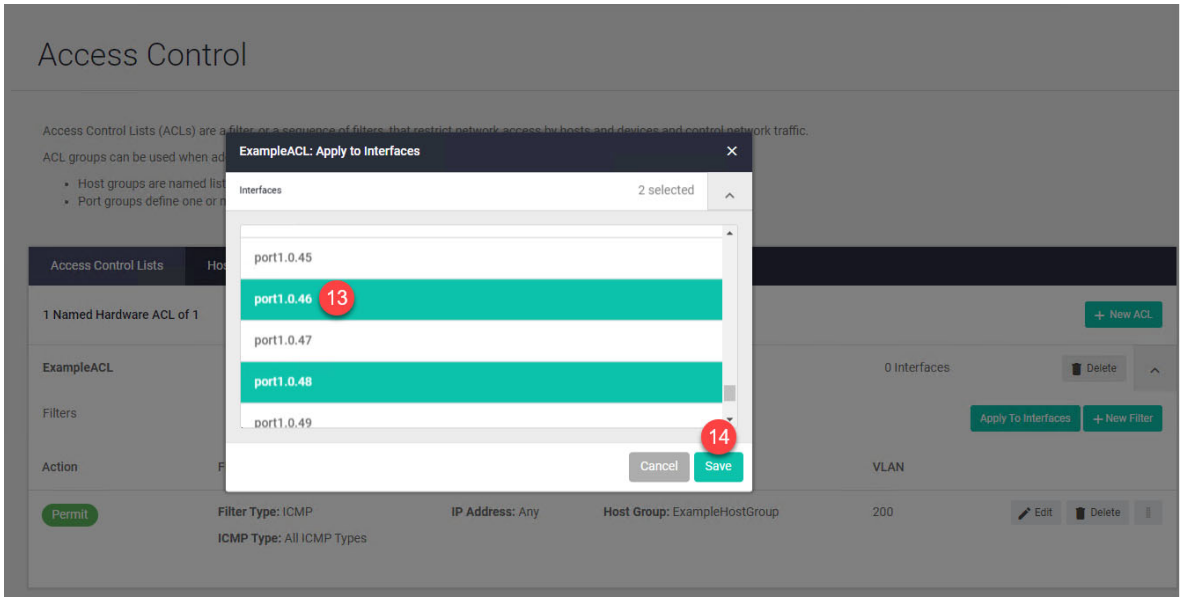


12. Your filter will now display on the Access Control Lists page. Add more filters to the ACL as needed. Once you have finished, click **Apply To Interfaces** to choose which switch ports to apply the ACL to.



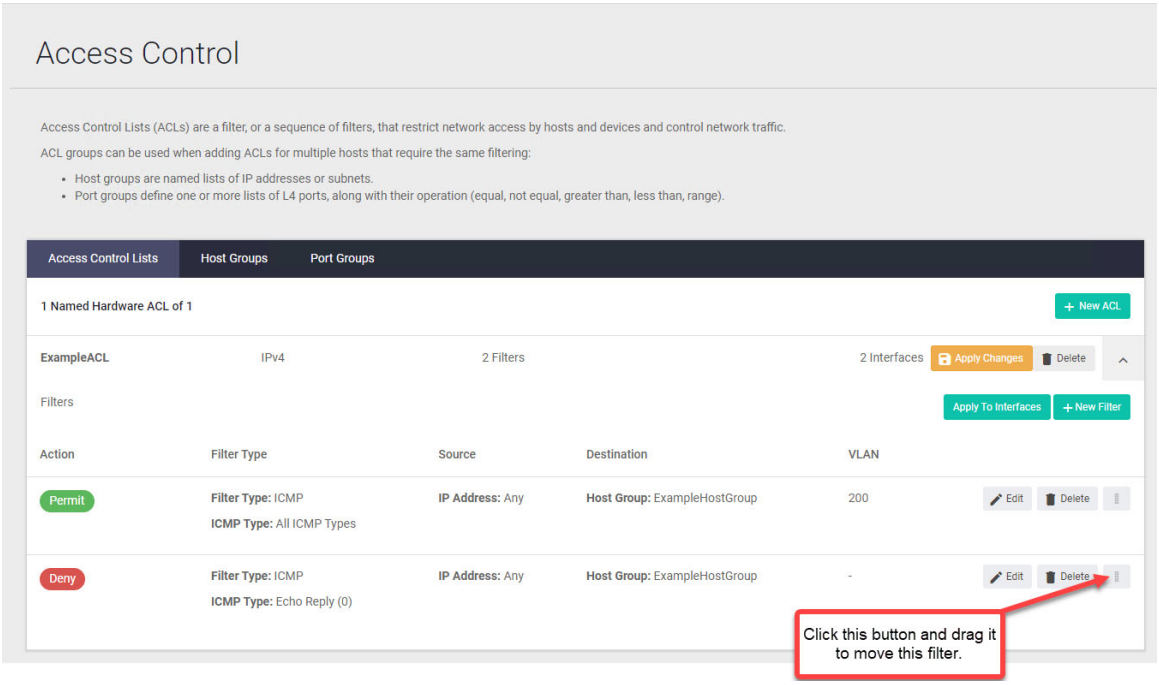
13. Click on the desired ports to select them. The GUI lets you apply ACLs to switch ports and link aggregation groups. If you want to apply the ACL to VLANs, use the CLI to create a VLAN access map and add ACLs to it. For more information, see the **vlan access-map** command in your switch's Command Reference.

14. Once you have finished, click **Save**.

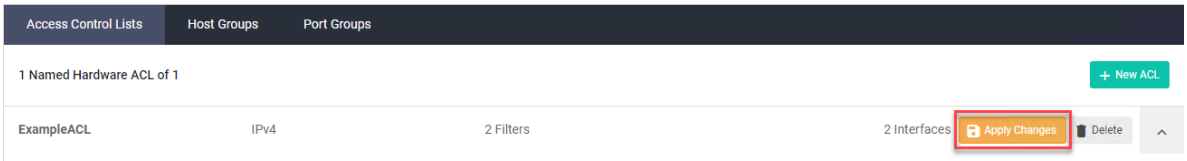


Re-ordering filters in an ACL:

The GUI makes it easy to re-order filters within an ACL. Simply click on the move button at the end of a filter's row and drag it up or down to the desired position.

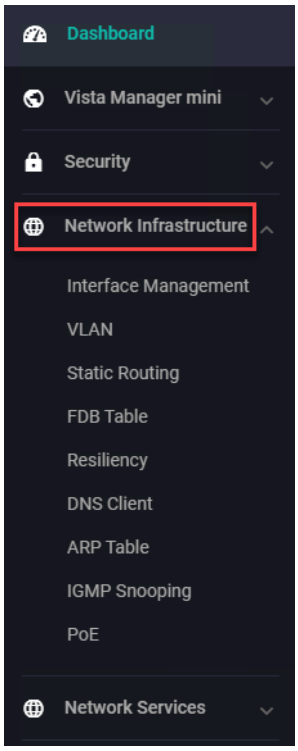


If the ACL has already been assigned to interfaces, you also need to apply the changes. To do this, click on the Apply Changes button.



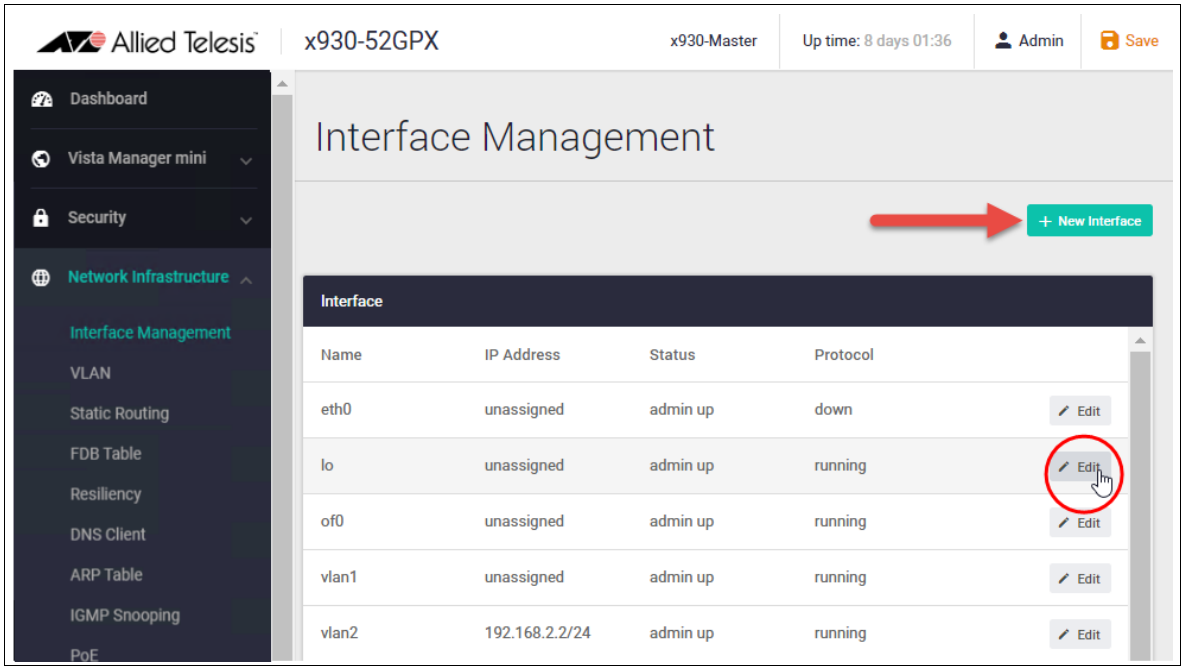
Network Infrastructure menu

The Network Infrastructure menu provides access to: Interface Management, VLAN, Static Routing, FDB Table, Resiliency, DNS Client, ARP Table, IGMP Snooping, and PoE sub menus.



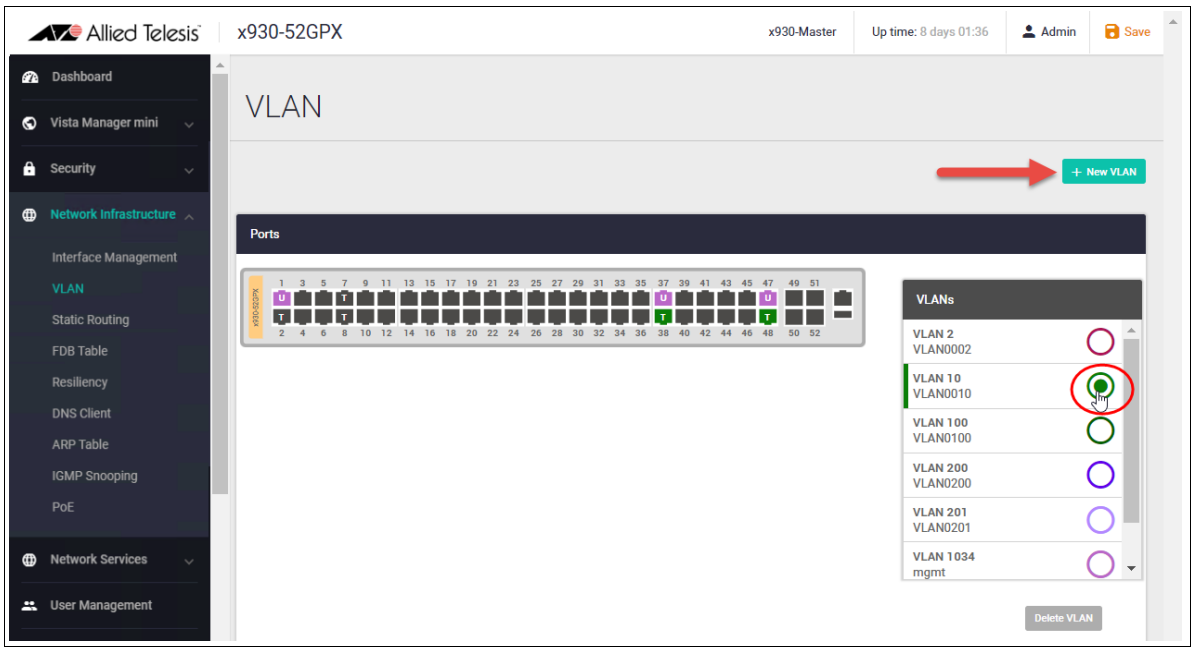
Let's look at the Network Infrastructure sub menus:

Interface Management



The Interface Management page shows the interfaces currently configured on the switch and their IP address, status, and protocol details. From here you can add a new interface and/or edit an existing one.

VLAN



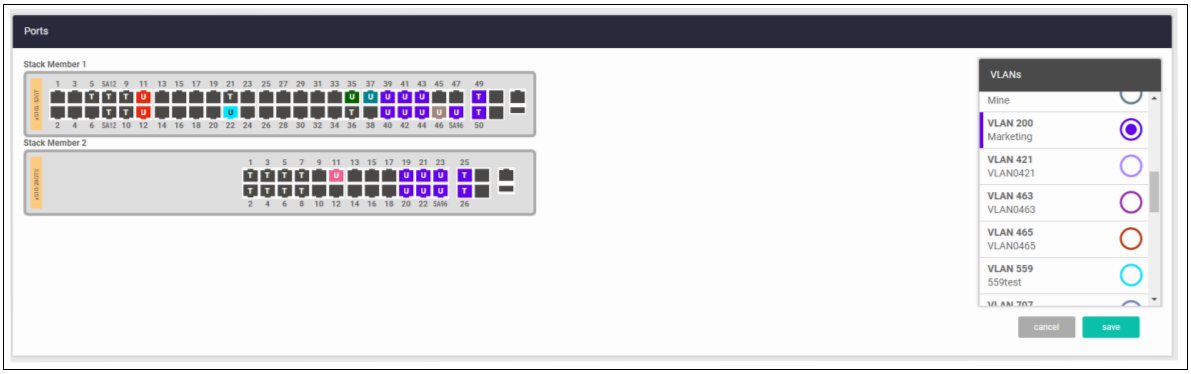
The VLAN page shows the VLANs currently configured on the switch. From here, you can easily create, edit, and delete VLANs.

Creating a VLAN:

- Click the **+New VLAN** button and type in a **VLAN ID** and **VLAN Name**.
- Click **Save**.

New VLANs are added to the VLAN list on the right side of the window. Each VLAN has a different colored circle assigned to it. When a VLAN is selected in the list, the ports that belong to that VLAN are displayed in the switch image using the color assigned to that VLAN.

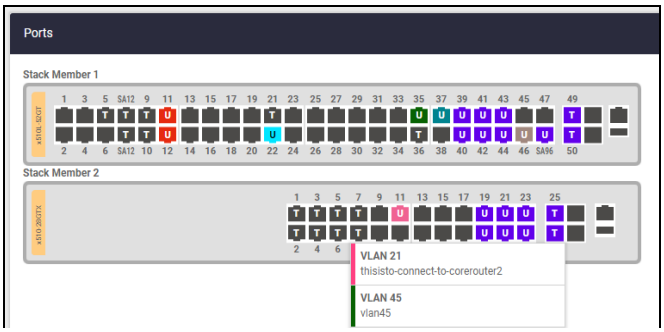
In the example below, VLAN 200 is selected, and it has the color purple assigned to it. When VLAN 200 is selected, all the ports that belong to VLAN 200 are also colored purple in the device images.



Adding ports to a VLAN:

- Select the VLAN.
- Click on switch ports to add them as tagged or untagged. A triple-click system (untagged, tagged, unselected) makes port management simple.
- The same method is used to edit any current VLAN and its port members

Tip: Hover over any port to see its VLAN membership. Any ports that are tagged members of multiple VLANs will be shown as dark gray.



Configuring native VLANs:

From Device GUI version 2.11.0 onwards, you can use the VLAN map to assign native VLANs to switchports.

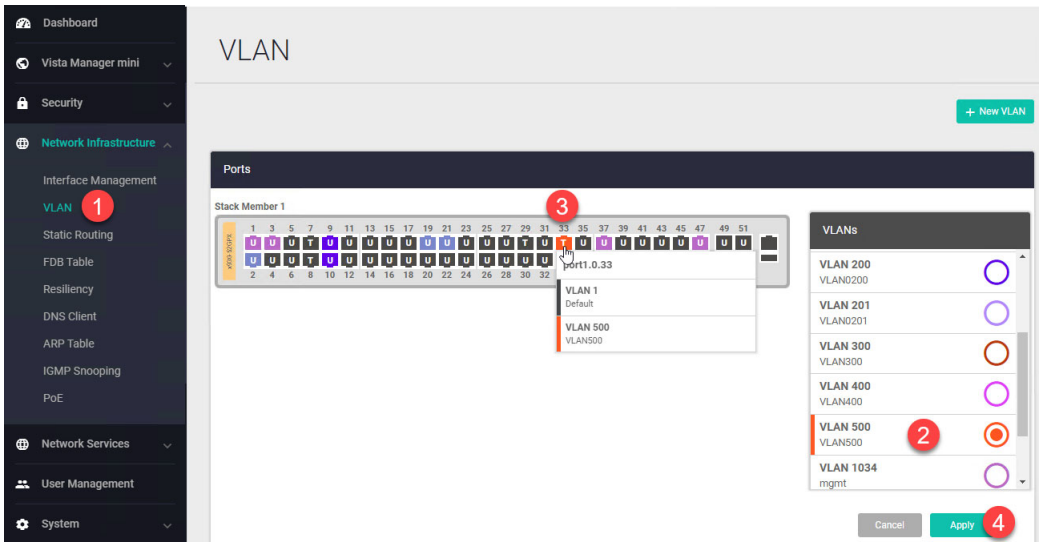
Once a port has a native VLAN, any packets received on the switchport without a VLAN tag are placed into the native VLAN. Packets leaving a switchport on the native VLAN will not be tagged.

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

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

1. Select **Network Infrastructure** > **VLAN** to open the **VLAN** page.
2. If the VLAN you want to add as a native VLAN doesn't exist, click **New VLAN** to create it. Otherwise, select the VLAN in the VLANs list.
3. Click on the **U** on the switchport until it takes on the color of your selected VLAN and changes to a **T** (for Trunk).

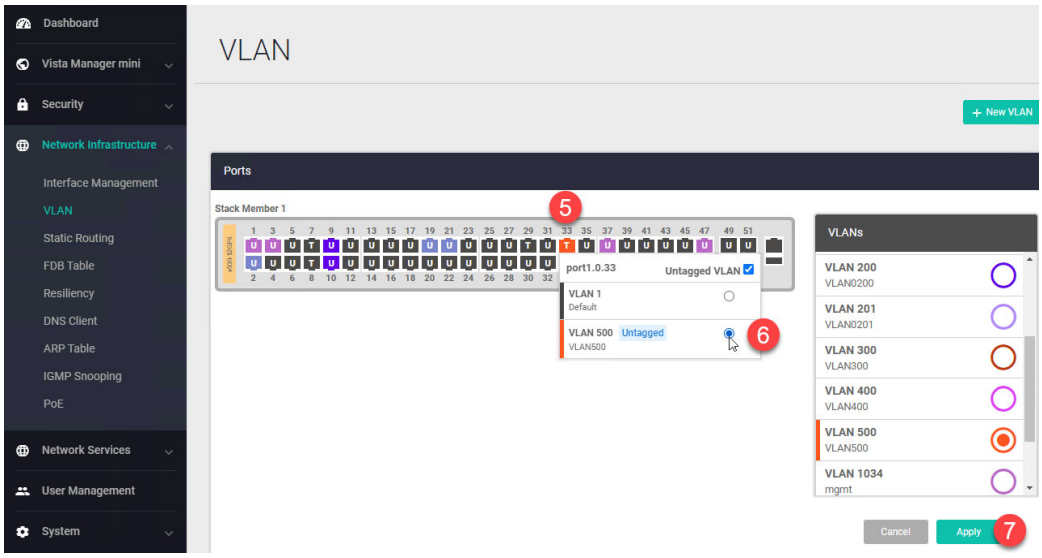
4. Click **Apply** to set the port mode to Trunk.



5. Hover over the switchport. A pop-up will appear, showing the current native VLAN (probably VLAN1) and the VLAN you want to add as native VLAN.

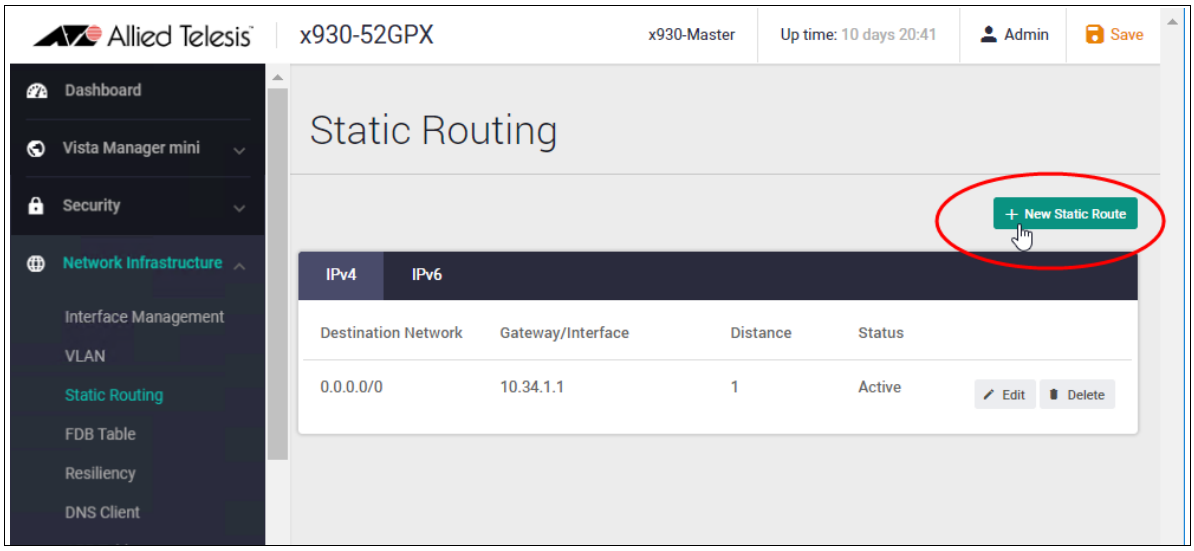
6. In the pop-up, select the VLAN that you want to make the native VLAN.

7. Click **Apply** again.



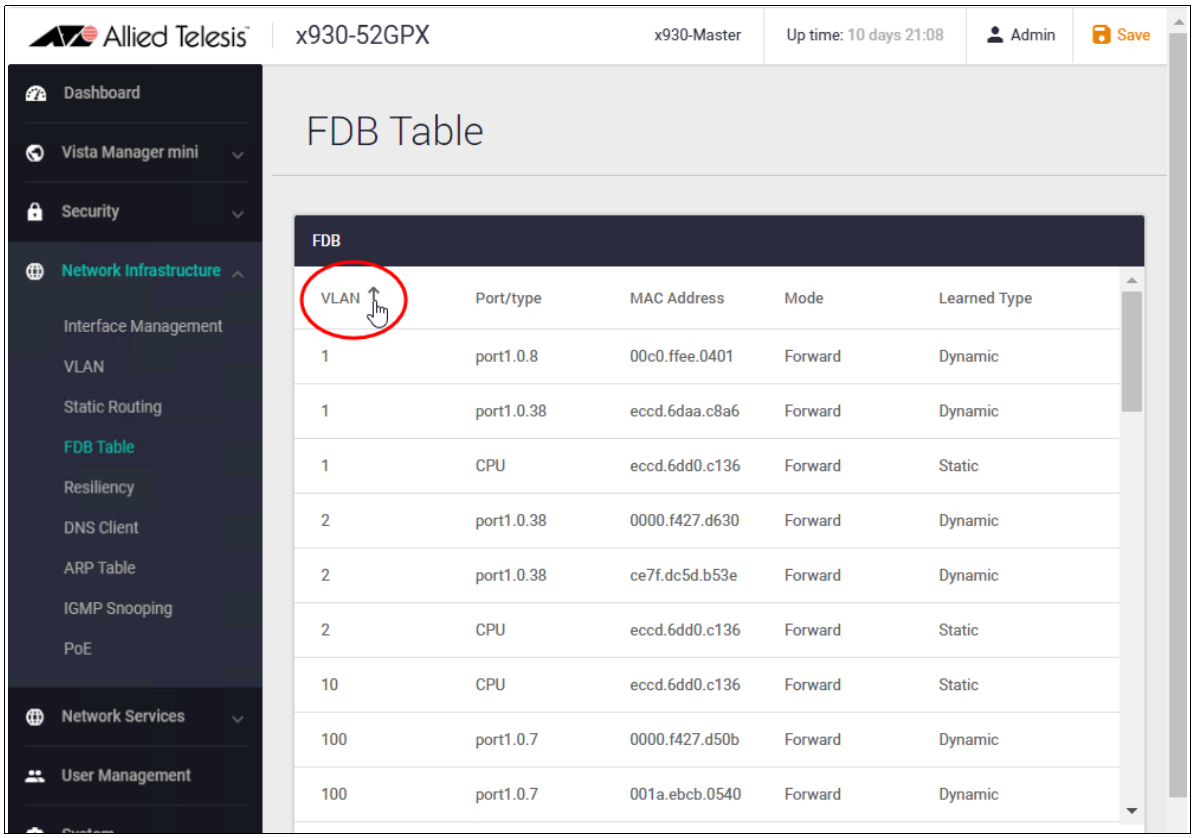
Static Routing

The Static Routing page displays the static routes currently configured on the switch. From here you can add, edit, and delete static IPv4 and IPv6 routes.



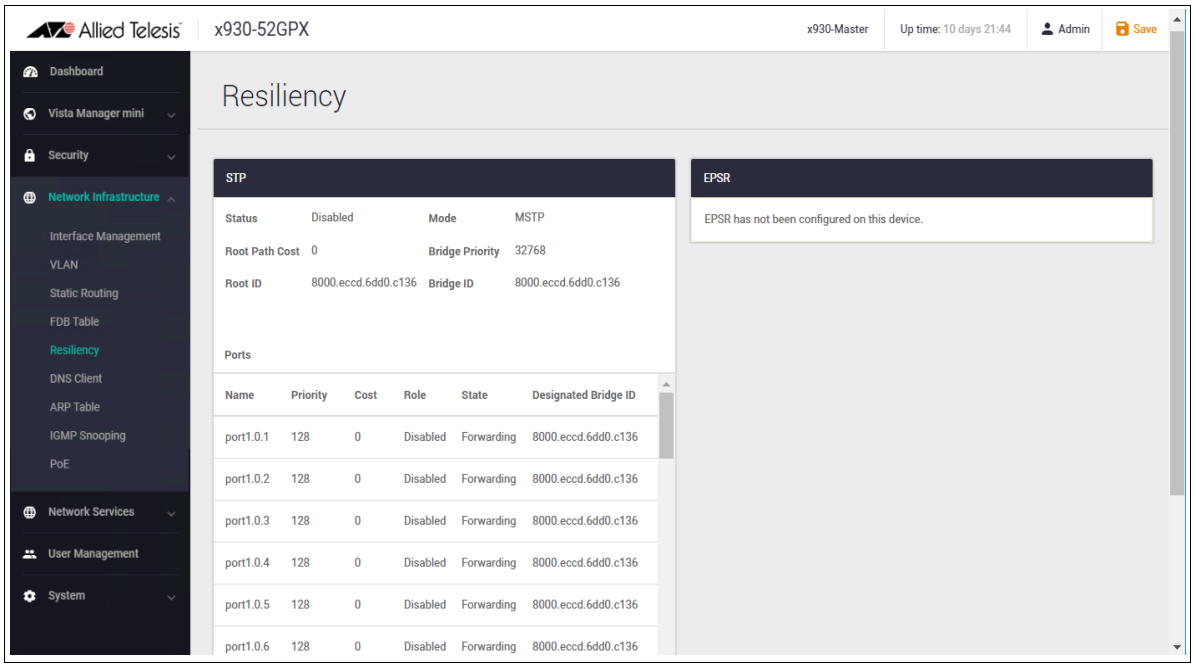
FDB Table

The FDB (forwarding database) table is used to store the MAC addresses that have been learned and which ports that MAC address was learned on. Hover your mouse over a column header to access the up or down arrow. Then, click on the header to change the sort criteria to either ascending or descending.



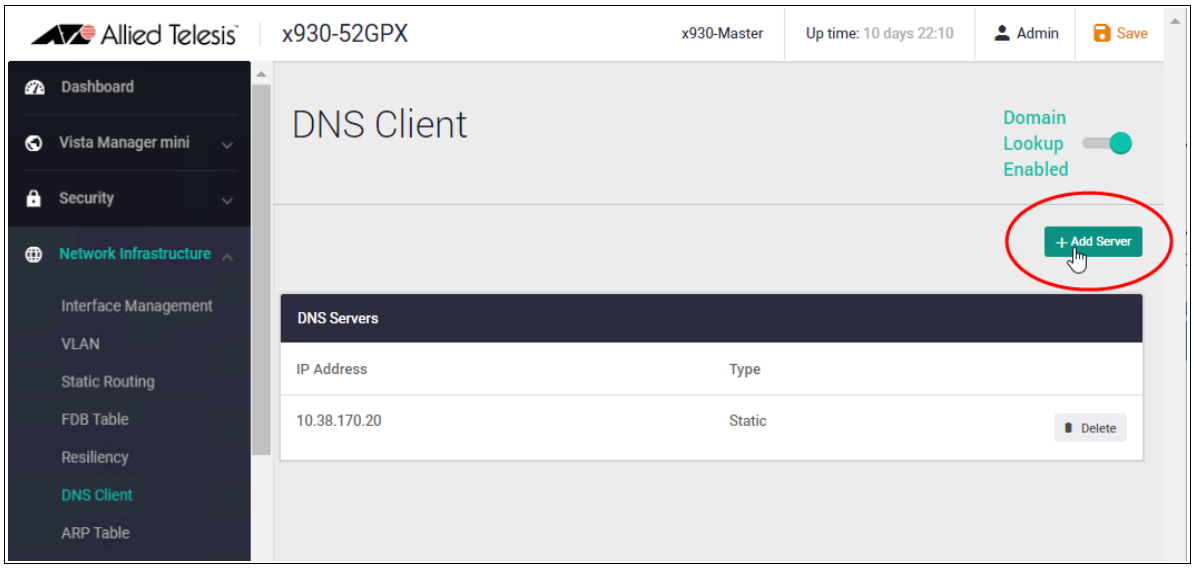
Resiliency

The Resiliency page displays the STP, RSTP, MSTP, and EPSR settings currently configured on the device.



DNS Client

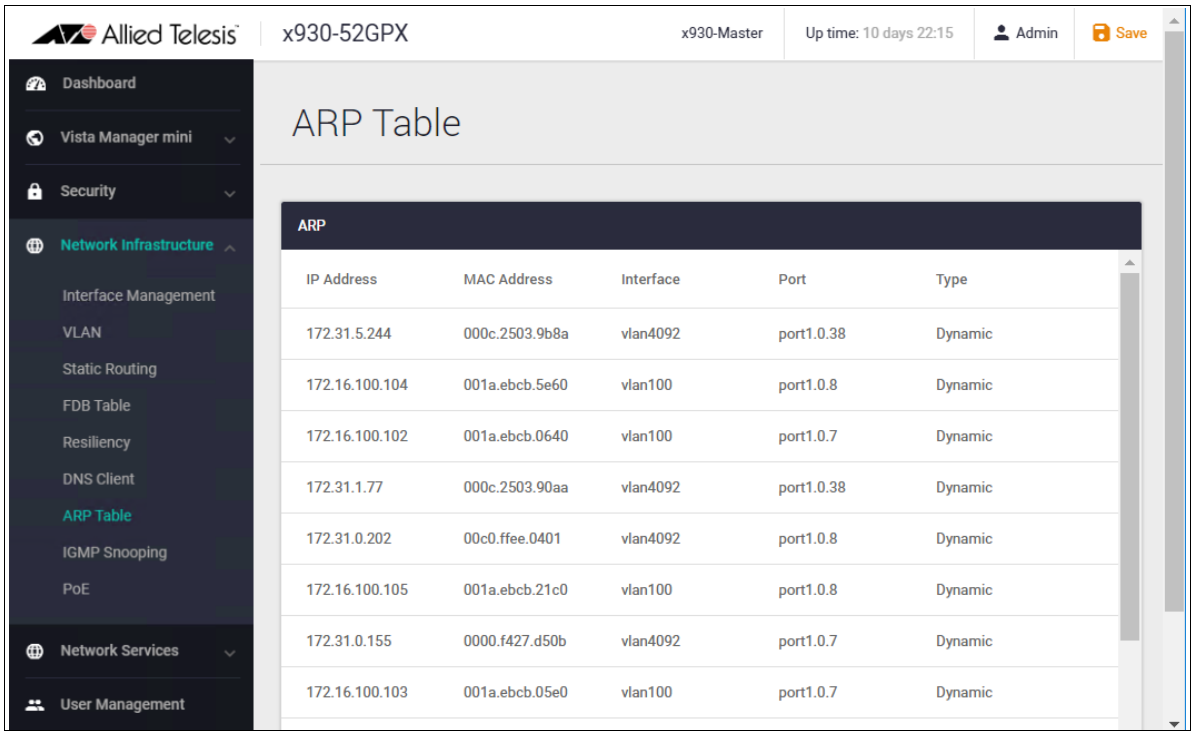
The DNS Client page displays the DNS servers currently configured on the device. You can also add new DNS servers from this page.



ARP Table

Devices look up the ARP (Address Resolution Protocol) table to determine the destination for traffic with a given IP address. The ARP table stores the MAC address, port, and VLAN for each IP address.

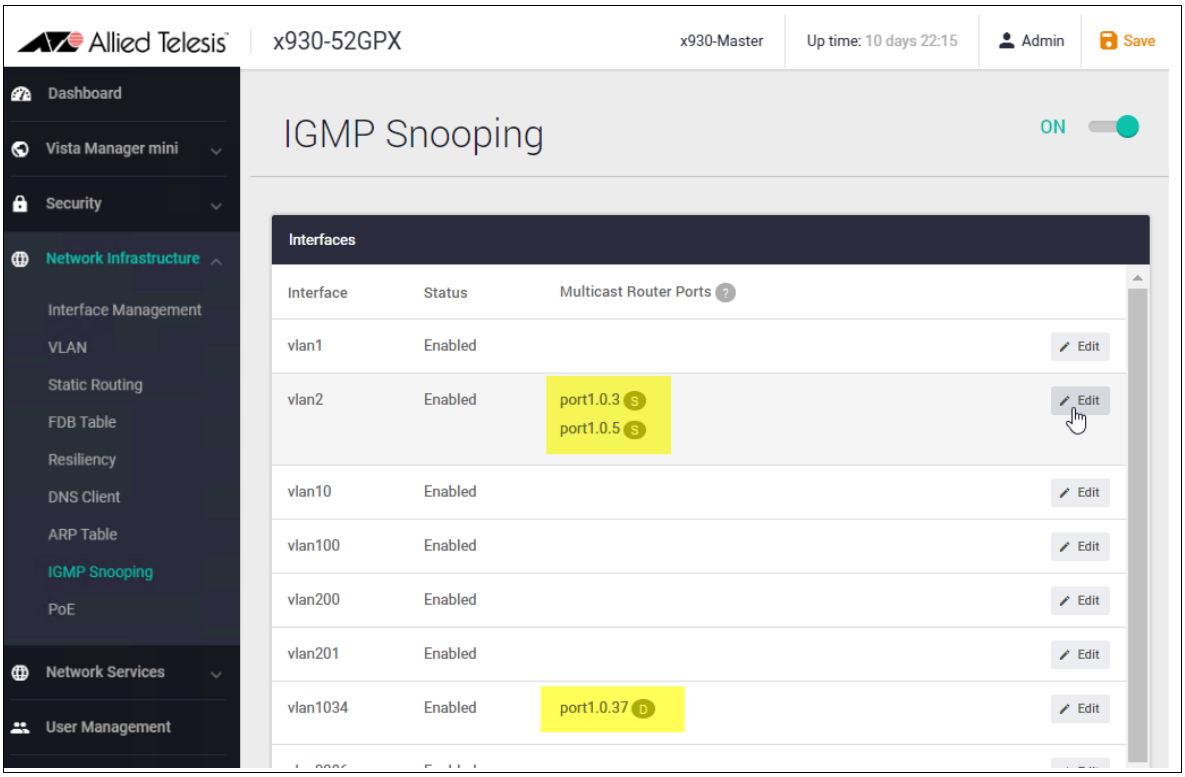
Hover your mouse over a column header to access the up or down arrow. Then, click on the header to change the sort criteria to either ascending or descending.



IGMP Snooping

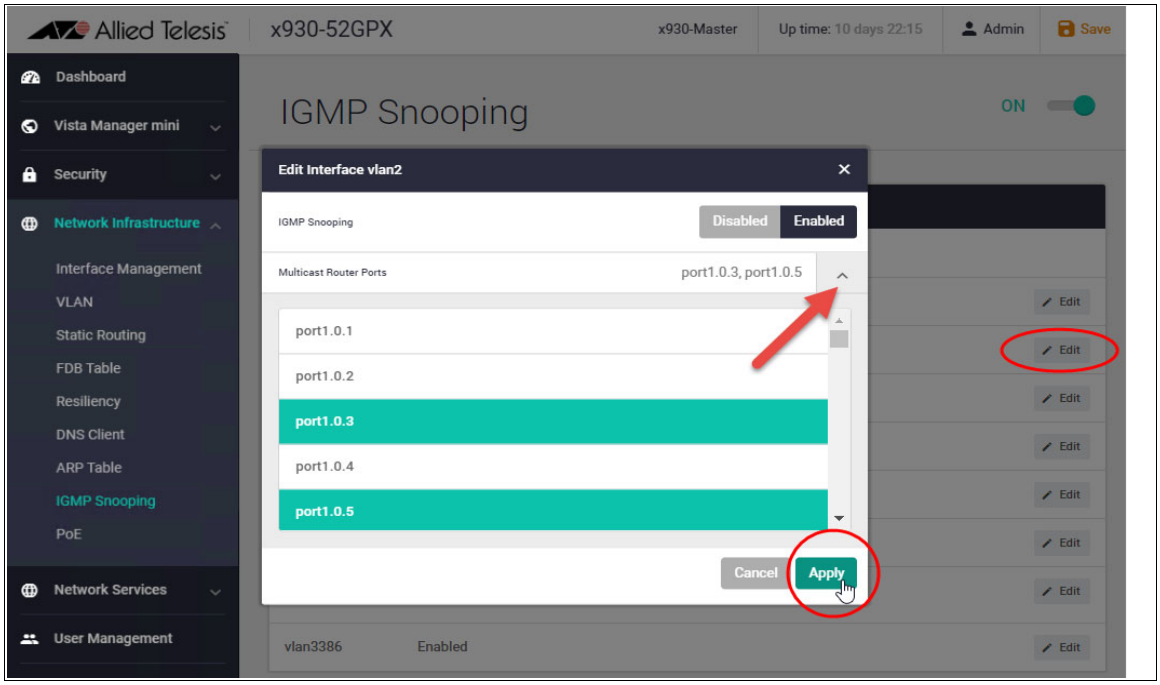
You can statically configure an interface as an IGMP snooping multicast-router interface—that is, an interface that faces toward a multicast router or other IGMP querier. The interface may be a device port (e.g. port1.0.2), a static channel group (e.g. sa3), or a dynamic (LACP) channel group (e.g. po4).

The IGMP Snooping window displays interfaces, their status, and the configured multicast ports.



To add a multicast router port to an interface, select an interface and click **Edit**, then in the **Edit Interface** window:

- Click on the drop down box arrow.
- Select the port(s) you wish to include.
- Click **Apply**.



PoE

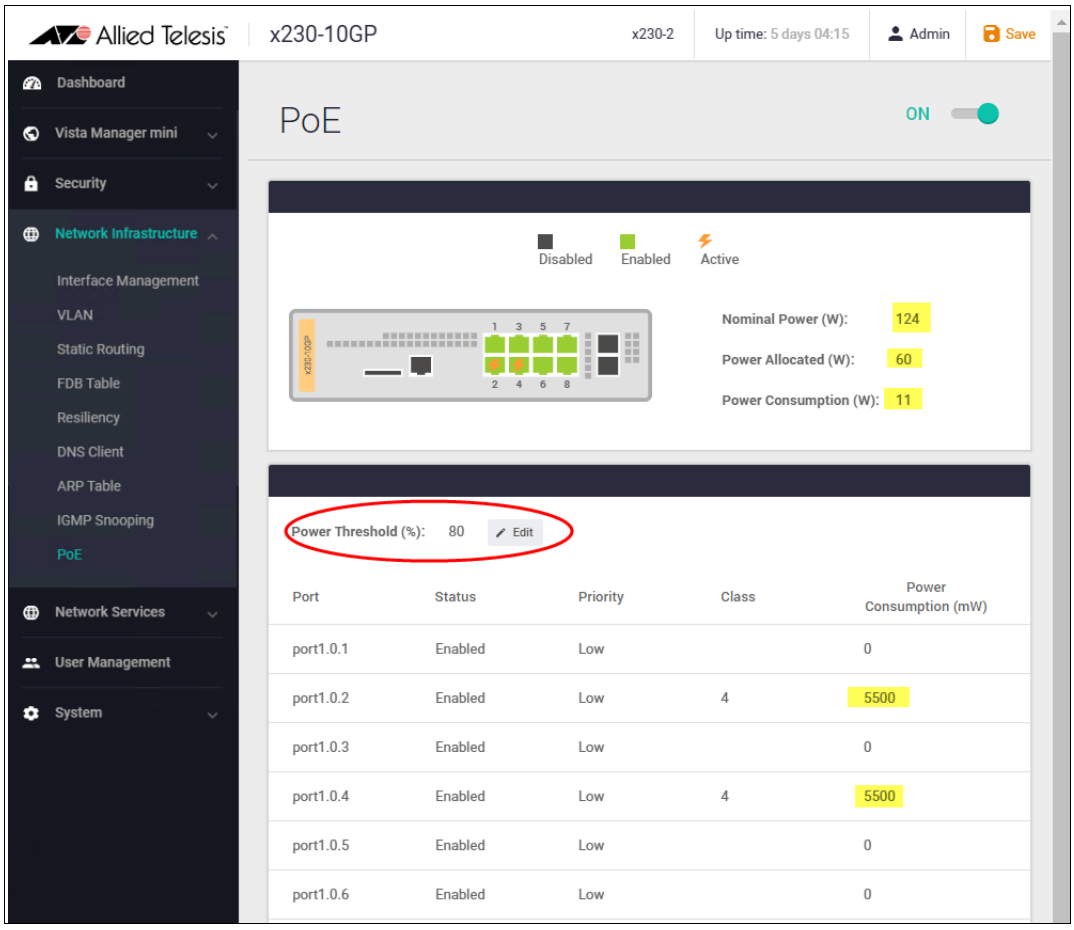
You can use the PoE page to:

- View detailed port information.
- Configure the PoE power threshold for a device.
- Configure the PoE power priority per interface.

Let's look at each of these tasks in more detail.

View detailed port information

You can view detailed PoE port information. For example, in the screenshot below, you can see that nominal power available to this device is 124 Watts. The power allocated over the device's 8 ports is 60 Watts. The actual power consumption currently being used by the two active ports is 11 Watts. The power threshold is currently set at the default of 80%.

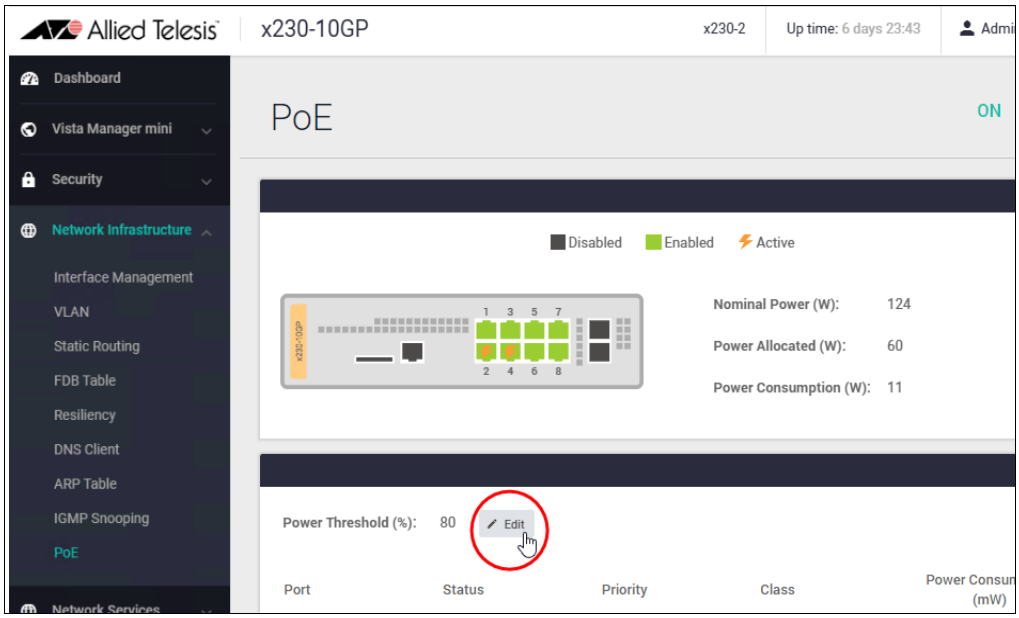


Configure the PoE power threshold for a device

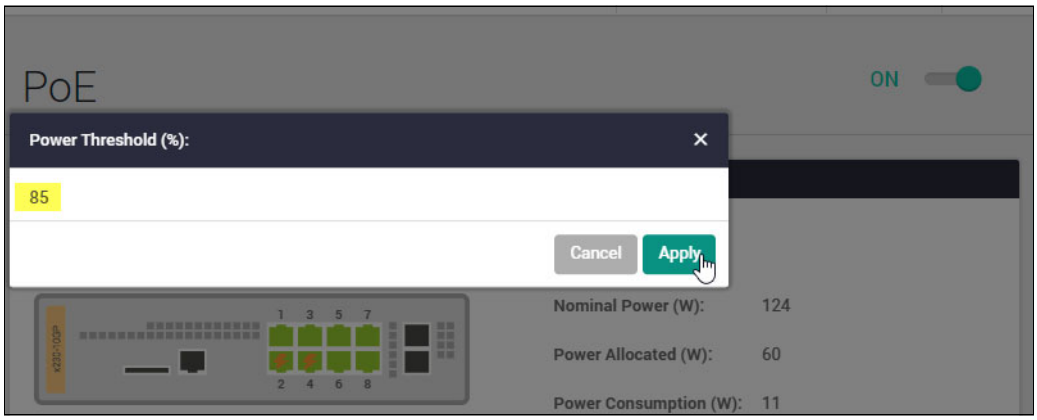
Use the power threshold settings to trigger an alert when the total PoE power consumption for a device goes above a configured limit. Previously, this feature was only configurable using the command **power-inline usage-threshold**.

To change the power threshold setting:

- Click on the Power Threshold (%) **Edit** button.



- Type in the power threshold percentage number. You can set the threshold to any value between 1% and 99%.
- Click **Apply**.



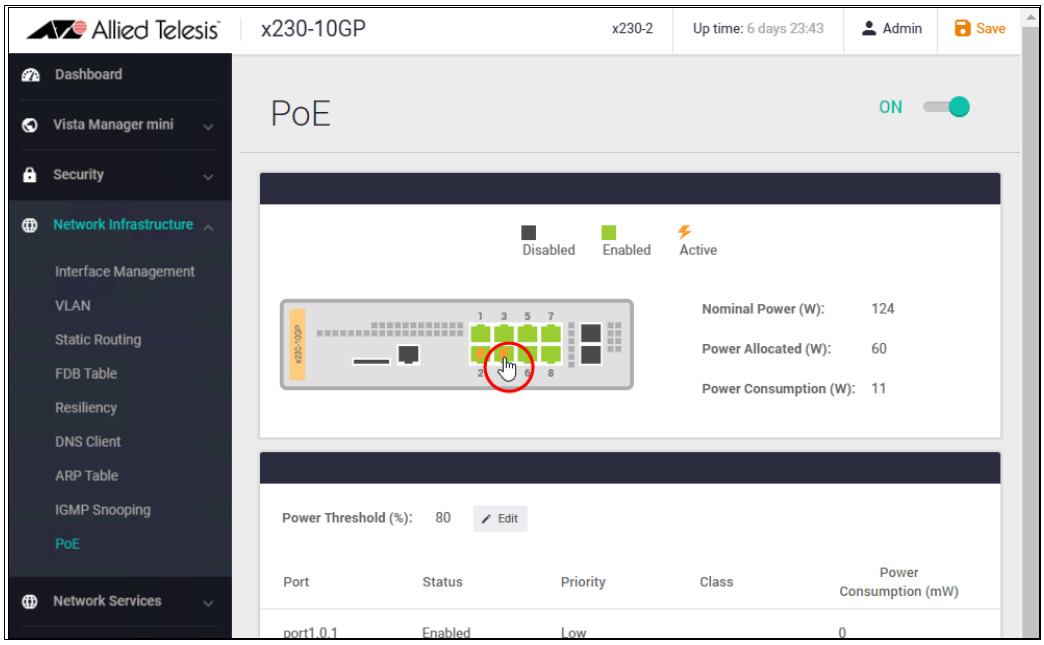
Configure the power priority per interface

If the PDs connected to a switch require more power than the switch is capable of delivering, the switch will deny power to some ports. Port prioritization is the way the switch determines which ports are to receive power if the needs of the PDs exceed the available power resources of the switch. This could happen, for example, if one of the power supplies stops functioning. The switch will remove power from the ports in the order of Low first, then High, then Critical.

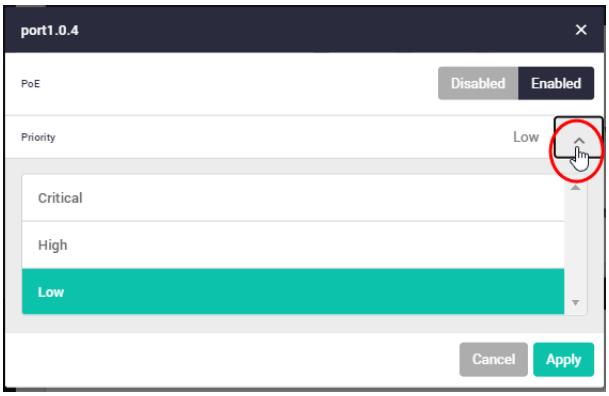
If there is not enough power to support all the ports set for a given priority level, power is provided to the ports based on the switch port number.

To change a port's power priority setting:

- Click the port you require (on the device image at the top of the page).



- The port detail window opens.



- With PoE enabled, click the **Priority** drop down box and select a **Level**: Critical, High, or Low.

  Critical: The highest priority level. Ports set to Critical level are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all the Critical ports are receiving power. Your most critical powered devices should be assigned to this level.

High: The second highest level. Ports set to High level receive power only if all the ports set to the Critical level are already receiving power.

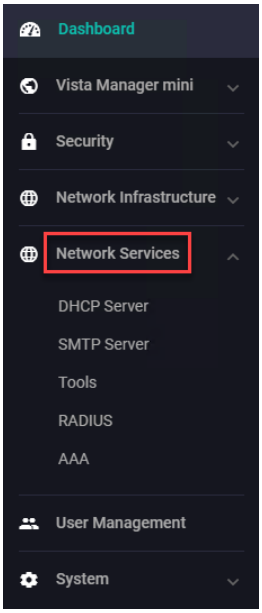
Low: The lowest priority level. This is the default setting. Ports set to Low level only receive power if all the ports assigned to the other two levels are already receiving power.

- Click **Apply**.

For more information on PoE, see the PoE Feature Overview and Configuration Guide.

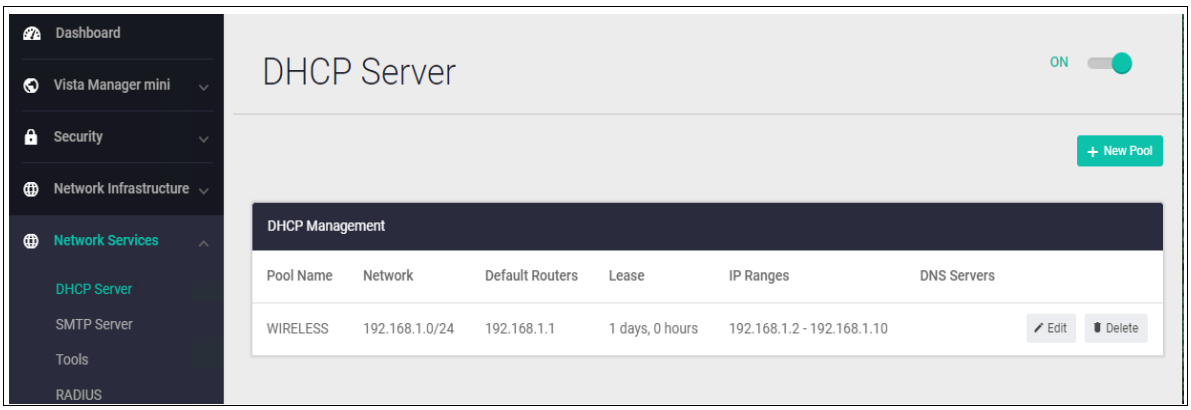
Network Services menu

The Network Services menu provides access to sub menus: DHCP Server, SMTP Server, Tools, RADIUS, and AAA.



DHCP Server

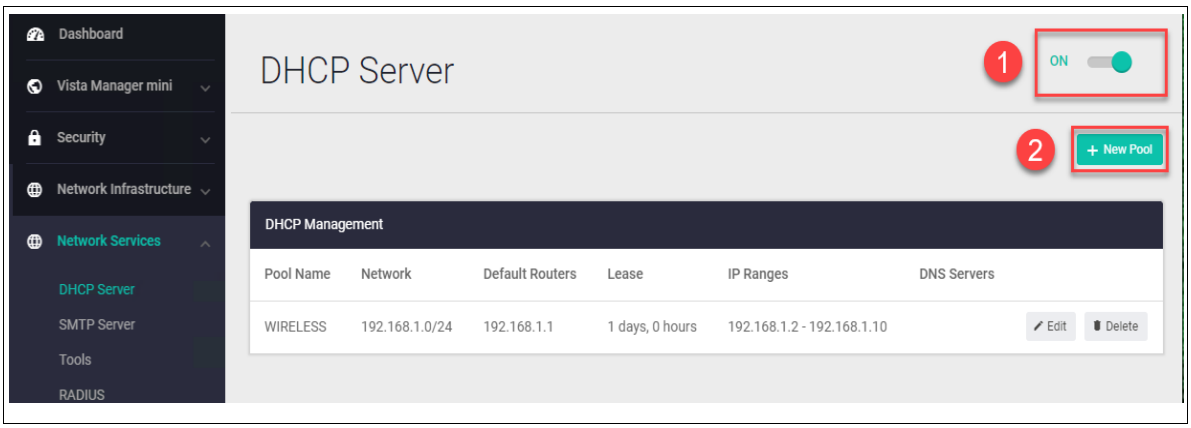
This is a very useful feature built into many Allied Telesis switches, firewalls, and routers. It allows the switch to provide IP addresses to connected nodes in the LAN, without the need to set up a separate DHCP server.



Any currently configured DHCP server pools are shown with their details.

1. Use the On/Off button at the top right of the page to enable DHCP server functionality.
2. Click **+New Pool** to add a new pool.

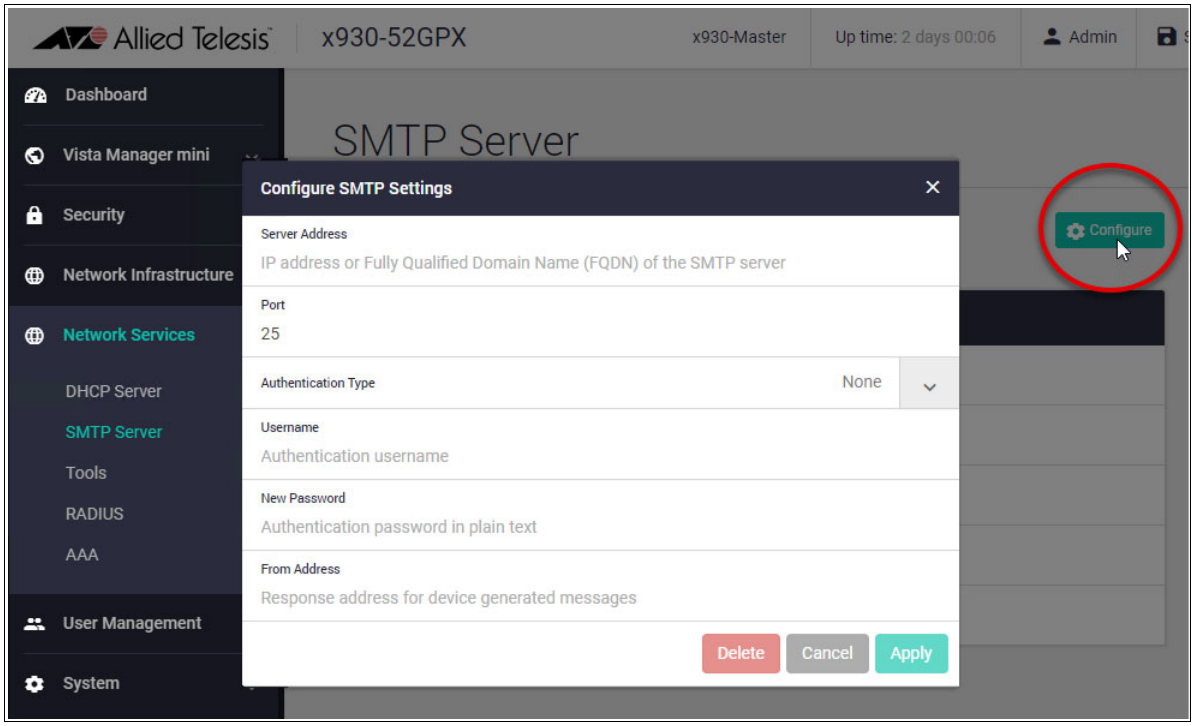
   When you create a new pool, you can specify the network, default router, lease time, IP address range/s, and DNS server/s.



- Click **Edit** to edit an existing pool (available from v2.11.0 onwards).
- Click **Delete** to remove an existing pool.

SMTP Server

The SMTP server can be configured to add email filters. When an event happens, the system triggers a notification to a specified email address via the configured SMTP server.



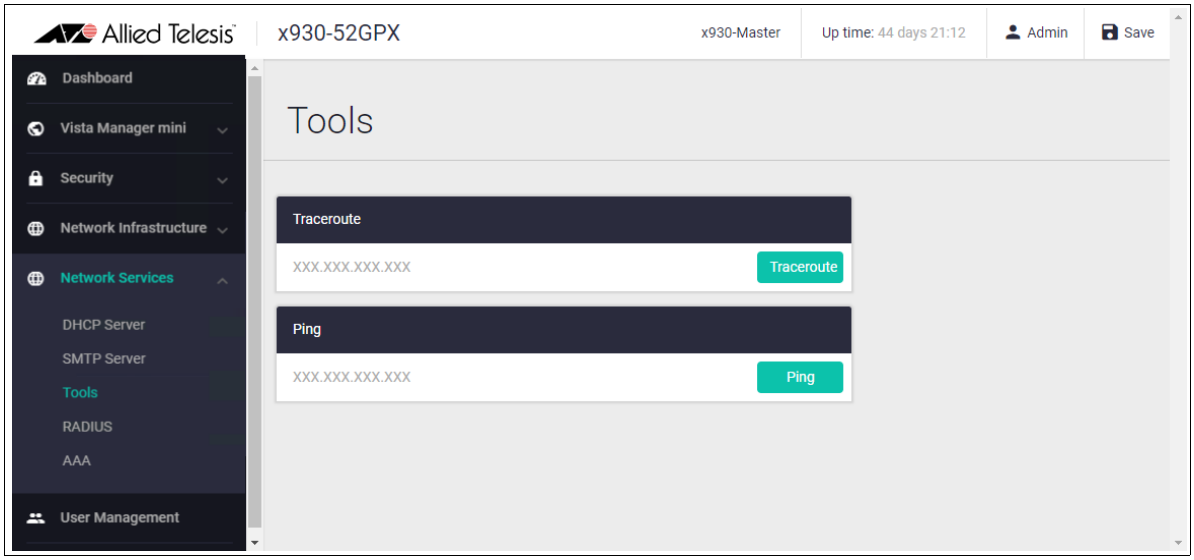
To configure the SMTP settings:

- Click **Configure**.
- Type in the **server address** and **port number**. The other fields are not mandatory.
- Click **Apply**.

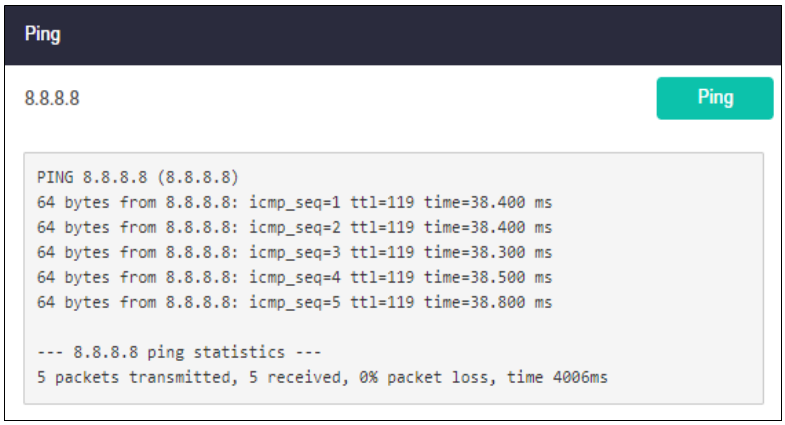
To add email filters, see "Logging" on page 35.

Tools

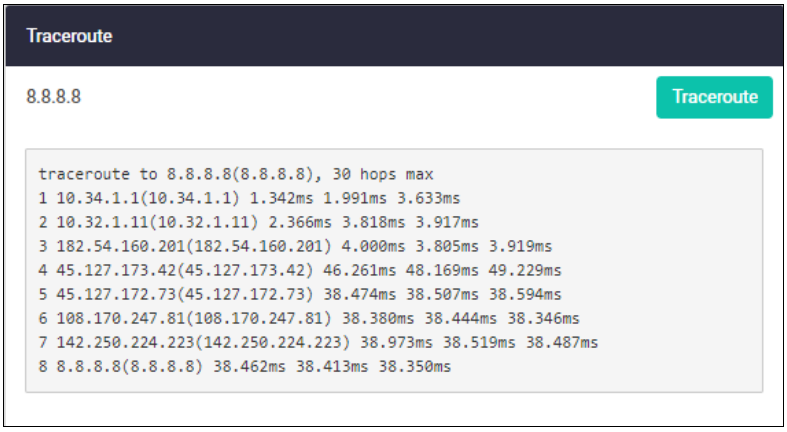
The Tools menu provides Ping and Traceroute which are useful for checking network connectivity and remote site reachability.



For example, shown here is a Ping of the IP address 8.8.8.8 (the Google public DNS service), and the results of 5 ICMP packets sent and received.

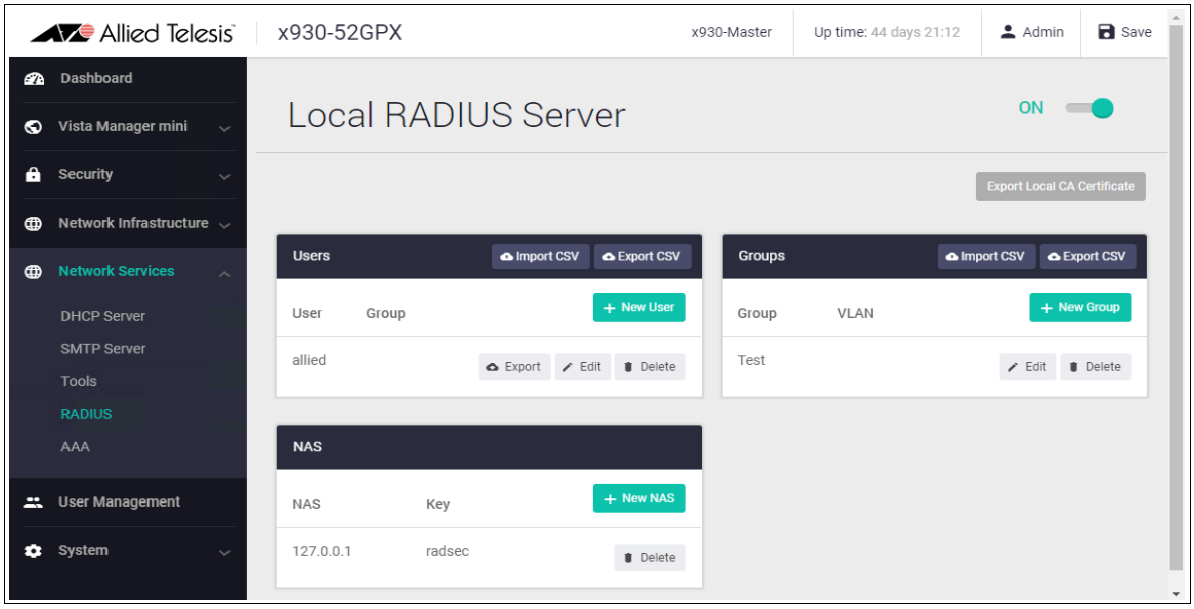


Here is the Traceroute to IP address 8.8.8.8, and the path taken to reach the closest Google DNS server.



RADIUS

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.



Use the Local RADIUS Server window to manage Groups, Users, and NASs (Network Access Servers), which are devices that can send authentication requests to the RADIUS Server.

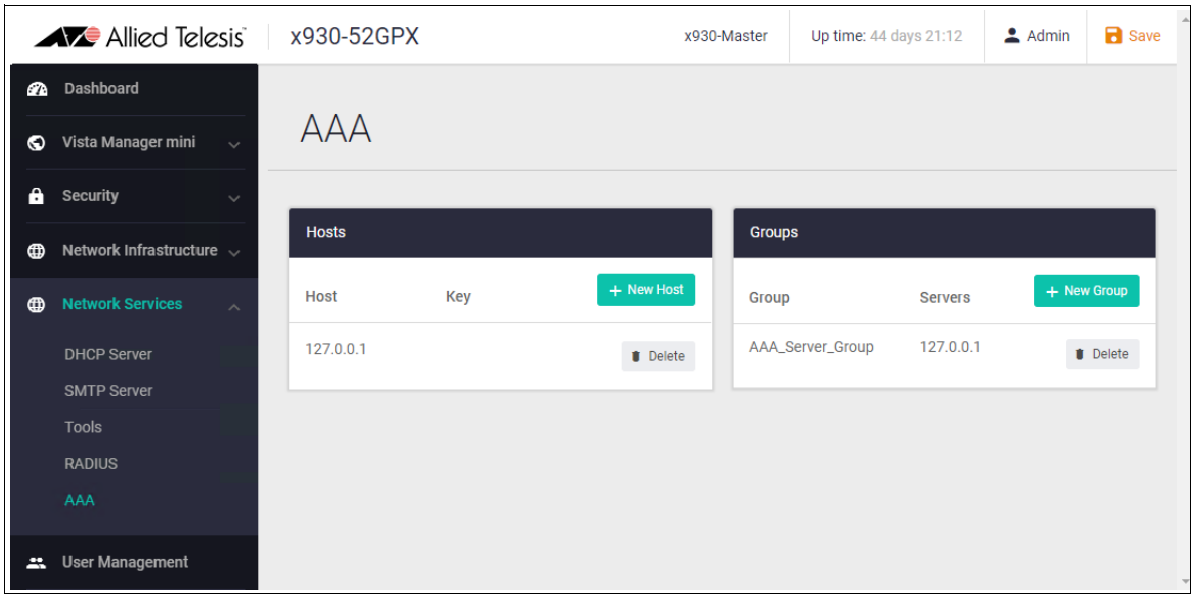
For more detailed information on configuring a local RADIUS server, see the Local RADIUS Server Feature Overview and Configuration Guide.

AAA

AlliedWare Plus enables you to specify three different types of device authentication: 802.1X-authentication, Web-authentication, and MAC-authentication.

- 802.1X is an IEEE standard for authenticating devices attached to a LAN port or wireless device.
- Web-authentication applies to devices that have a human user who opens the web browser and types in a user name and password when requested.
- MAC-authentication authenticates devices that have neither a human user nor use 802.1X when making a network connection request. This can include devices like network printers.

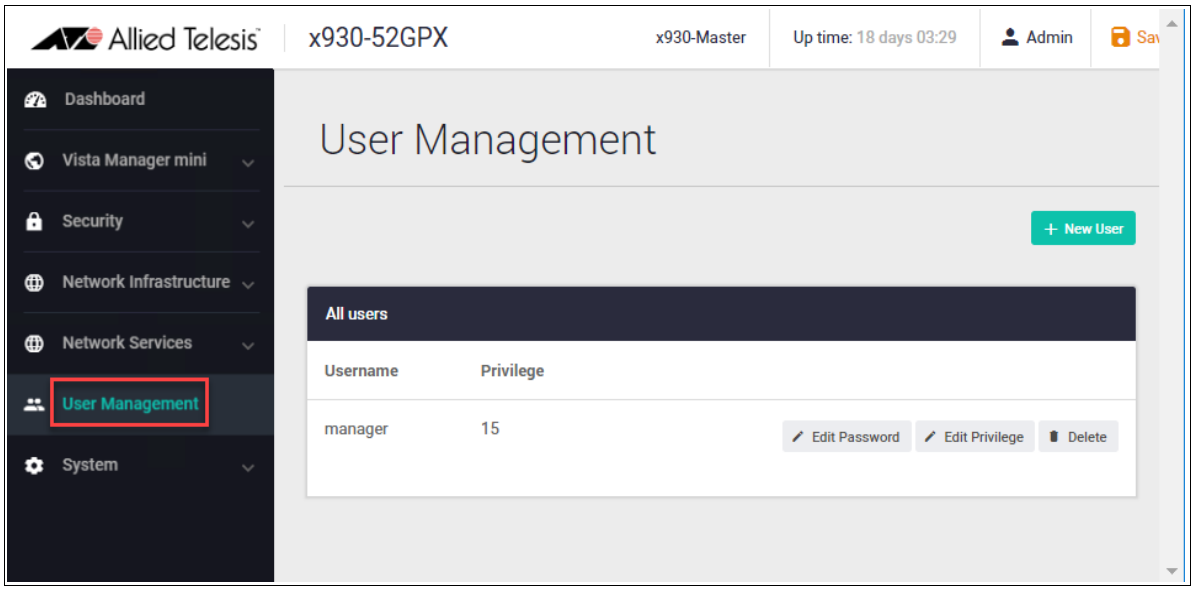
You can use these forms of device authentication separately or in combination, creating a powerful authentication feature set.



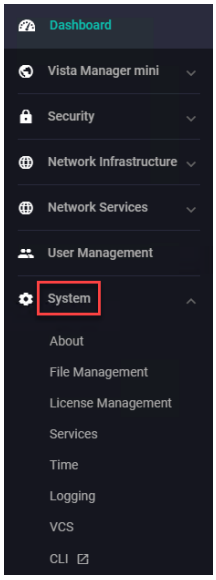
Use the AAA window to manage RADIUS server hosts and Groups. For more detailed information on AAA, see the AAA and Port Authentication Feature Overview and Configuration Guide.

User Management menu

The User Management menu lets you add a new user, and set a user password and privilege level: either 1-14 (limited access) or 15 (full access).



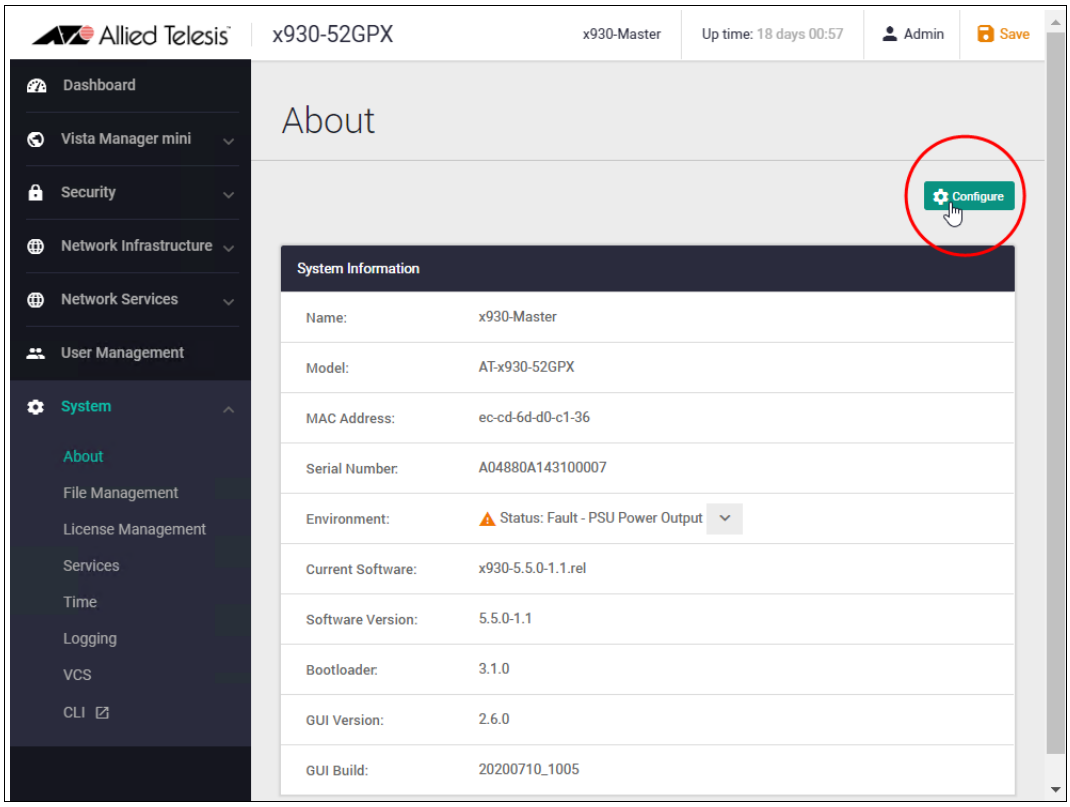
System menu



The System menu provides access to information about your device, file management, license management, services, time, logging, VCS, and a CLI window.

Let's look at each of the System sub menus in more detail.

About



The **About** page provides details of your switch, or switches if stacked. This includes the model, MAC address, serial number, current software release, bootloader, GUI version and so on.

The **About** information provides a good overview of your switch and its current setup, and is very helpful in the event of a problem, to assist Allied Telesis support.

You can optionally use the Configure button to add a device's contact and server location, and to change the GUI timeout.

Configuring the contact and server location:

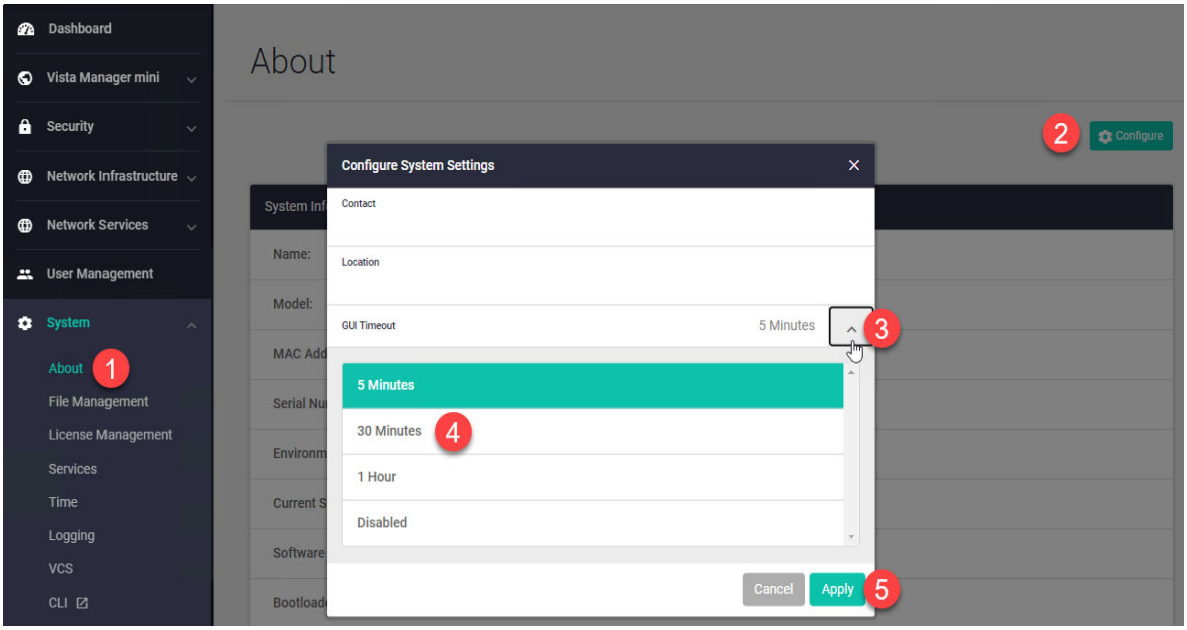
1. Click the green **Configure** button, at the top right of the window.
2. Type in the **Contact** and **Location** details.
3. Click **Apply**.

Setting the GUI timeout period:

From version 2.11.0 onwards, you can set a timeout period for the GUI. The default setting is 5 minutes, meaning that after 5 minutes idle time, the GUI will log you out.

To change the timeout period:

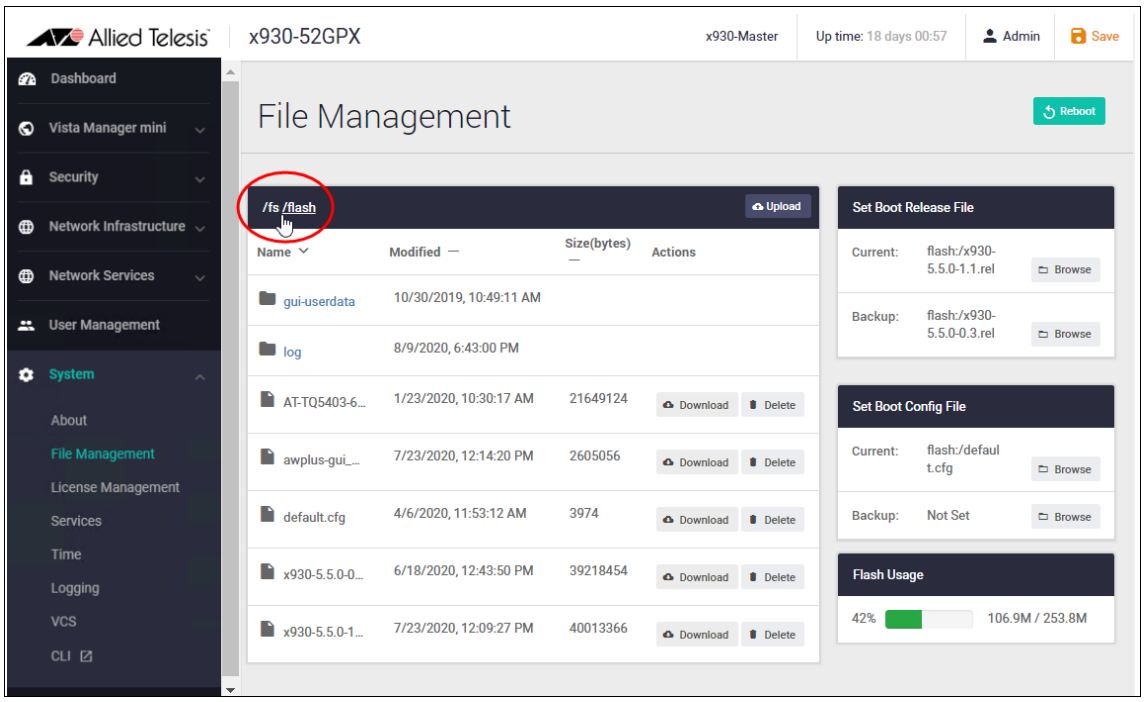
1. Select **System** > **About** to open the **About** page.
2. Click the **Configure** button. The **Configure System Settings** dialog opens.
3. Click the arrow beside the current **GUI Timeout** value.
4. Select the new timeout value.
5. Click **Apply**.



File Management

The File Management page shows all files that are stored in flash, and on USB or SD card if installed. By default the flash memory files are displayed.

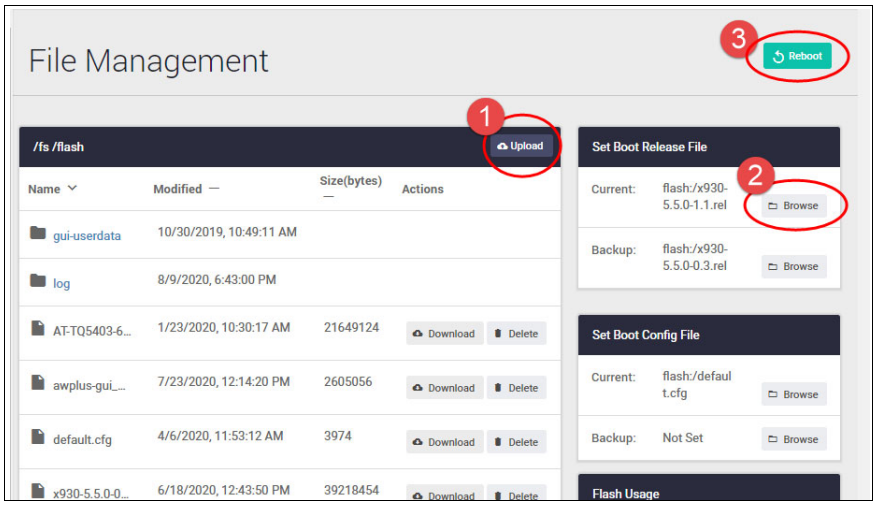
Click on the file storage link to navigate through the different storage options.



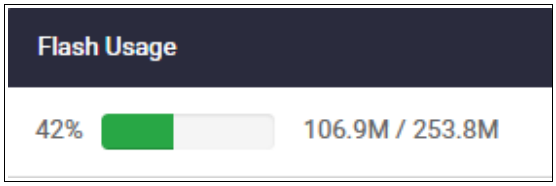
You can easily upload, download, or delete any file, as well as set the current and backup software release for the switch, and the current and backup configuration files.

It's an easy 3-step process to upgrade the switch software.

1. upload the new release to flash
2. set it to be the boot release
3. click the **Reboot** button.

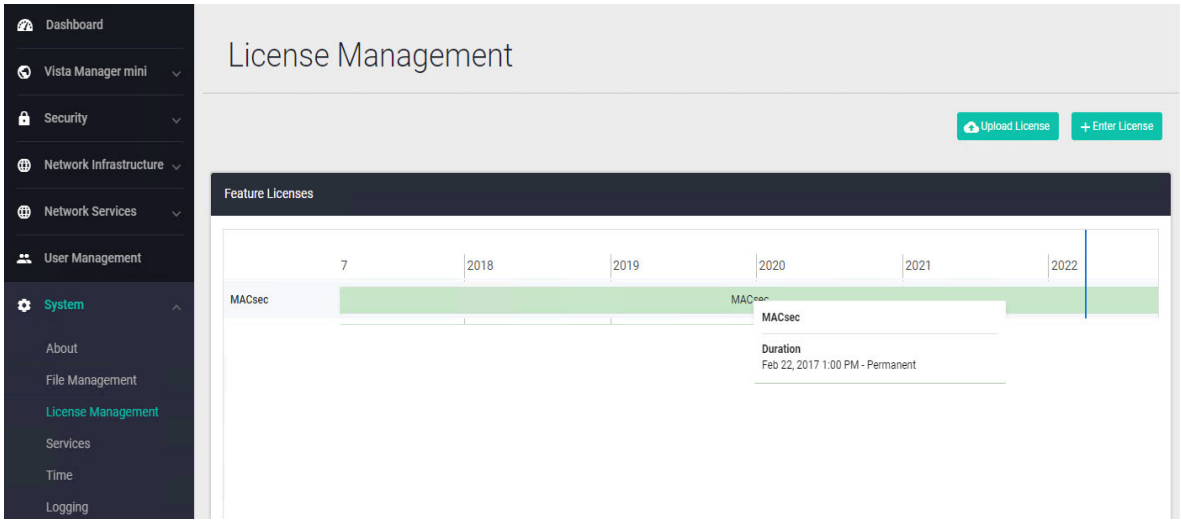


Tip Use the **Flash Usage** panel to check you have enough available space prior to uploading any large files.



License Management

Feature licenses are available for many switch models to unlock advanced functionality. The License Management page shows the licenses you currently have on your device, and their expiry date. It also allows you to add new permanent or subscription feature licenses.



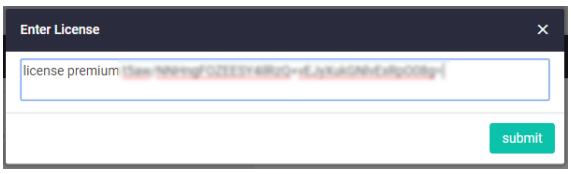
Hover your mouse over a license to show details, including duration and included features.

Adding a new permanent feature license

Once you have purchased your new license (for example, a Premium license), here's how to add it to your device:

1. Click the **+enter license** button.

2. Enter the license enable command you will have been sent by Allied Telesis.



Adding a new subscription feature license

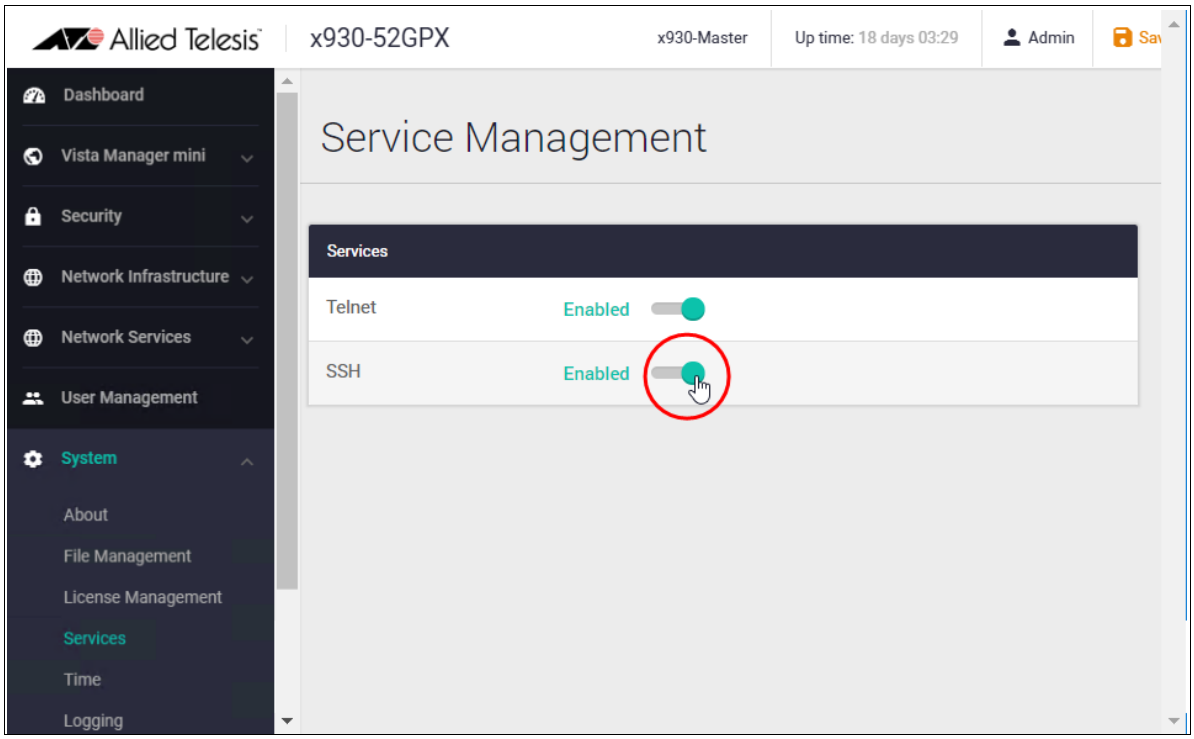
Once you have purchased your new subscription license (for example, a 1 year OpenFlow license), here's how to add it to your device:

1. Click the **upload license** button.

2. Browse and select the .bin file you will have received. Once selected, the .bin file will be uploaded, and the license added to your device.

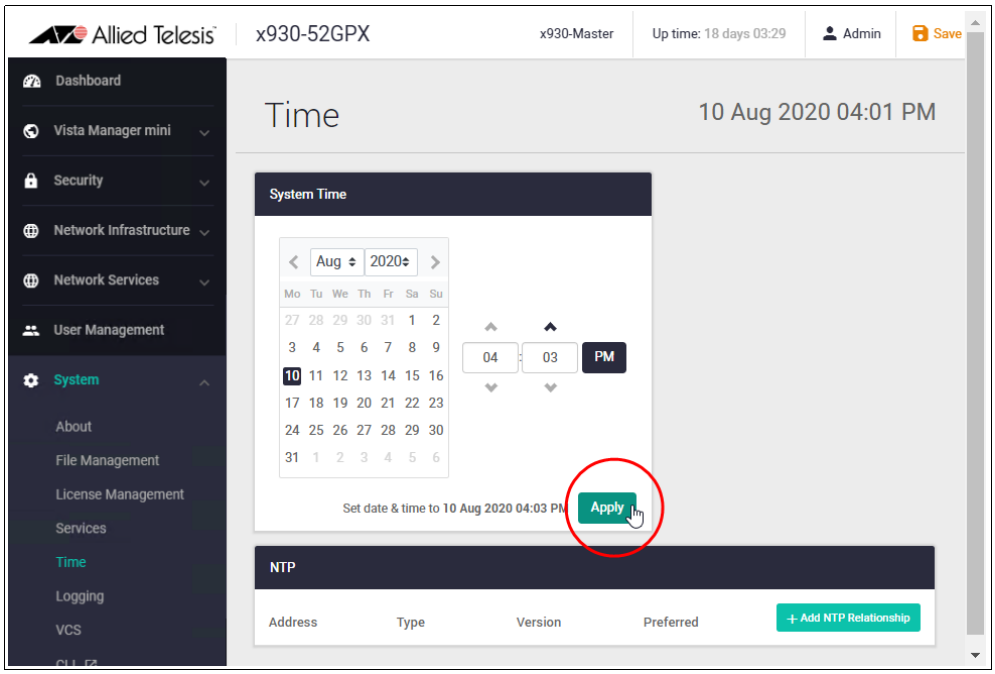
Services

Use the Services window to enable or disable Telnet and SSH services.



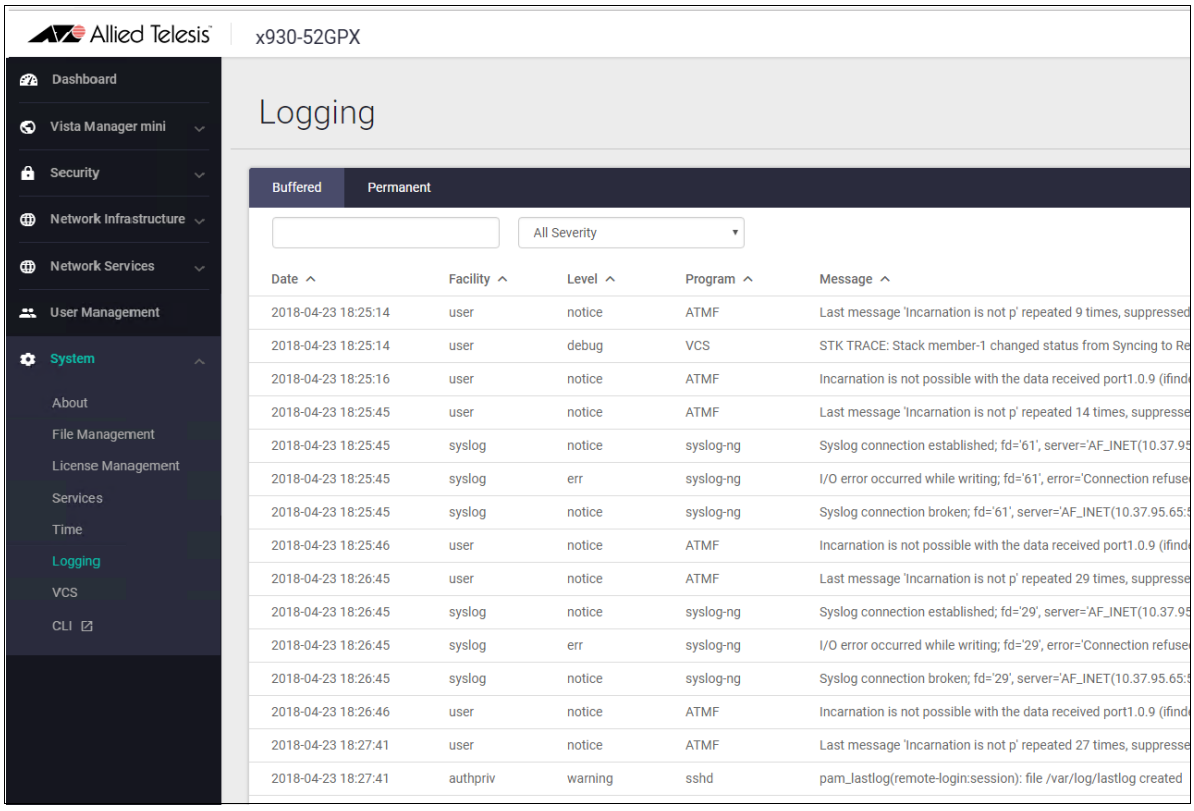
Time

You can change the System time and date using the **Time** window:



Logging

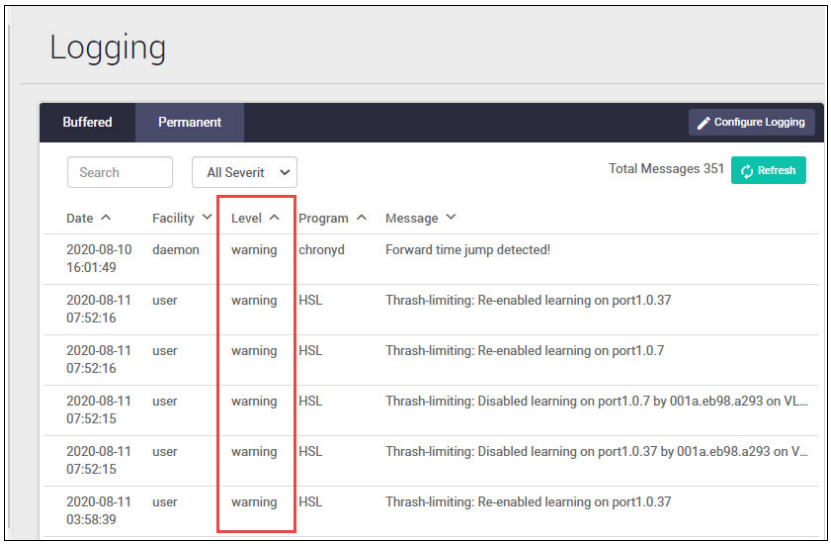
The Logging page shows buffered and permanent log messages stored on the device. By default the buffered logs tab is displayed.



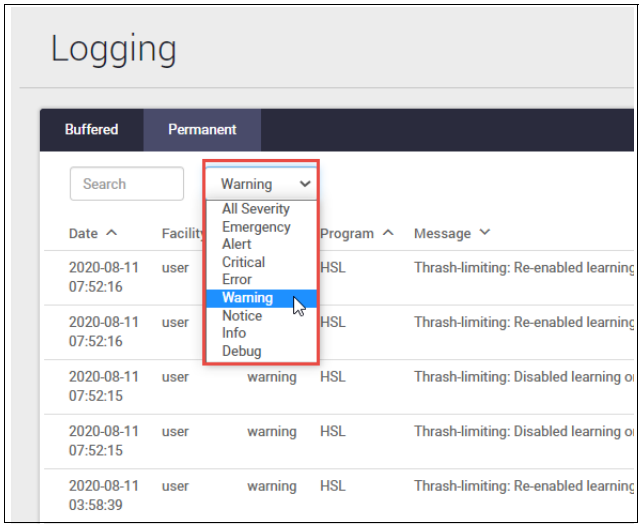
You can filter the logs in 3 ways to focus your view and support easy analysis:

Filter logs by:

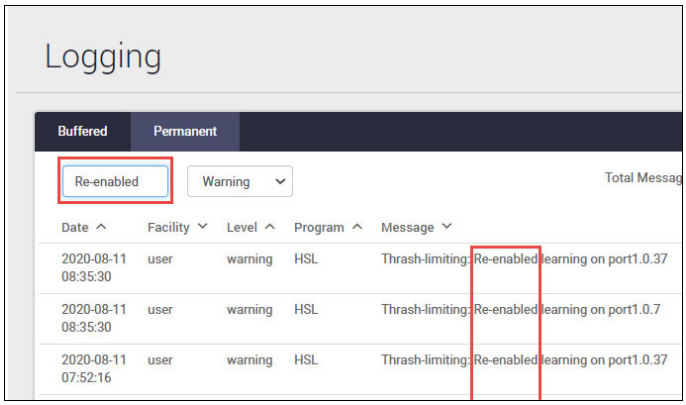
1. any information column in ascending or descending order



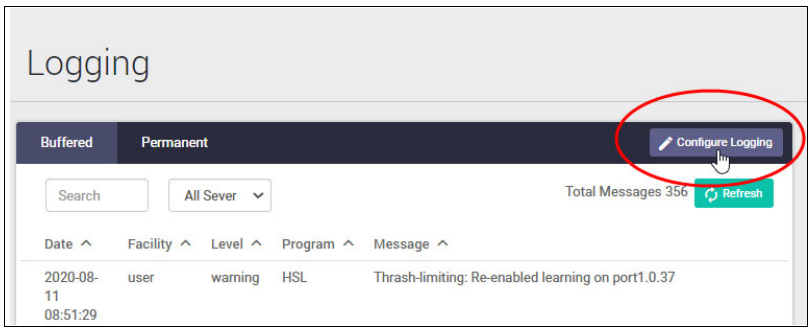
2. selecting the level of logs to display, e.g Critical, Warning, Error etc.



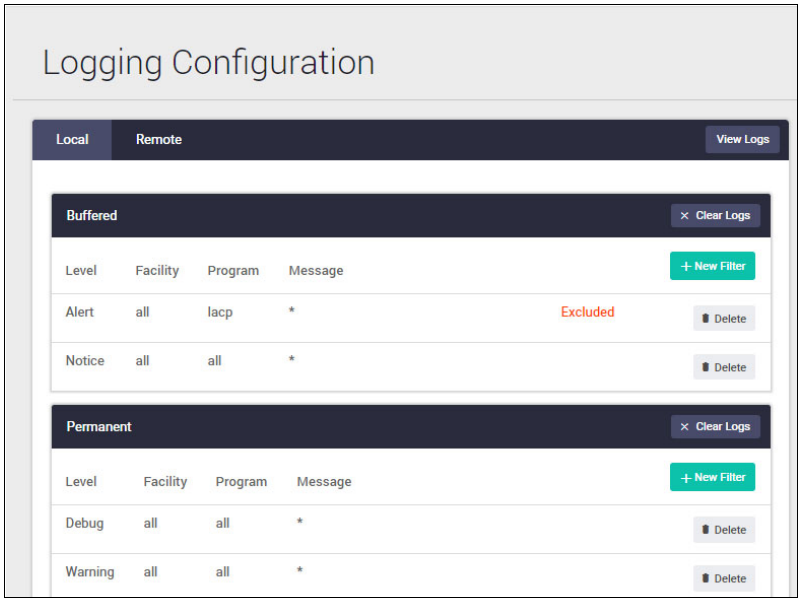
3. searching for any text string found in the logs.



Click the **Configure Logging** button to access the Logging Configuration page. This page allows you to create filters to manage which logs are stored on the switch and also set up a Syslog server(s) for remote log storage.



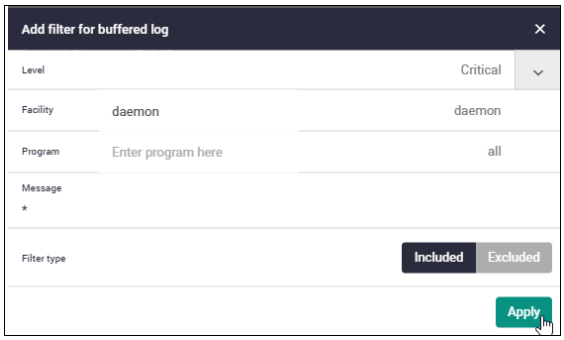
The **Logging Configuration** page has tabs for local and remote (syslog server) settings.



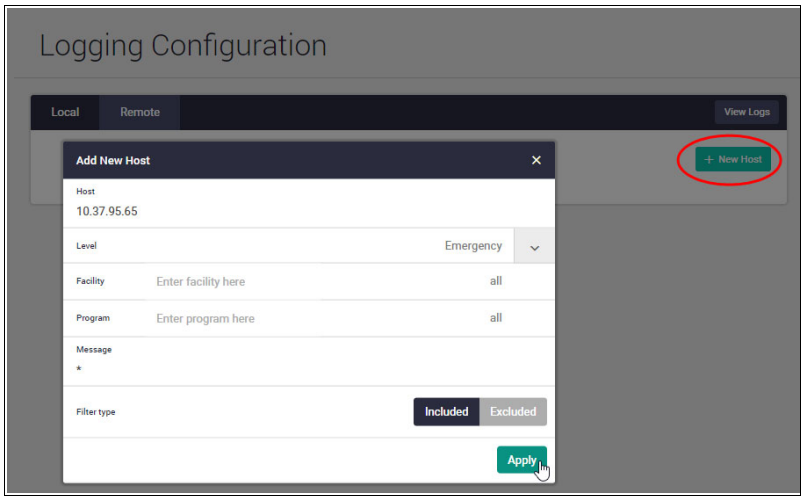
Use the **Local** tab (default) to create filters to manage the level of logs that are stored in the buffered and permanent logs on the switch. You can also delete the buffered or permanent logs using the **Clear Logs** button.

Use the **View Logs** button to return to the Logging page.

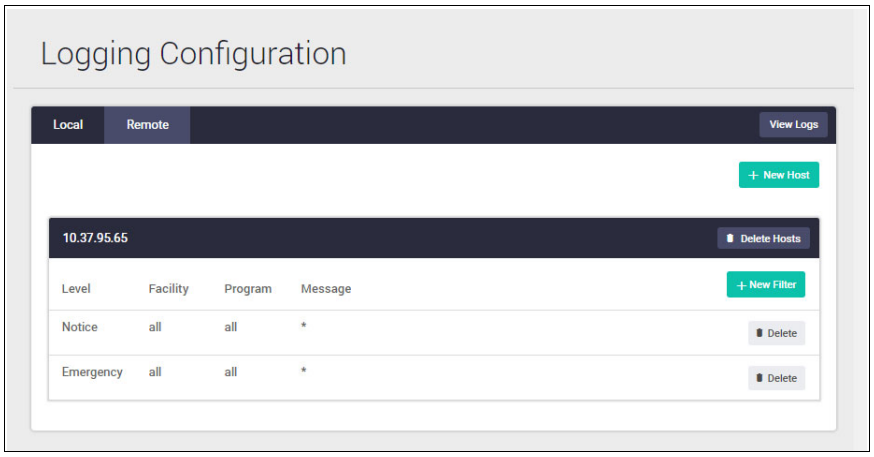
When creating a new logging filter you can specify any/all of level, facility, program, and message to be included or excluded in the log storage. This enables log storage on the device to be configured exactly as desired.



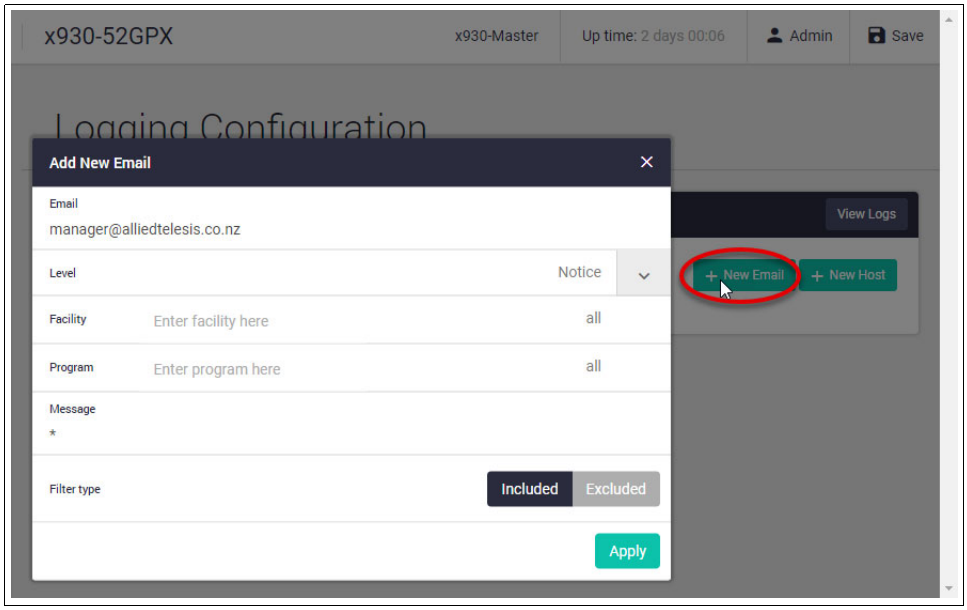
Use the **Remote** tab and the **+New Host** button to set up a syslog server to send log messages to for storage and analysis.



Use the **+New Filter** button to configure filters that specify the type of logs (include or exclude) to be sent to the syslog server.

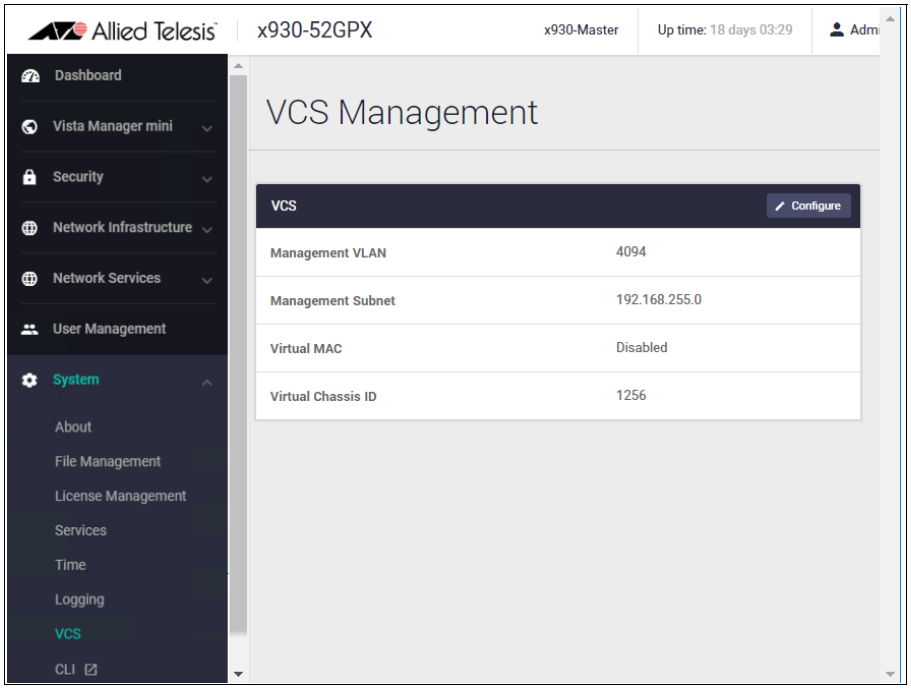


Similar to hosts, you can also add new filters to an email once you create it. First, use the **+New Email** button to type in a destination email address. Then click **Apply**.



VCS

For VCS (Virtual Chassis Stacking), internal communication between stack members is carried out using IP packets sent over the stacking links. This stack management traffic is tagged with a specific ID and uses IP addresses in a specified subnet.



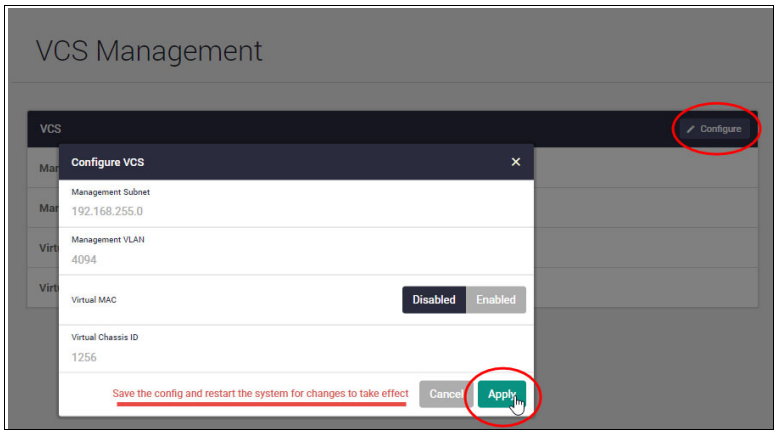
By default, the VLAN and subnet used are:

- VLAN 4094
- Subnet 192.168.255.0/28

You may need to change these values if they clash with a VLAN ID or subnet that is already in use in the network.

It is important that the settings for management subnet and management VLAN are the same for all the switches in a stack. If you add a switch to a stack, and its setting for management VLAN and/or management subnet differ from those on the other stack members, the new switch will not be joined to the stack.

Remember to save your VCS configuration and restart the system for changes to take effect.

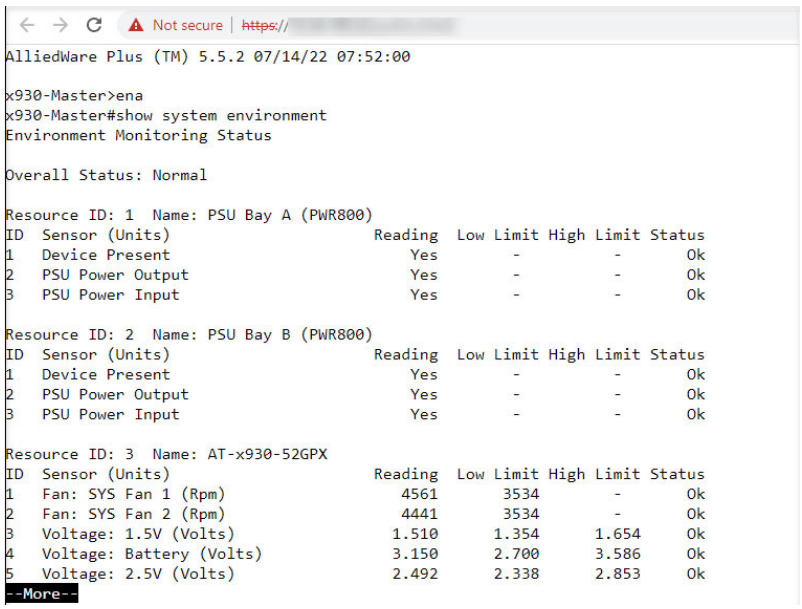


For more detailed information on cabling up a stack and configuring VCS, see the VCStack Feature Overview and Configuration Guide.

CLI

Allied Telesis devices running the AlliedWare Plus operating system have an industry-standard command line interface (CLI) where all features and functionality can be configured.

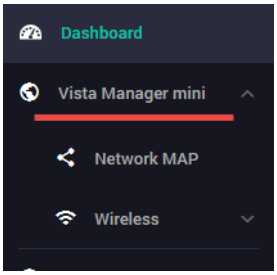
To access the CLI from the GUI for advanced configuration, click **CLI** under the **System** menu to open a CLI window.



Vista Manager mini menu

On selected switches, the Vista Manager mini menu allows you to view a network map and configure your wireless network. Autonomous Wave Control (AWC) wireless management uses wireless intelligence to constantly model AP location and signal strength information. It then automatically optimizes wireless output and channel selection for optimum performance.

Vista Manager mini is useful for smaller networks that may not need the capabilities of Vista Manager EX. It is a simplified version of Vista Manager EX and is integrated into the Device GUI on selected AlliedWare Plus switches, firewalls, and VPN routers.

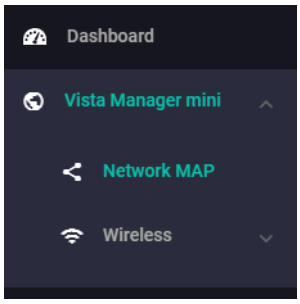


The device GUI also displays heat maps for managed APs on the network map.

For more information about heat maps, AWC and how to manage wireless devices, see the User Guide: Wireless Management (AWC) with Vista Manager mini.

The network map

Under the Vista Manager mini menu, there is a network topology map:



This map shows details of the devices connected to the switch or firewall. You can use it to see your:

- wired devices
- APs
- wireless deployment and coverage.

This section begins with a brief description of the network map window and the tasks you can perform there. The section ends with a look at configuring the network topology view and customizing node icon images.

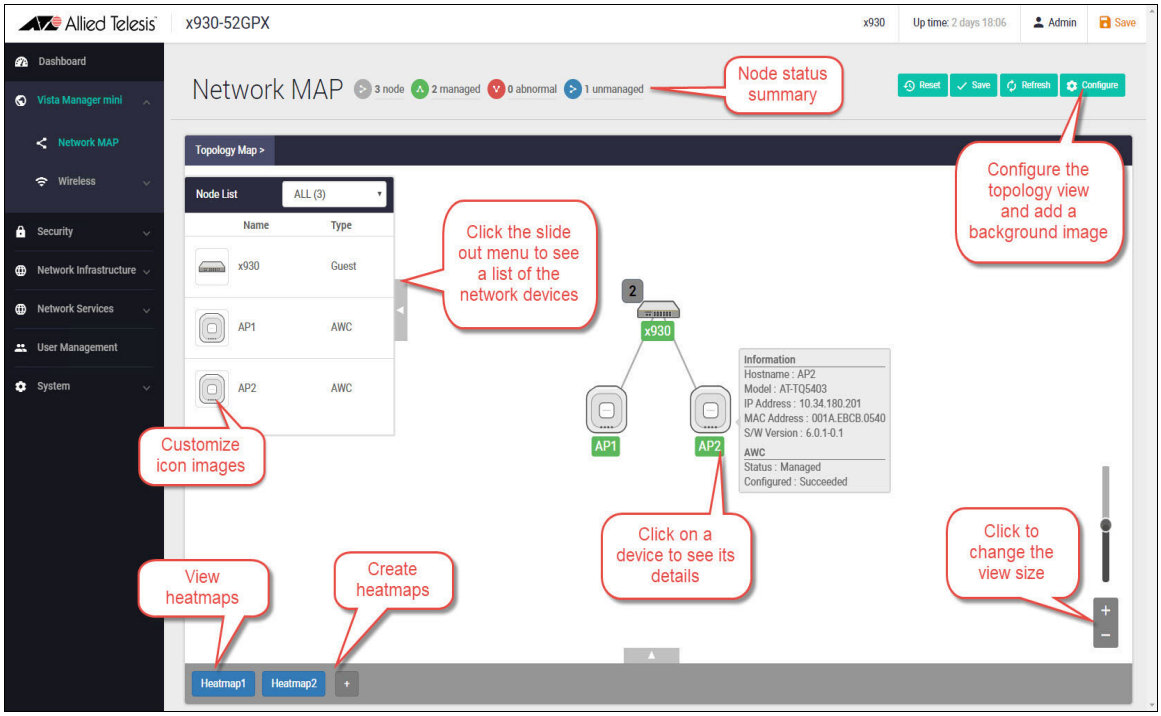
Note that the screenshots in this section show an x930 Series switch, but the functionality is the same for all models that include Vista Manager mini.

The network map features

The network map displays details of a network configuration. Double click on an area to see all the nodes in that area. Use the network map to check the status of a node at a glance. Node status is indicated by the node title background color. Abnormal is red, managed is green, and blue indicates an unmanaged node.

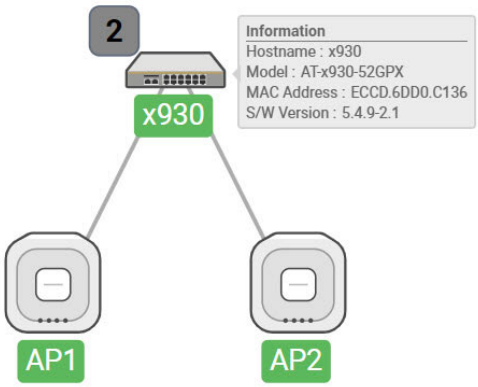
From the **network MAP** page, you can:

- customize network icon images
- view individual node details
- see a list of network nodes
- configure the topology view
- create a heat map
- view stored heat maps



Viewing node information

In the network topology map view, click on a device to see information about the Hostname, Model, MAC address, and software version.



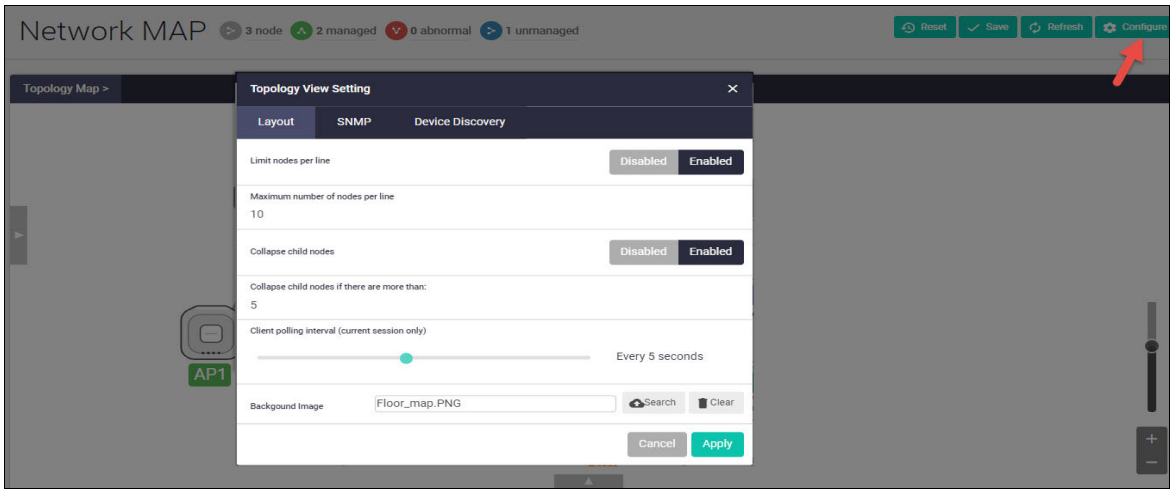
Configuring the topology view

Vista Manager mini automatically creates a complete topology map from an AMF network of switches, firewalls, and wireless access points (APs), showing areas and multiple levels of connected nodes and devices.

To change the topology view settings:

- In the Topology Map view, select **Configure** - the menu is located at top right corner.

- In the **Topology View Settings** window, you can choose to:
  - limit nodes per line
  - collapse child nodes
  - select a background image
- **Save** your changes.



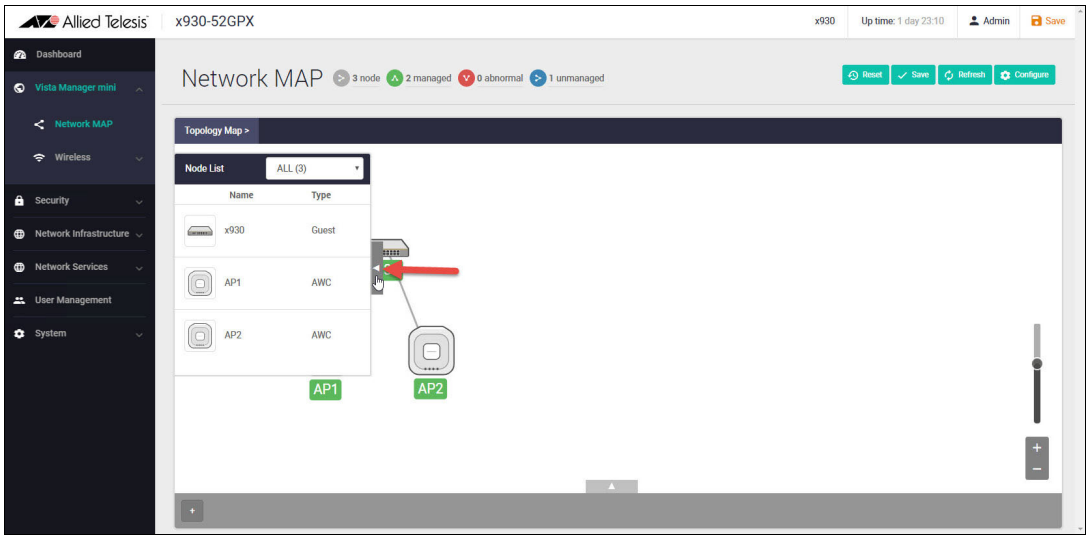
Customizing network node icon images

You can customize the look of your network nodes with icon images. For example, you can add access point, switch, and router images to make the network map easier to understand at a glance.

You can create an icon library to help store, organize, and find images.

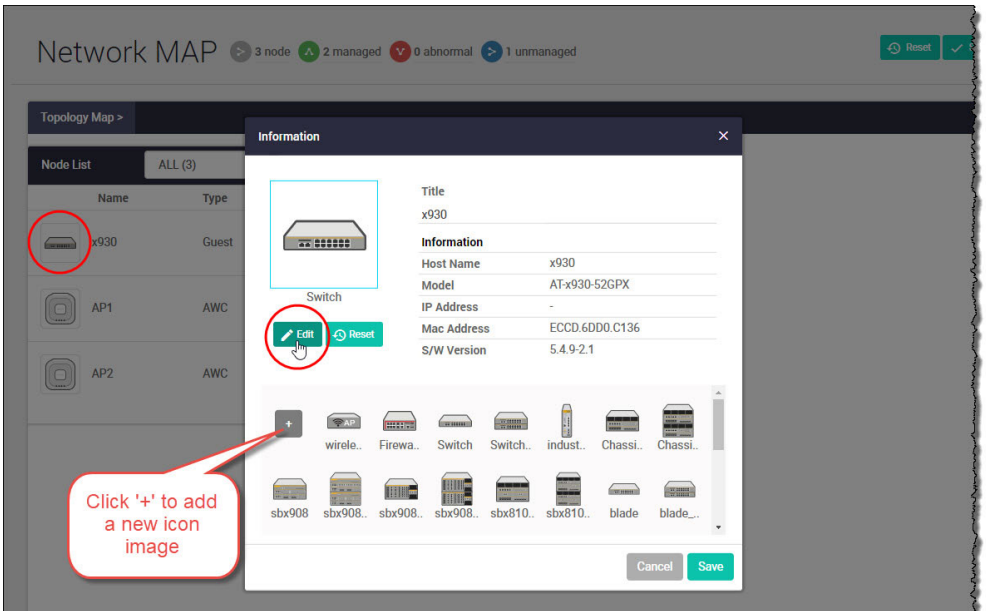
To customize a network node icon:

1. In the Topology Map view, open the **Node List** (slide-out menu)



2. Click on a node's icon image.
3. Click **Edit**.

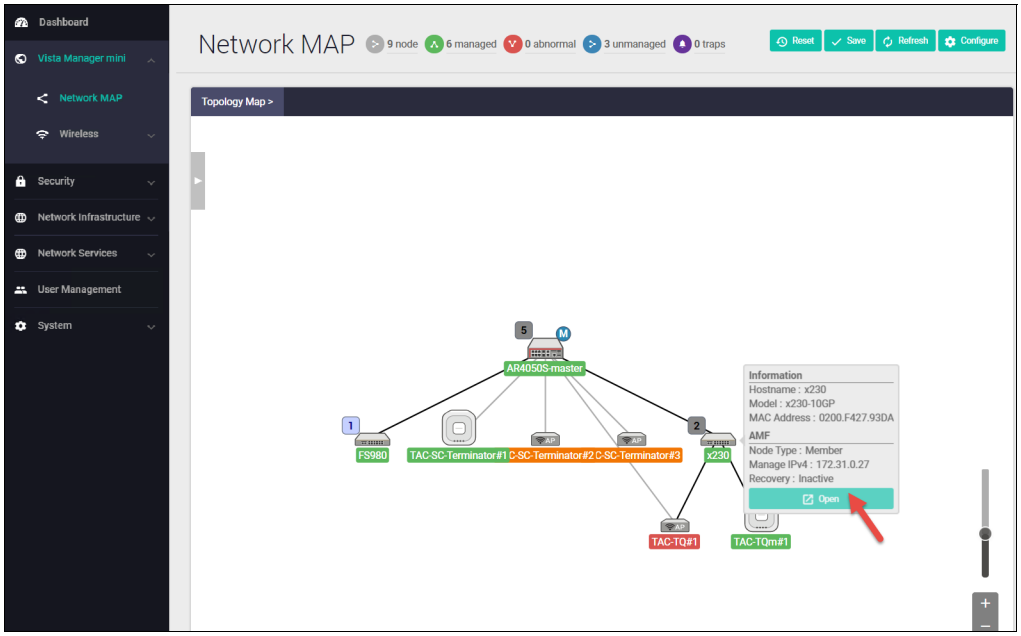
4. Select an image from the library or click the '+' sign to add a new one.
5. Click **Save**.



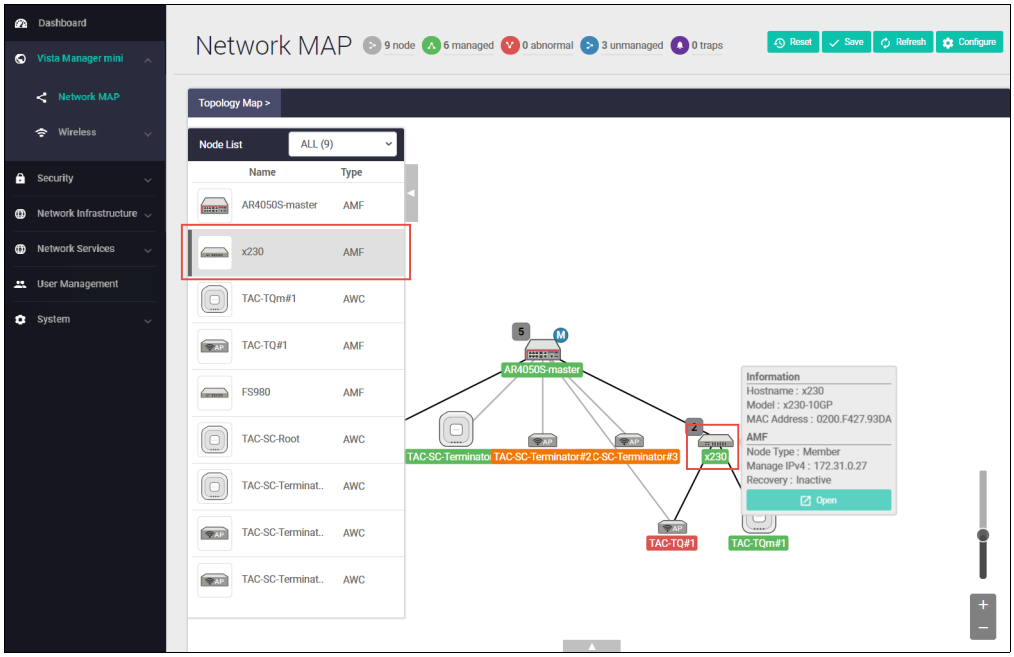
Access to device GUI by clicking on device icon

From version 2.5.2 onwards, you can open the GUI for a device in your network (e.g. an x230) from the network map in the GUI of another device in your network (e.g. an AR4050S).

When you click a node icon on the Network Map, the node information is displayed. In the node information window, click on the **Open** button to access the device's GUI.

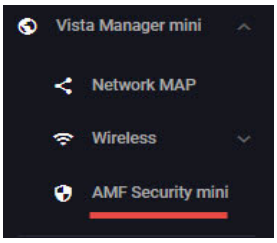


You can use the **Node List** to help you locate a device in the network map. Simply click the device in the Node List to see its **Information** details.



AMF Security mini on the x950 Series

From Device GUI version 2.8.0 onwards, the GUI supports AMF Security mini (AMF-Sec mini) on the x950 Series switches. Allied Telesis Autonomous Management Framework (AMF) simplifies and automates network management. AMF Security mini adds a powerful security component with an intelligent SDN controller that works with firewalls and other security devices to instantly respond to alerts, and block the movement of malware threats within a wired or wireless network.



For more information on using AMF-Sec mini, see the User Guide: AMF Security mini.

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