Technical Guide

Getting Started with the Device GUI on Switches

Feature Overview and Configuration Guide

Introduction

The Allied Telesis Device GUI is available on switches, firewalls, and routers running the AlliedWare Plus™ operating system. It provides an easy-to-use interface for monitoring and managing your device, with access to the Command Line Interface (CLI) for more advanced configuration tasks.

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 full AlliedWare Plus feature set through the industry-standard CLI
- On supported switches, use the Wireless Controller to manage wireless APs and monitor devices connected to the switch

For guides to using the Device GUI on other platforms, see "Related documents" on page 4.

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.

In order to use the latest features with the latest Device GUI versions, update to the latest version.

The screenshots in this guide were made with a switch running AlliedWare Plus software version **5.5.4-0.1** and Device GUI version **2.18.0**. To replicate this setup, please use these versions.

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

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.

The screenshots in this guide were made with a switch running AlliedWare Plus software version **5.5.4-0.1** and Device GUI version **2.18.0**. To replicate this setup, please use these versions.

Supported web browsers for connecting to the Device GUI are:

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

Browsing 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. The GUI starts up and displays a login screen.

3. Log in with your username and password.

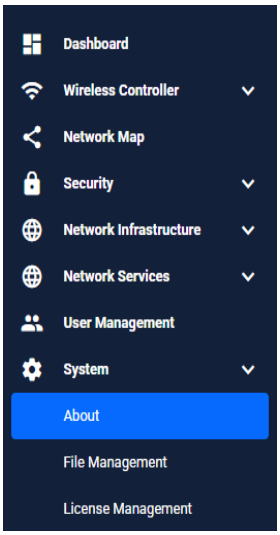
   The default username is ***manager*** and the default password is ***friend.***

4. Change your password from the default username and password combination.

   From AlliedWare Plus version 5.5.5-1.1 and Device GUI version 2.21.0 onwards, when you first login using the default username and password, you will be prompted to change your password.

   Do not use the default username and password combination.

Checking 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 Downloads and Support Center.

Updating 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.

You can obtain the latest GUI file from the Software Downloads and Support Center.
For example, the filename for v2.22.0 on AlliedWare Plus version 5.5.5-2.x is awplus-gui_555_40.gui.

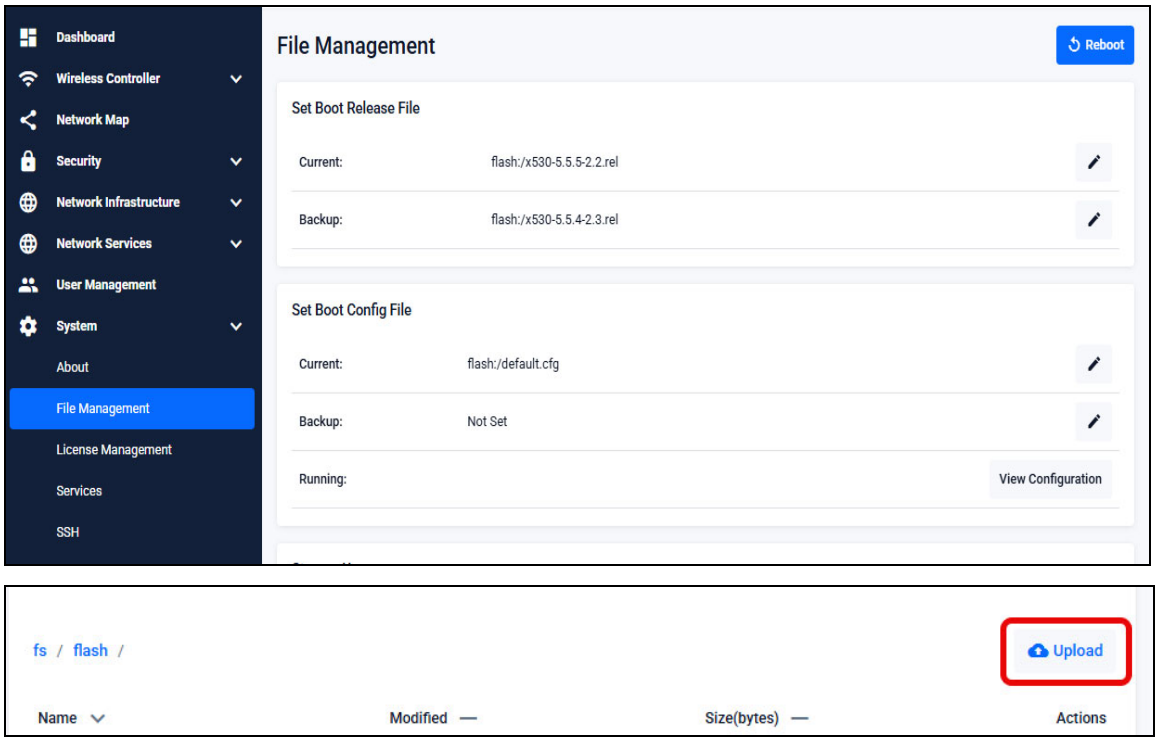
Make sure that the version string in the filename (e.g. 555) matches the version of AlliedWare Plus running on the switch. The file is not device-specific; the same file works on all devices.

2. Log into the GUI.

Start a browser instance and browse to the device's IP address by typing it into the address bar. 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.

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

3. Go to **File Management** to upload the GUI file.



4. Locate and select the GUI file.

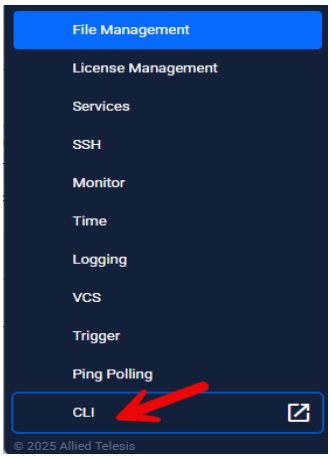
The new GUI file is added to the **File Management** window.

- You can delete older GUI files if you would like by clicking the **Delete** button next to the file.
- You can also back up files in this window locally by clicking **Download**.

5. Reboot the switch

- You can either reboot the switch from the **File Management** window with the reboot button at the top left of the page.
- **Alternatively**, use a Serial console connection or SSH to access the CLI.

You can access the CLI from the **System** sidebar.



6. Restart the HTTP service

Restarting the HTTP service is required because the device's web server must reload the updated GUI files and configuration. Without restarting, the server would continue using old cached files, which can cause outdated or inconsistent GUI behavior.

From the CLI, 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:

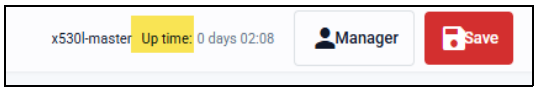
```
awplus(config)# exit
awplus# show http
```

The Dashboard

After logging in, you'll see the Device GUI dashboard. This dashboard provides key information for monitoring the status and health of your switch, including port connectivity and traffic details.

The dashboard is made up of widgets—interactive components that let you perform functions or access services. You can click and drag these widgets to rearrange them as needed.

At the top right of the screen you can see the **Uptime** for the switch, as well as the **Admin** (login) and **Save** buttons.

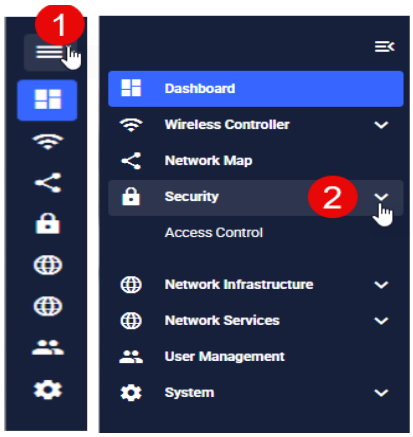


The **Save** button is colored **red** any time there is unsaved configuration, or blue if the configuration has been saved.

Menus

The main menus are located on the left side of the dashboard.

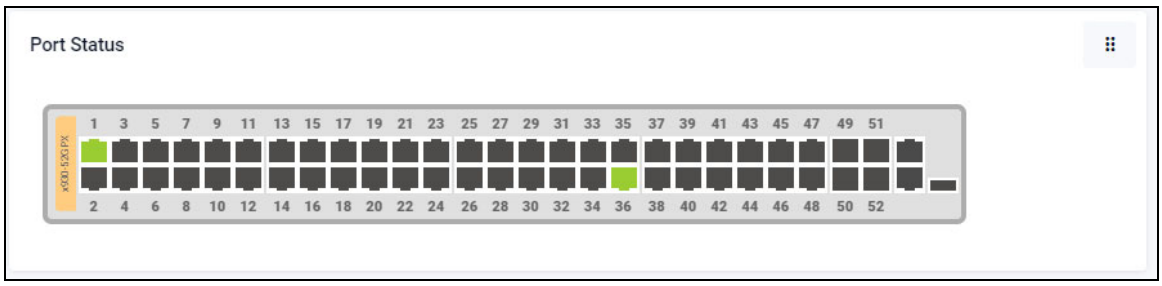
1. Click the Expand/Collapse icon to show or hide the menu.
2. Click the arrow next to a menu to expand its submenu.



Dashboard Widgets

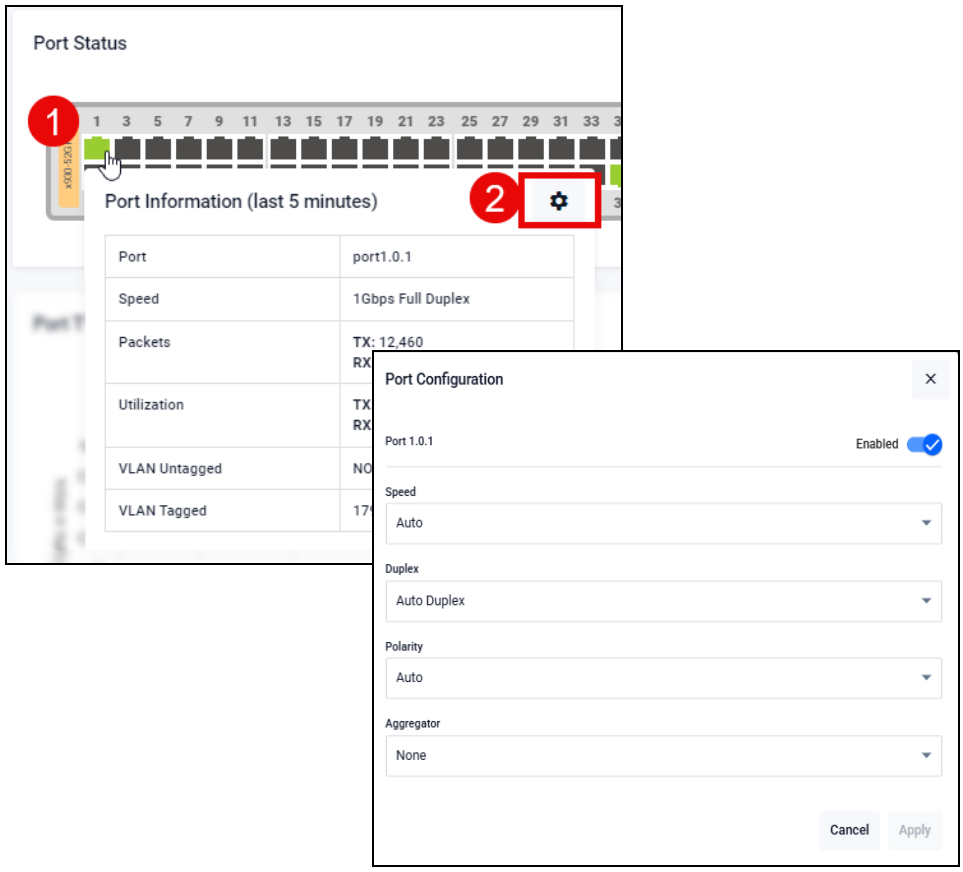
Port Status

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.



1. Hover your mouse over any port to display 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 information. Any ports that are currently 'up' are shown in green.

2. Click on the **Configure** icon inside the **Port Information** window to configure the port's speed, duplex mode, polarity, and aggregator status.



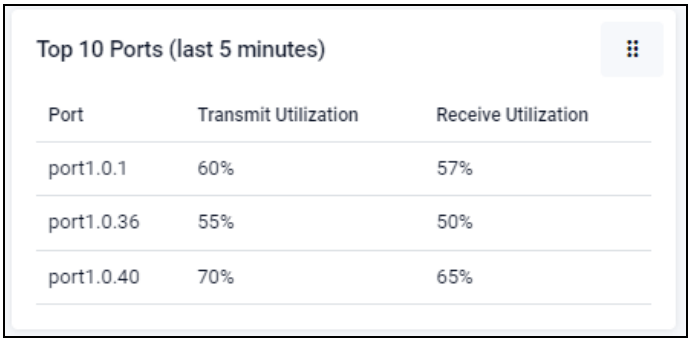
Port Traffic

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. Click on any port from the Port Status widget to display the port's traffic in this window.

Top 10 Ports

The Top 10 Ports widget displays the top 10 utilized ports on the switch (or stack of switches), over the last 5 minutes.

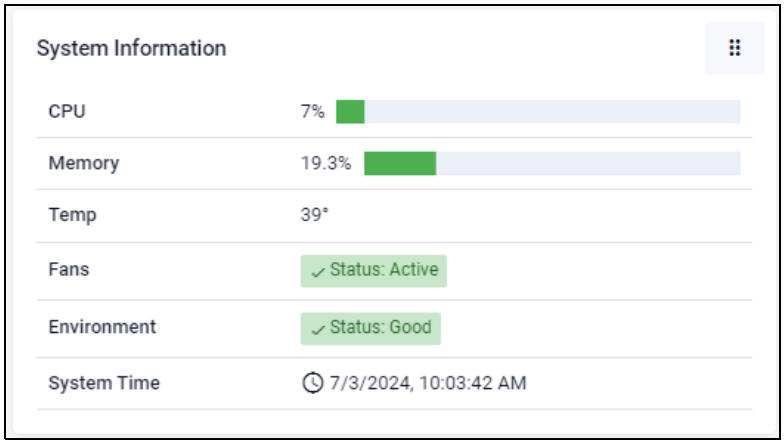


Port	Transmit Utilization	Receive Utilization
port1.0.1	60%	57%
port1.0.36	55%	50%
port1.0.40	70%	65%

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

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



Wireless Controller

You can use the Wireless Controller to configure TQR Series access points, as well as TQ Series access points. It is available on selected switches. From the wireless menu, you can view AWC clients and AP locations at a glance to monitor your connected client APs signal strength information and networks performance. The Device GUI displays heat maps for managed APs on the network map.

The Wireless Controller provides centralized visibility and control of wireless devices. Key features include:

Wireless Setup

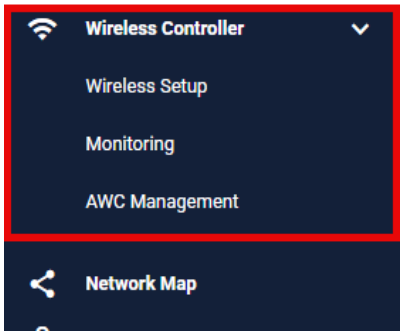
Quickly enable wireless management by assigning a management IP address. Use Auto-Setup to automatically discover and configure access points, or manually create networks and profiles through the Networks and Access Points tabs.

Monitoring

View the real-time status of wireless access points and connected clients. Easily identify unauthorized or failed APs, schedule immediate or delayed configuration or firmware updates, and reboot devices as needed.

AWC Management

Continuously analyze access point locations and signal strength with Autonomous Wave Control (AWC). It uses intelligent algorithms to automatically adjust wireless output and channel selection to deliver optimal performance and a better user experience.

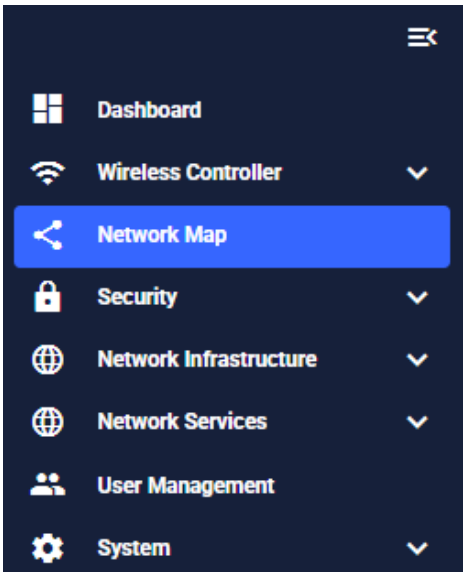


For more information about how to set up your device for use with the Wireless Controller see the Wireless Controller using the Device GUI.

The Network Map

The Network Map shows details of the devices connected to your 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, and the tasks you can perform there. The section ends with a look at configuring the network topology view and customizing node icon images.

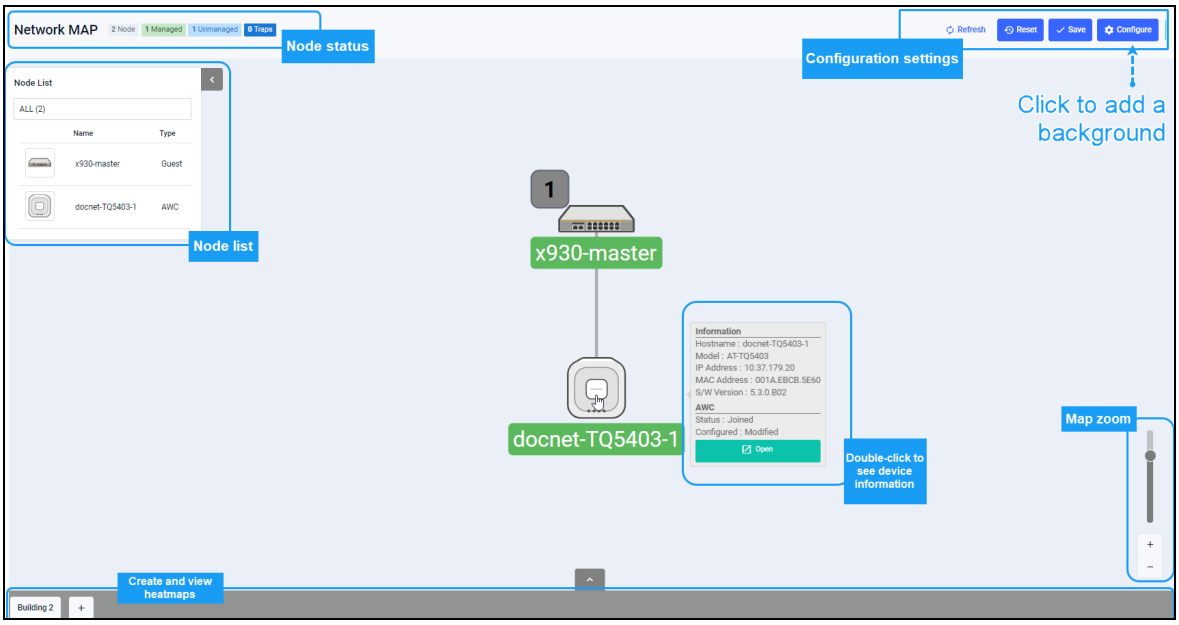
Note that the screenshots in this section show an x930 Series switch, but the functionality is the same for all devices that include a Network Map.

Network Map features

When you access the Network Map from your device's GUI, it shows a graphical display of your device and any wired connections associated with it.

From the **Network Map** page, you can:

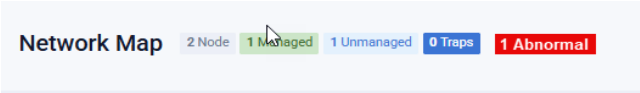
- Customize network icon images by clicking on them from the Node List.
- See a visual list of network nodes, including individual node details.
- Configure the topology view, SNMP, and Device Discovery settings.
- Create and view a Heatmap by clicking the **+** button in the footer.
- View stored heat maps.



Use the network map to check the status of a node at a glance.

Node status is indicated by the node title background color:

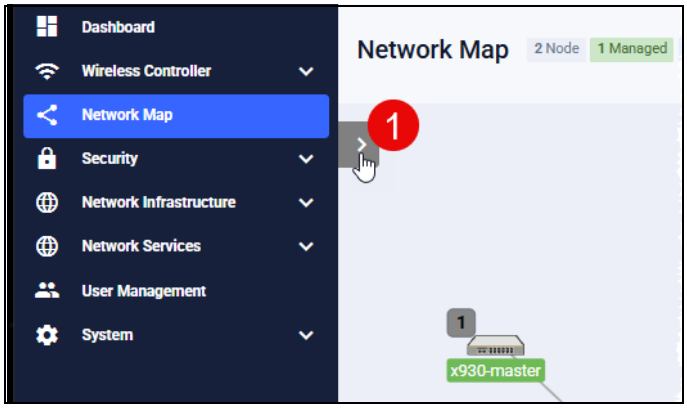
- Abnormal is red,
- managed is green,
- light blue indicates an unmanaged node.
- Dark blue indicates Traps



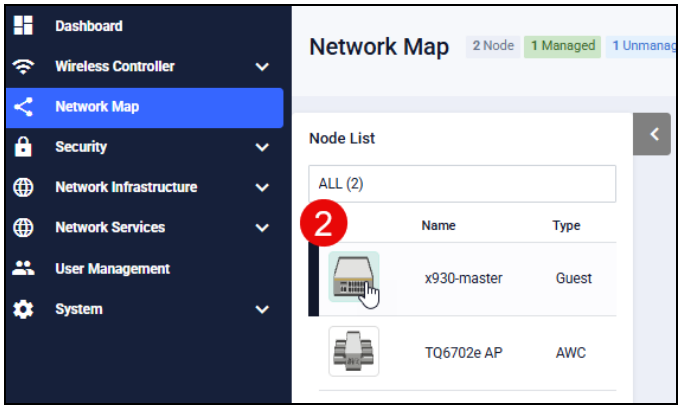
Viewing device information

The network topology map displays your main device and any connected devices. To view individual device information:

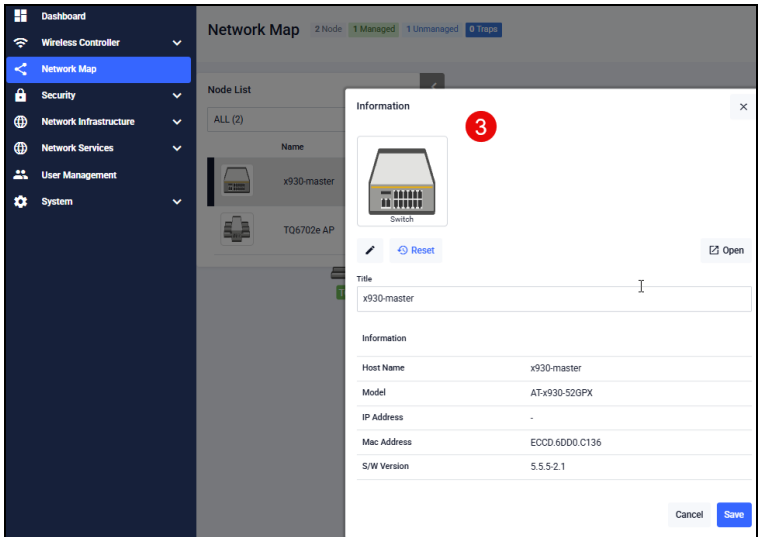
1. Expand the Node List.



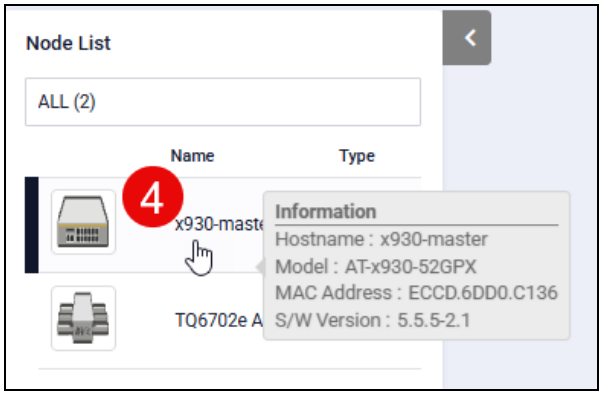
2. Clicking the device's icon in the Node List opens its Information window.



3. The Information window displays the device's Title, Hostname, Model, IP address, MAC address and software version. For information on changing images for device icons, see "Customizing device icons" on page 17



4. Clicking the device's Name or Type (instead of the icon) quickly displays the Hostname, Model, MAC address, and software version.



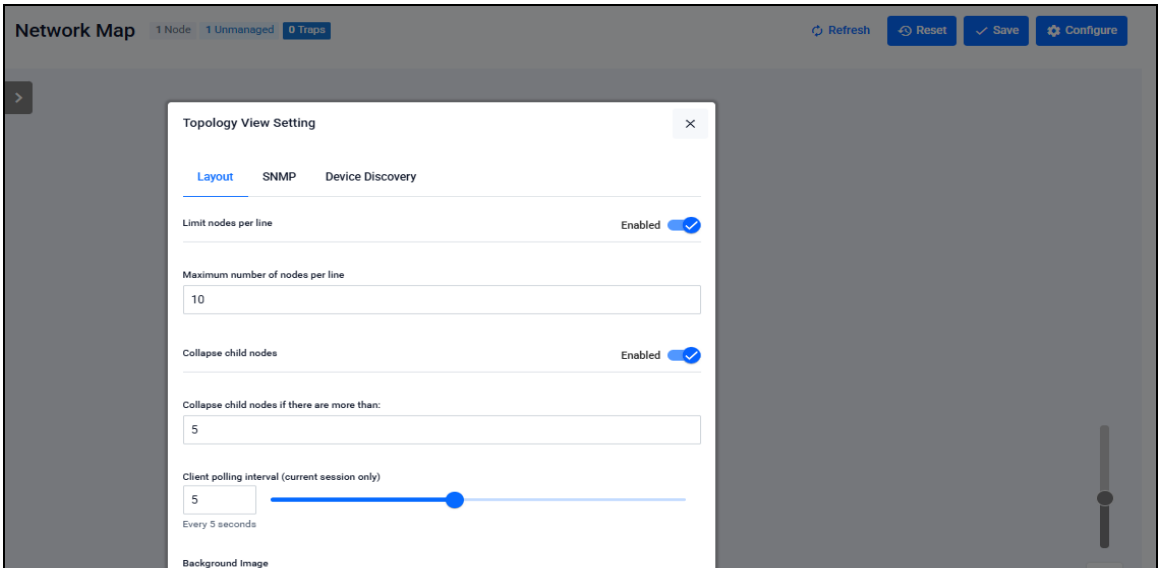
Device information from AMF nodes are gathered by SNMP and Device Discovery. This information is displayed in the Network map. For information about Device Discovery and SNMP, see the Device Discovery and Monitoring using SNMP Feature Overview and Configuration Guide.

Configuring the topology view

The Device GUI 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. From the Configure menu, you can configure a variety of settings related to the Network Map. These include layout settings, SNMP settings, and Device Discovery settings.

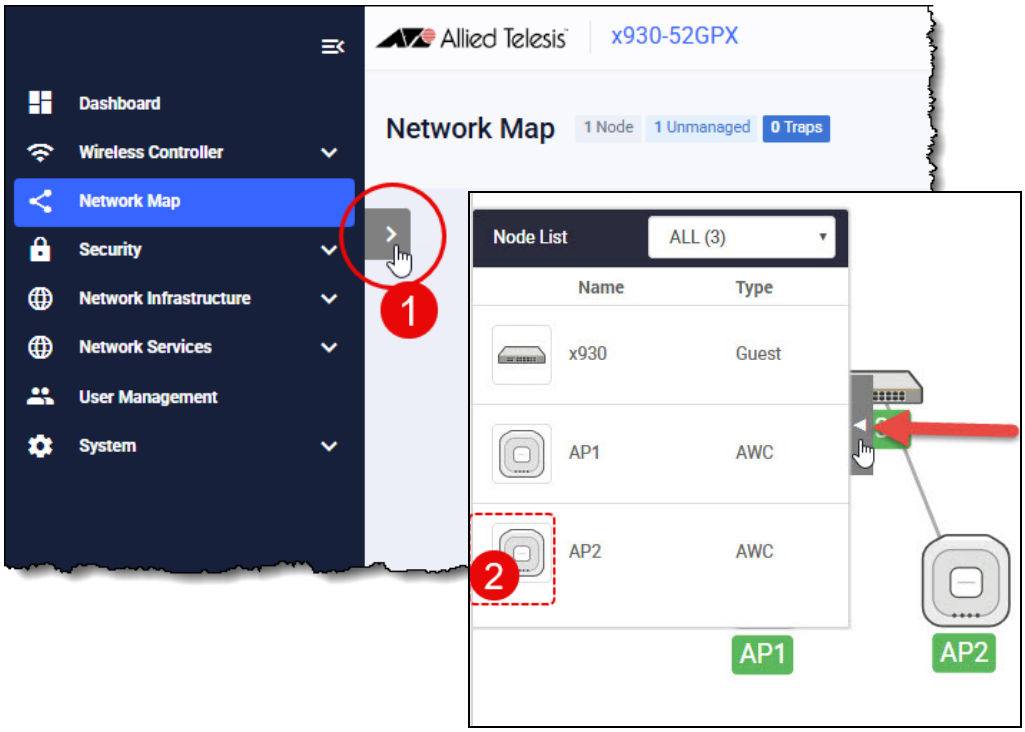
To change the topology view settings:

1. Click the **Configure** button in the top-right of the Network MAP page.
2. Select the tab you wish to view, this includes Layout, SNMP, or Device Discovery settings.
3. Click **Apply** to save changes.



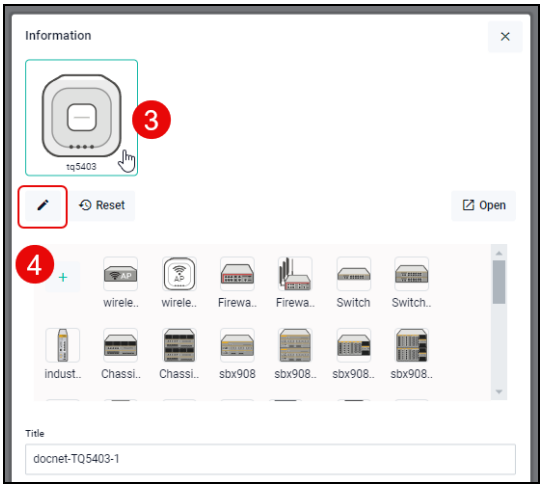
Customizing device icons

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.



To customize a device icon:

1. From the Network map, open the **Node List** by clicking the arrow.
2. Click on an image in the Node List to open its settings.
3. Click on the **device icon**, or the **edit pencil icon** to open the icon menu.

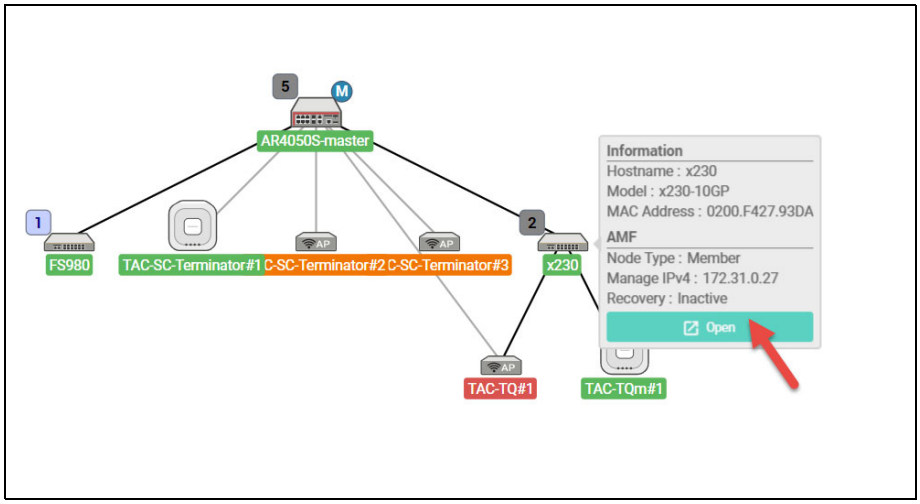


4. Select an image from the library or click the '+' sign to add a custom image.
5. Edit the device details as required.
6. Click **Save**.

Accessing the Device GUI from the Network map

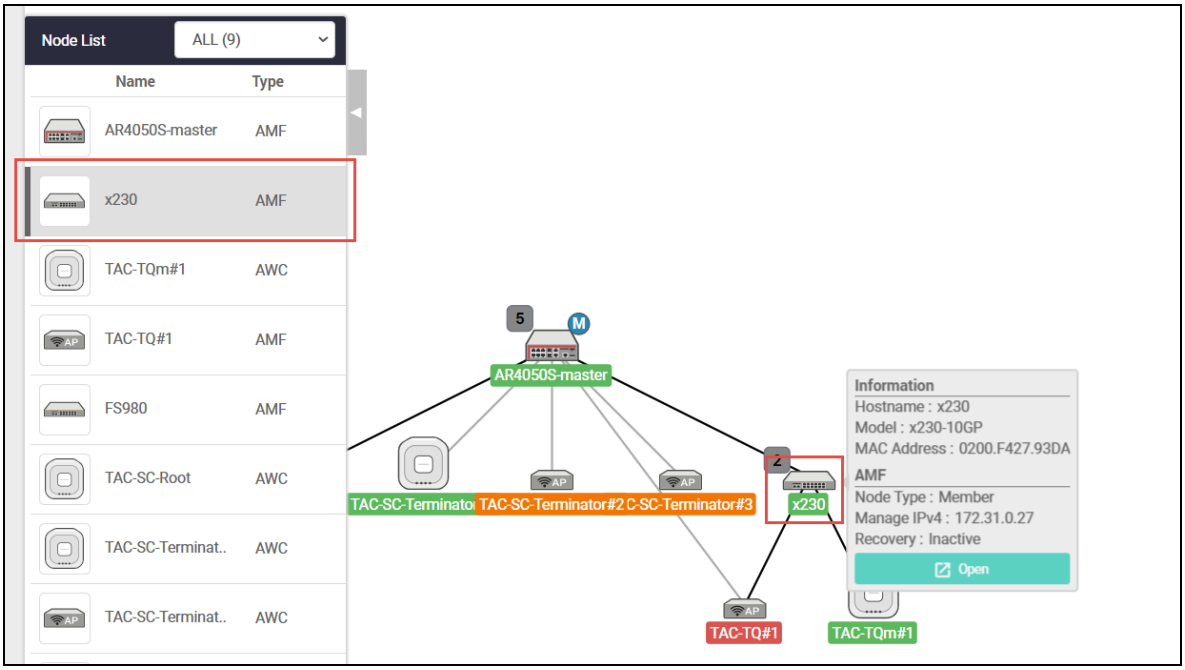
When you click a device's icon on the Network Map, its node information is displayed.

You can open another device's GUI instance from the Network Map by selecting the Open button in the **Information** panel. For example, in the screenshot below, an x230 is shown as a client device of an AR4050S. Clicking the **Open** button will launch the x230 switch's Device GUI in a new browser tab. You will be prompted to login to the device.



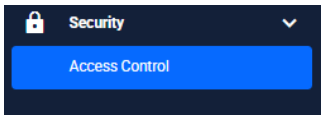
Locating a device in the network map

In a large network, it can be difficult to find a specific device. You can use the **Node List** to locate a device by simply clicking it. When selected, the device's Information details are displayed.

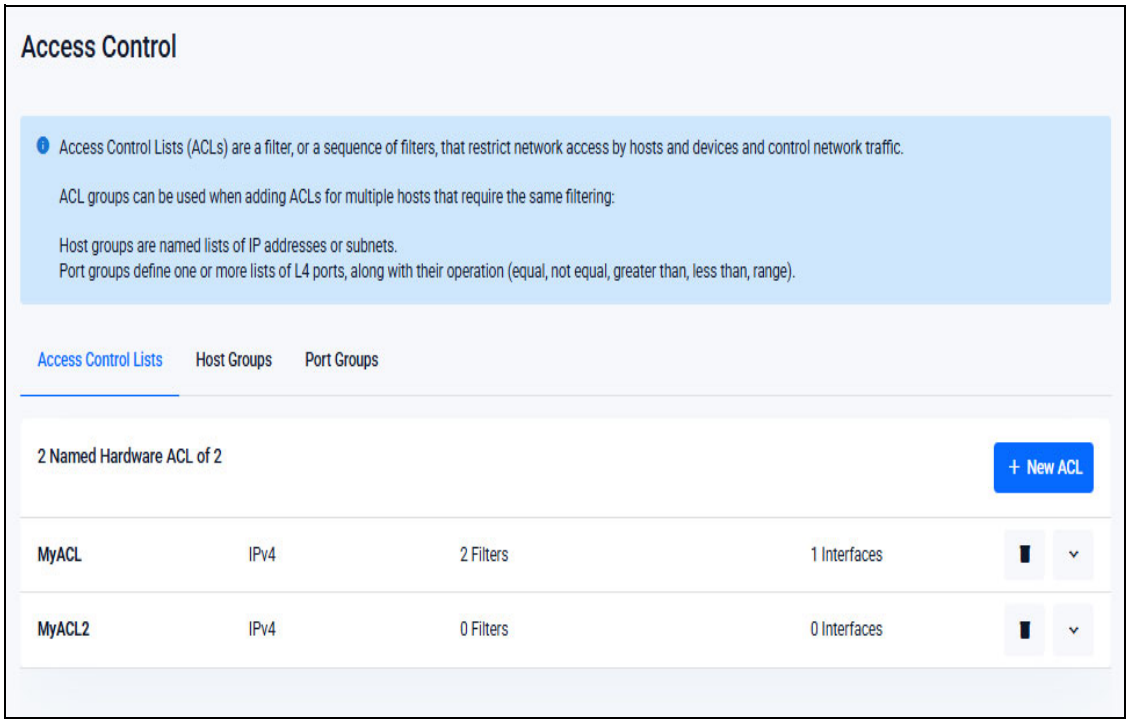


Security menu

You can 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.



Access Control



The Access Control page includes the ability to create Access Control Lists (ACLs). ACLs restrict network access for different host and device groups. You can use groups when adding ACLs for multiple hosts that require the same filtering. Group filtering is split into two group types:

- Host groups, which are named lists of IP addresses or subnets.
- Port groups, which define one or more lists of L4 ports, along with their operation.

Creating an Access Control List

To create an Access Control List, click the **+ New ACL** button from the Access Control page.You can configure the ACL to filter IPV4 or IPV6 traffic from the New ACL window.

To create a new ACL:

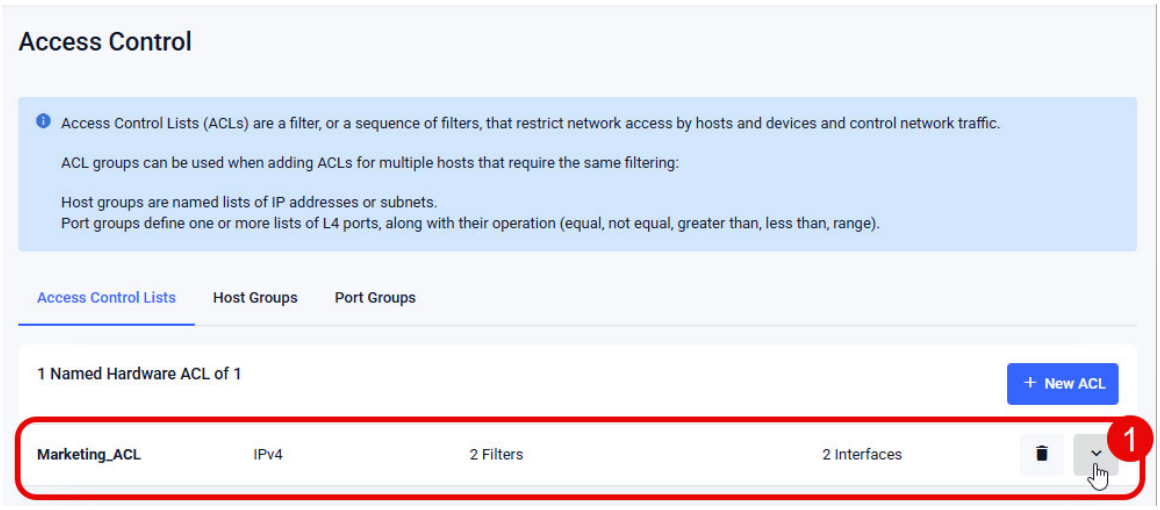
1. Click **+ New ACL**.
2. From the New ACL window, give the ACL a name.
3. Select whether the ACL will filter IPv4 or IPv6 traffic.
4. Click **Save**

Adding ACL Filters

The new ACL is listed on the Access Control page.

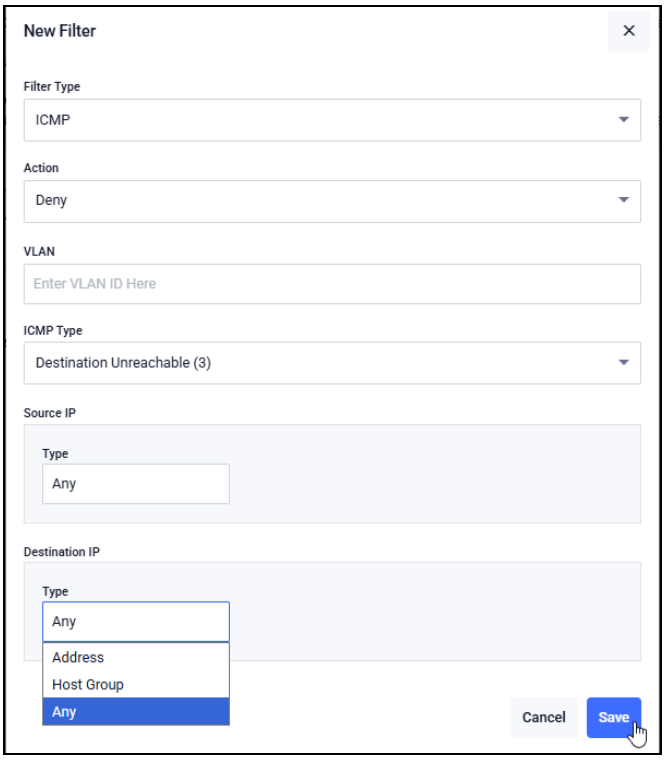
To add an ACL Filter:

1. Select and ACL, then click the arrow at right to expand the ACL.

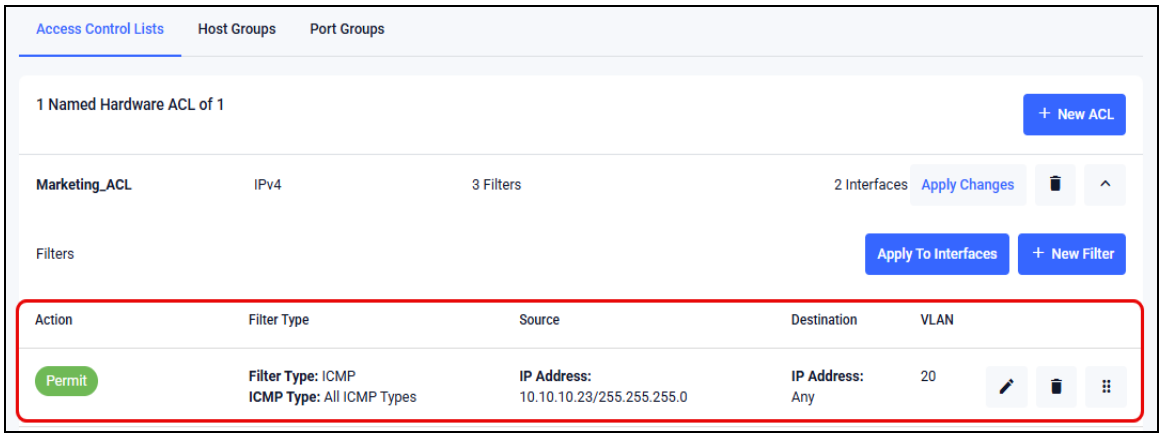


2. Click **+New Filter**.

3. 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 there are existing host groups or port groups, you can select them here.



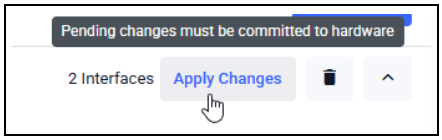
Your filter will now display on the Access Control Lists page. Add more filters to the ACL as needed.



4. Once you have finished adding filters to the ACL, click **Apply To Interfaces** to choose which switch ports to apply the ACL to.

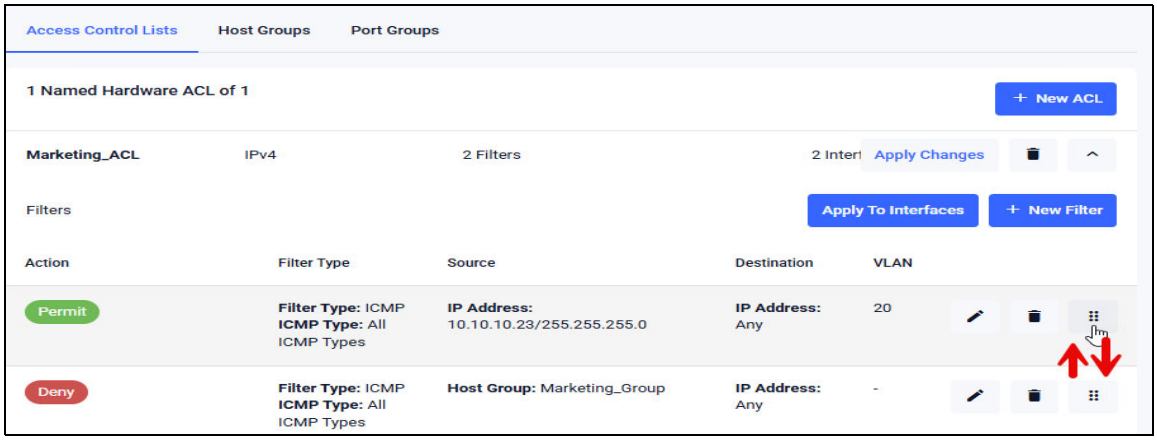
- Click on the arrow to see the port list.
- Select the port(s).
- The GUI lets you apply ACLs to switch ports and link aggregation groups.
- Once you have finished, click **Save**.

5. 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.



Re-ordering Filters

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



Host Groups and Port Groups

Host and port groups work together with filters, allowing a filter to match multiple IP addresses or port criteria at once. These groups appear in separate tables on the **Access Control** page.

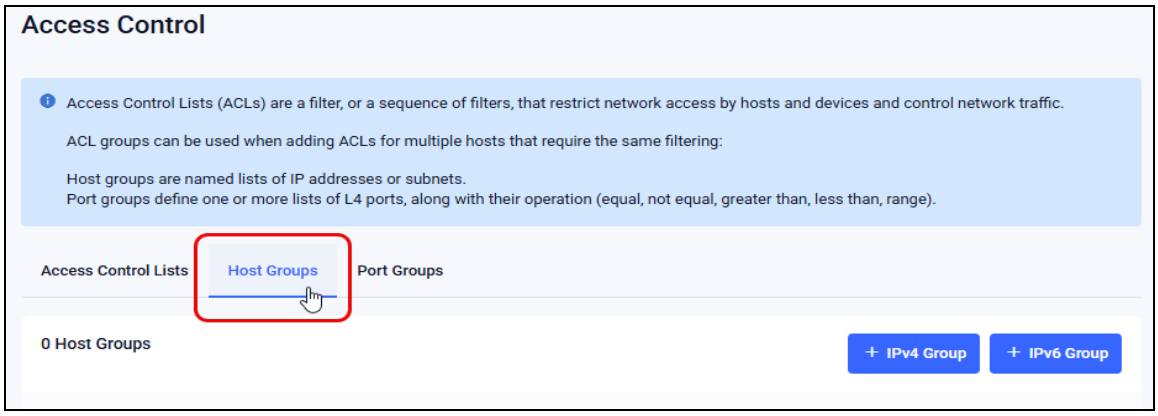
- You can assign meaningful names to each group, making it easier to understand what each filter is used for. For example, you could create a host group for each team in your company.
- If the same addresses or port numbers are used in multiple filters, host and port groups reduce maintenance. When those addresses or ports change, you only need to update the group instead of editing every filter.
- Port groups can also match ranges, such as all ports greater than a specific number. A single group can include a mix of different matching criteria, like this:

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

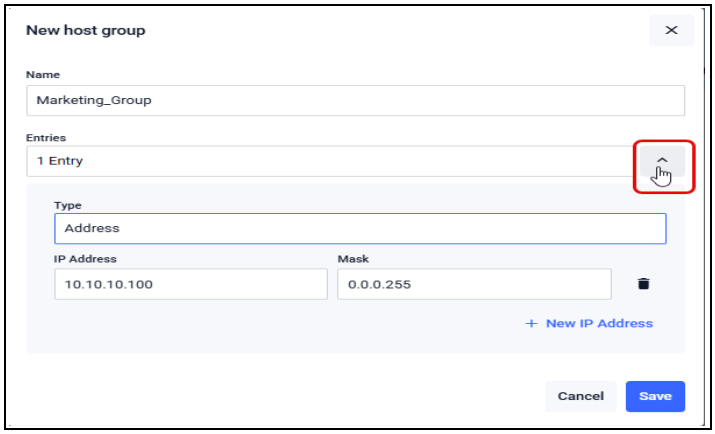
Creating a Host group

To create a host group for IP addresses:

1. Navigate to the Host Groups tab.
2. Select either **+ IPv4 Group** or **+ IPv6 Group** to create a new host group.



3. Give your group a name and expand the **Entries** field. Add IP address entries to the Host group by clicking **+ New IP Address**, adding a new entry for each address.



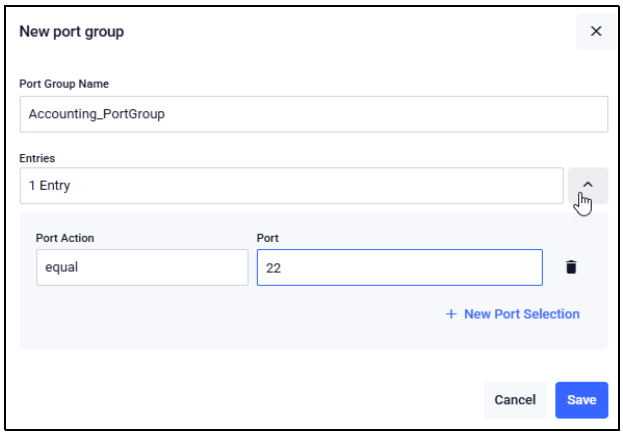
Port groups

From the Port Groups tab, you can create a port group to group TCP or UDP ports.

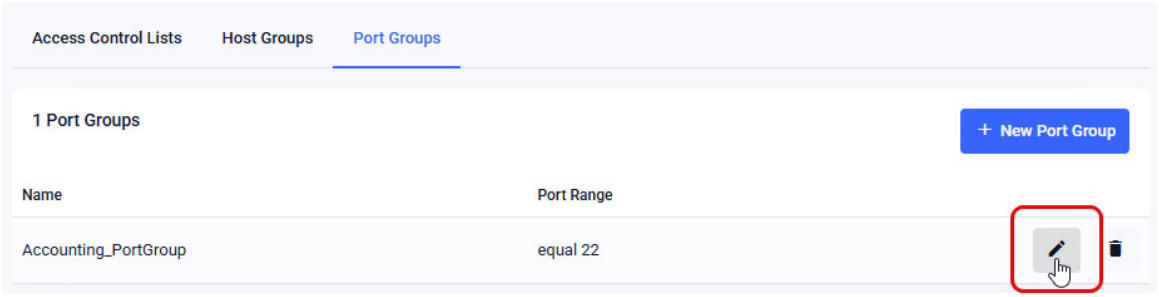
1. Click **+ New Port Group** to create a new group.

2. Give your group a name and expand the **Entries** field. Click **+ New Port Selection** and create the desired port entries.

3. Click **Save**.

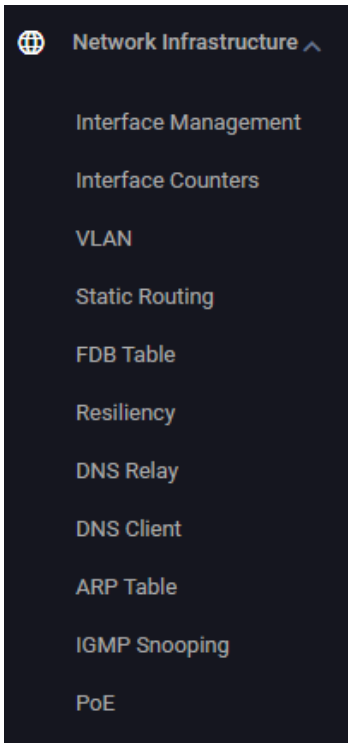


If you need to make changes, click the edit button to open the **Edit Port Group** window.



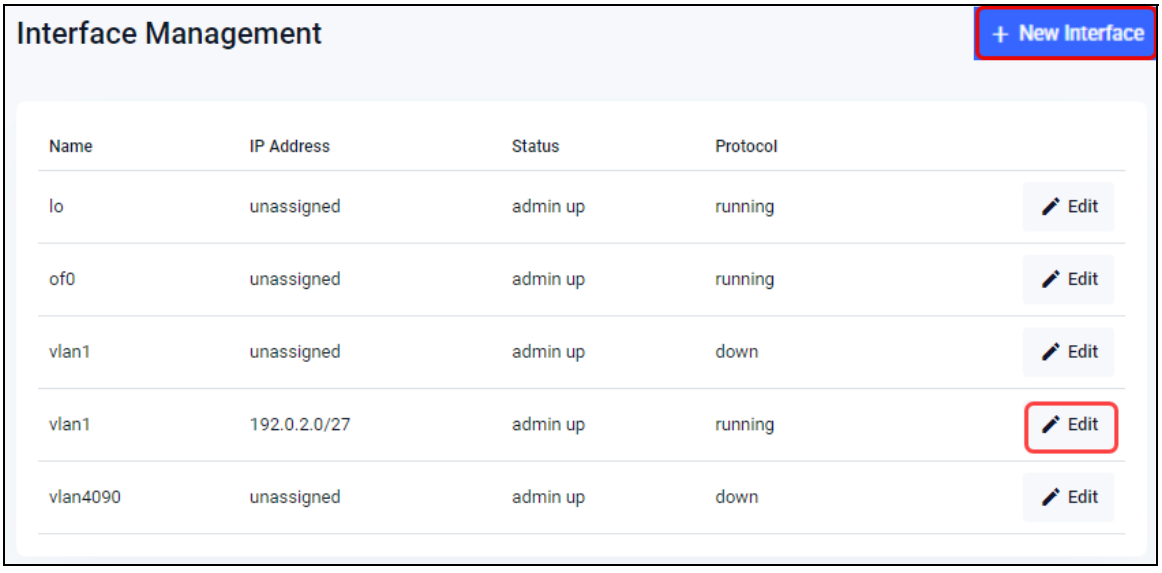
Network Infrastructure menu

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



These are 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.

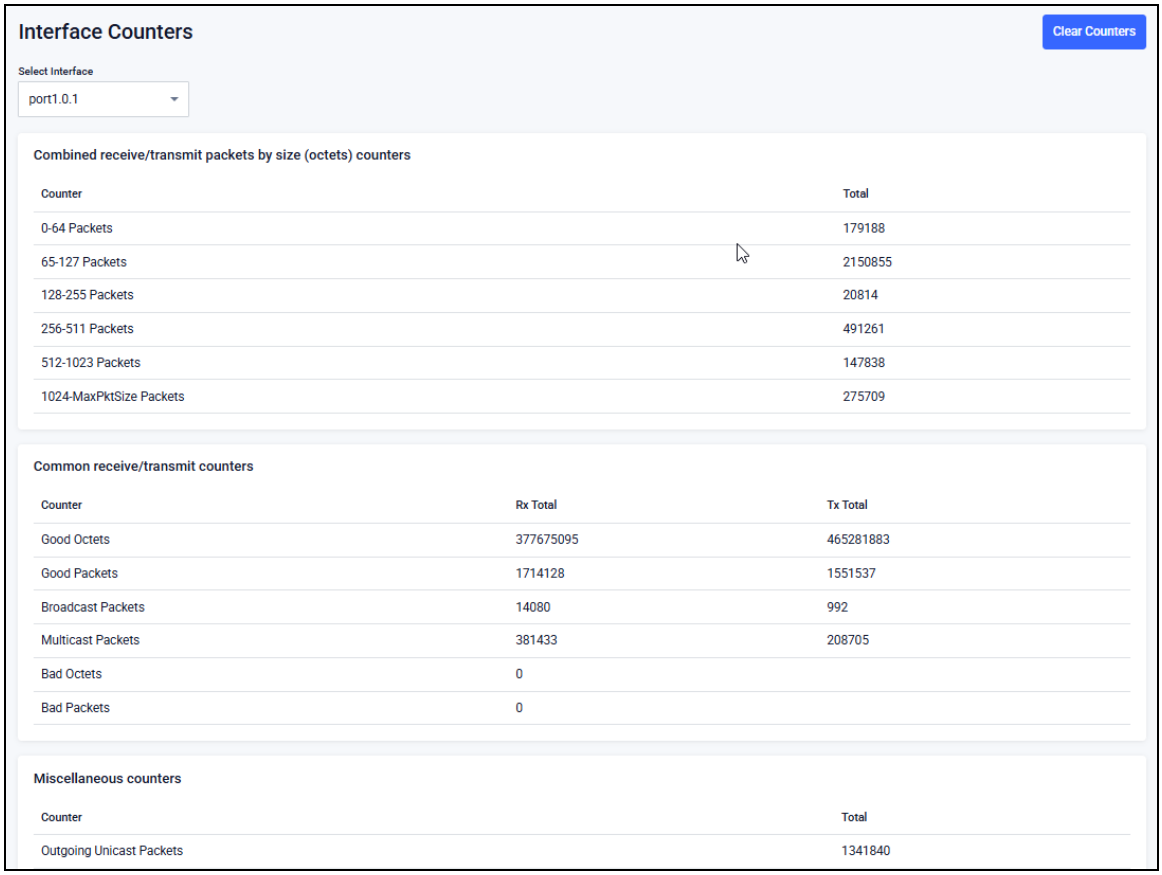
Note: Eth0 is the Ethernet link from your device to the Device GUI. If you decide to change the IP address associated from DHCP to a fixed IP address, you must reload the GUI with the new fixed address.

Interface Counters

To use this feature:

- Choose an interface from **Select Interface** at the top of the screen - e.g. port1.0.1
- View the corresponding port counters in the tables:
  - **Combined receive/transmit**
  - **Common receive/transmit**
  - **Miscellaneous**

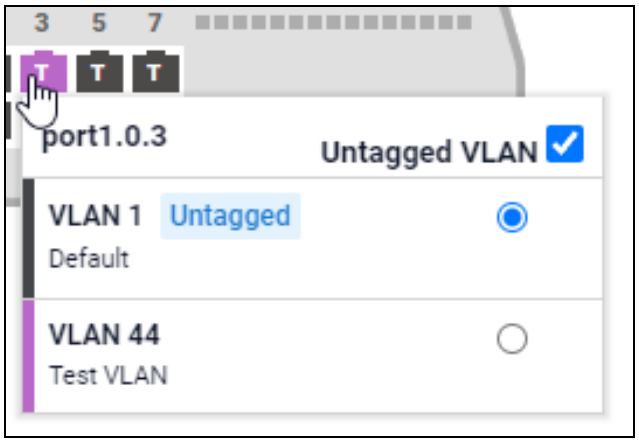
  Counters are updated live (every 3 seconds) while viewing page.
- You can also clear counters for the selected port.
- Jumbo frames are supported dynamically. In other words, if there are counts they will be displayed.



VLAN

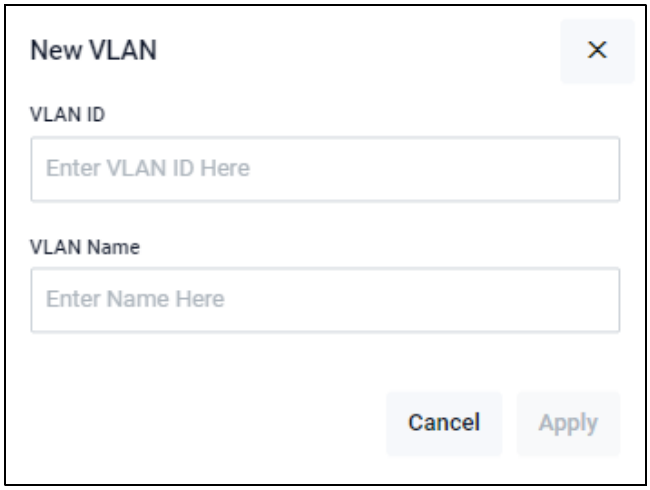
The VLAN page shows the VLANs currently configured on the switch. From here, you can easily create, edit, and delete VLANs.

Mouse-over a port to view VLANs associated with the port.



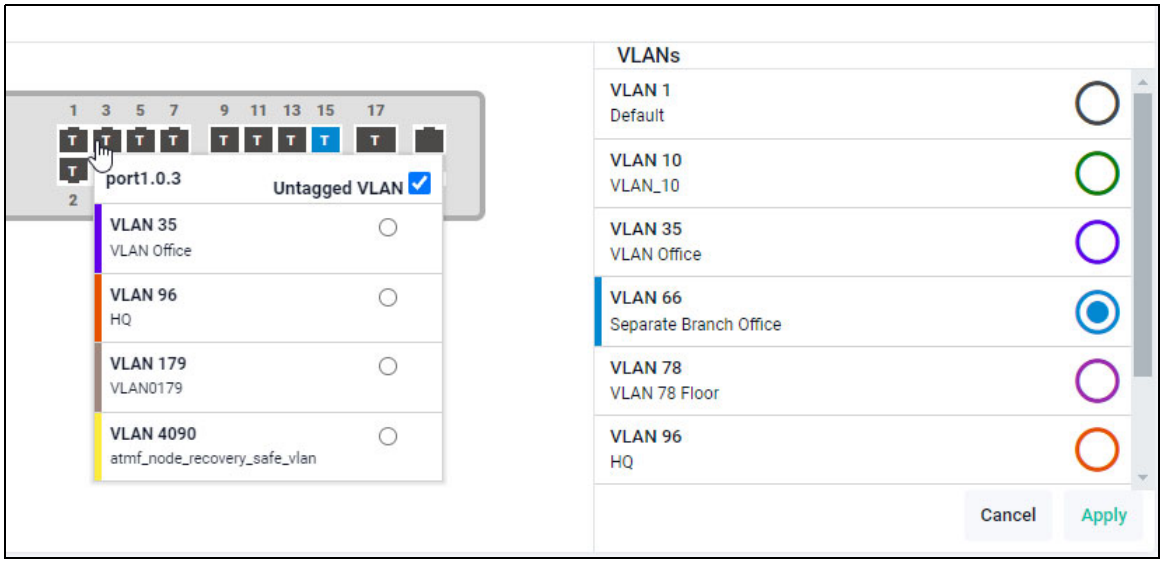
Creating a VLAN:

- Click the **+New VLAN** button to create a new VLAN.
- Enter a **VLAN ID** and **VLAN Name**.



- Click **Apply** to add the VLAN to the list.

New VLANs are added to the VLAN list on the right side of the window. VLANs are automatically assigned a color. When you select a VLAN from the list, the ports that belong to that VLAN are updated on the switch graphic using the color assigned to that VLAN.



In the example above, we have selected VLAN 66, which is assigned the color Blue. When we select VLAN 66, the ports that belong to VLAN 66 are also colored blue in the switch graphic.

To add a port 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.

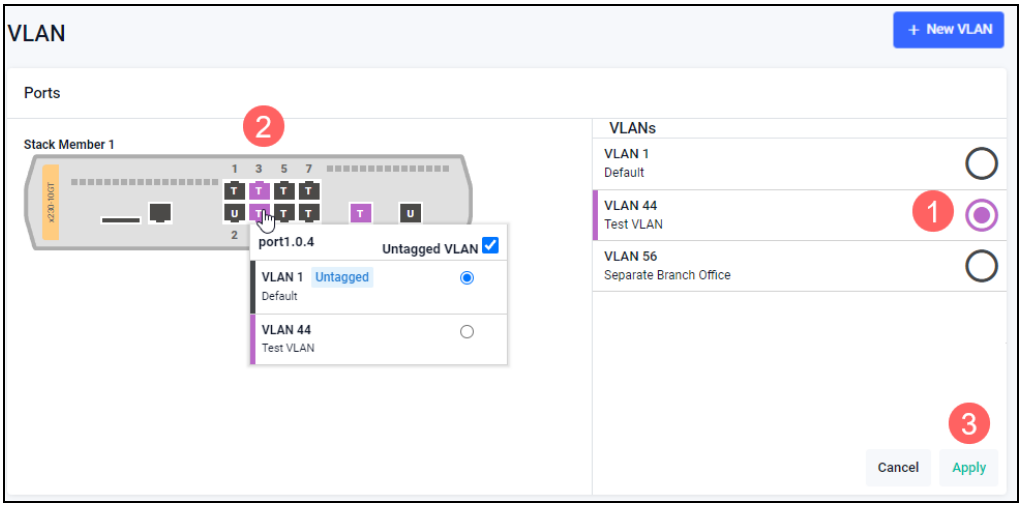
Configuring native VLANs

You can use the VLAN page 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.

- Native VLANs only apply to switchports in trunk mode.
- Untagged packets received on the switchport are placed into the native VLAN.
- You can assign different native VLANs to individual switchports on a single device.
- Only one native VLAN can exist per switchport.
- Packets leaving a switchport on the native VLAN are not tagged.

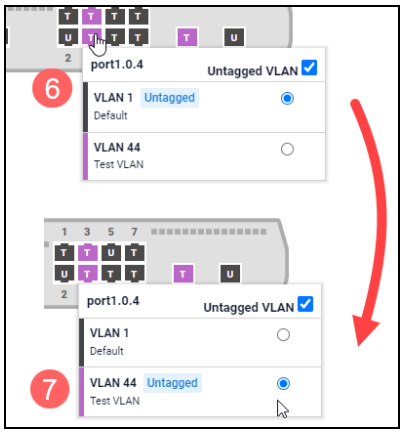
The following procedure first uses the VLAN map to put the switchport into trunk mode, then sets the correct native VLAN:

1. Select the VLAN you wish to add from the VLANs list,
   OR
   Click **+ New VLAN** to create a new VLAN.
2. Once you have a VLAN created, select the VLAN from the VLAN list.
3. Click on a port to assign the VLAN to the switchport.



4. Click on the **U** on the switchport until it takes on the color of your selected VLAN, click again to change the port to a **T** (for Trunk).
5. Click **Apply** to save your changes.
6. Hover over the switchport you just configured. A window will appear, showing the current VLANs assigned to that port. You can change the native VLAN from this list by clicking the radio button next to the VLAN.

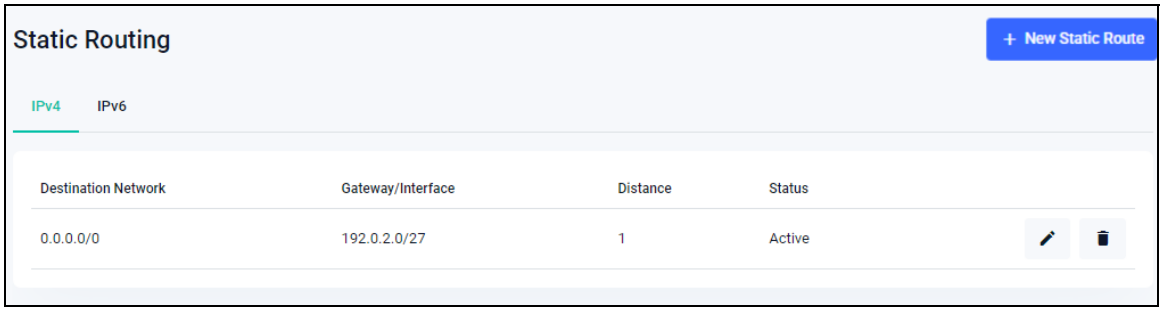
7. The new native VLAN will have an **Untagged** label next to its VID.



8. Click **Apply** to confirm your changes.

Static Routing

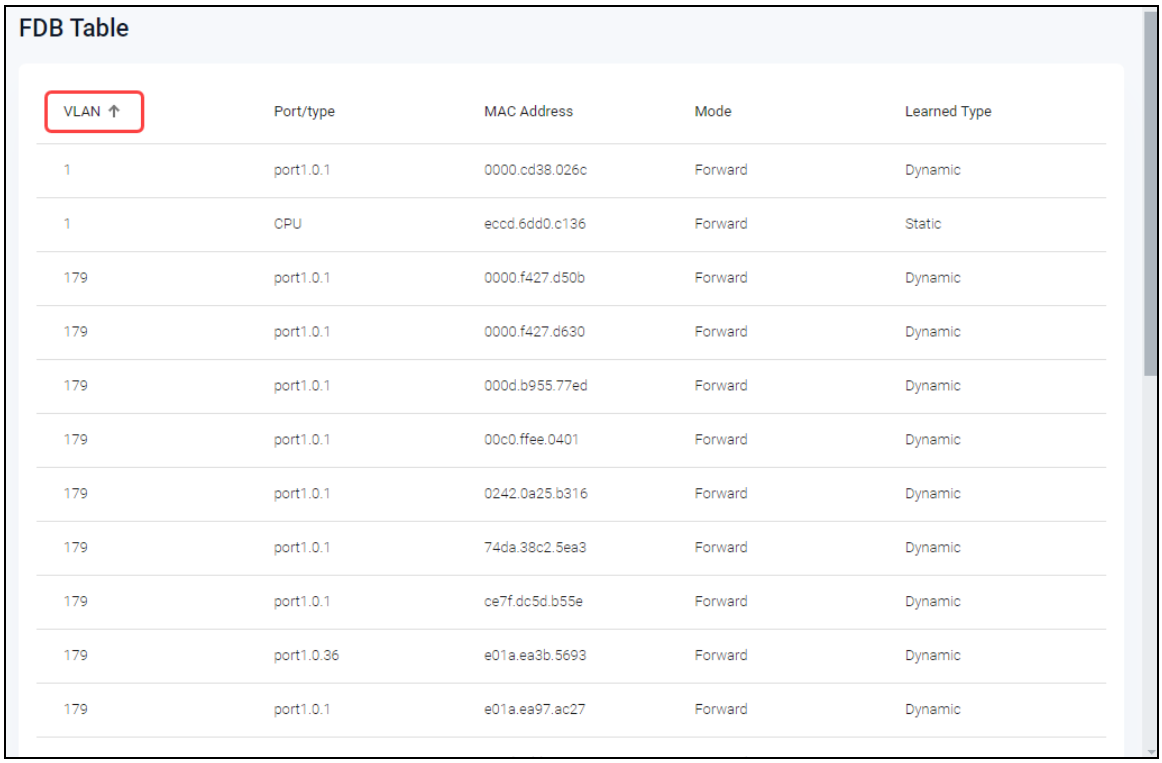
The Static Routing page displays the static routes currently configured on the switch. From here you can add, edit, and delete static IPv4 and IPv6 routes.



To add a new Static Route, click **+ New Static Route**.

Forwarding Database (FDB) Table

The FDB (Forwarding Database) table stores learned MAC addresses along with the ports on which each MAC address was detected.



Hover your mouse over a column header and click to change the sort criteria to either ascending or descending.

Resiliency

The **Resiliency** page provides a centralized view of the device's loop-prevention and rapid-recovery mechanisms. These features ensure continuous network operation by preventing broadcast storms, eliminating switching loops, and enabling fast failover when links or paths go down.

You can switch between STP and EPSR views by clicking their headings at the top of the page.

- Spanning Tree Protocol (**STP**) is a networking protocol used on switches to prevent loops in a Layer 2 network. It works by detecting redundant paths and temporarily blocking some of them so that only one active path exists between any two devices. This ensures data doesn't endlessly loop around the network, keeping it stable and preventing broadcast storms.
- Selecting the **EPSR** heading displays configuration and status for Ethernet Protection Switching Rings, commonly used in metro Ethernet and high-availability ring topologies.

The Resiliency page allows you to:

- Confirm the device is participating correctly in loop-prevention protocols
- Quickly diagnose network topology changes or link failures
- Validate configurations after deploying or modifying redundancy features

DNS Relay

The DNS Relay page displays DNS Relay settings. To configure DNS Relay on your device, click the **Configure** button.

Enabling DNS Relay on your device provides the capability for it to act as a local virtual DNS server. You device can then service DNS lookup requests sent to it from local hosts.

When your device receives a DNS query from a client, the device will attempt to match the request with entries in its cache. If the device does not have this address cached, it forwards the request upwards through the hierarchy of DNS servers for resolution. When acting as a DNS Relay, the device will relay (pass on) the requests to an external, or upstream, DNS server.

Retry

Sets the number of times a device will retry to forward DNS queries <0-100>.

Timeout

Sets the number of seconds to wait for a response <0-3600>.

Deadtime

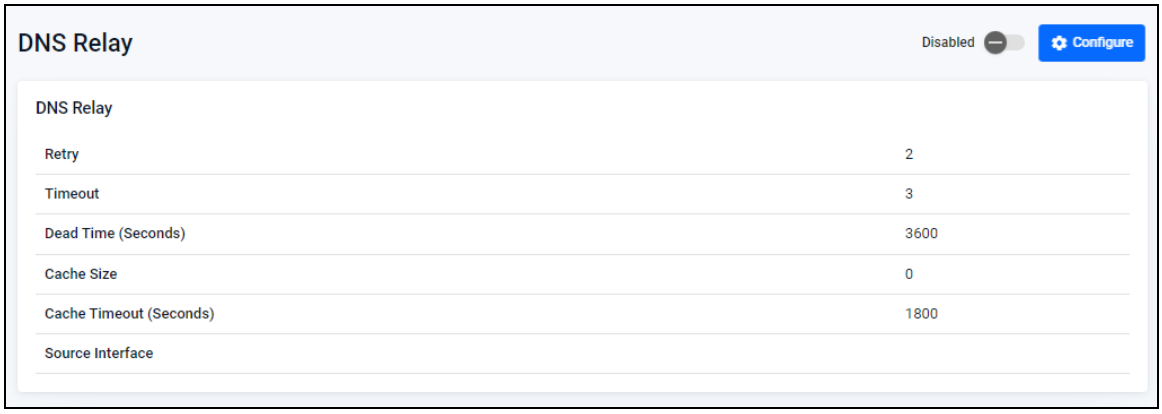
Sets the DNS forwarding dead-time period in seconds <60-43200>

Cache Size and timeout

Sets the DNS Relay name resolver cache size and lifetime, cache size <0-1000>, timeout <603600>

Source Interface

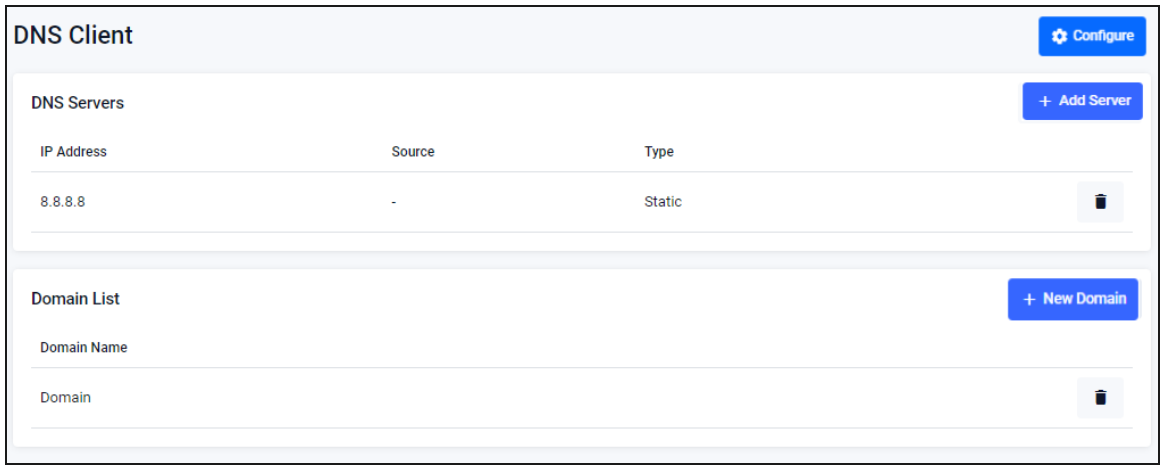
Sets the interface to use for forwarding and receiving DNS queries <interface-name>.



For more information on the Domain Name System, see the Domain Name System (DNS) for AlliedWare Plus Switches.

DNS Client

The DNS Client page shows the DNS servers configured on the device, and allows you to add new DNS servers and domains.



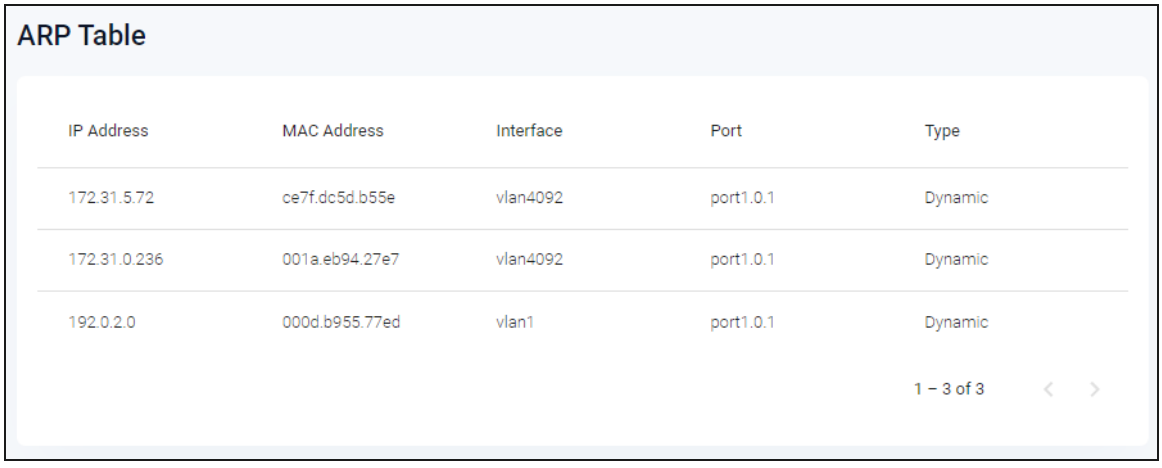
- The **DNS Servers** table shows the **Source** column, which is the source that the DNS server's IP is learned from.
- The **Domain List** category is visible under the DNS Servers table.

For more information on the Domain Name System, see the Domain Name System (DNS) Feature Overview and Configuration Guide.

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. **(READ ONLY page)**



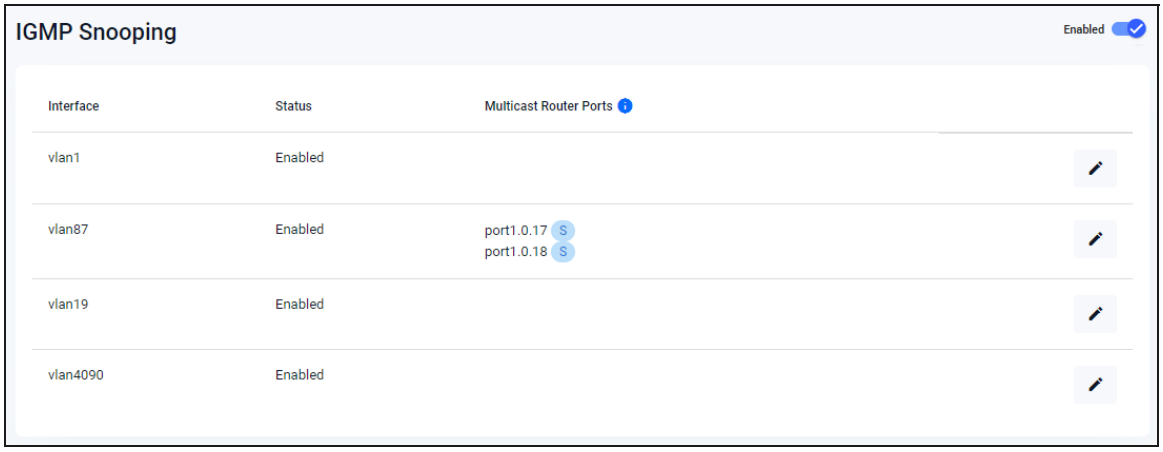
IGMP Snooping

IGMP Snooping is a feature in network switches that helps send multicast traffic only to the devices that actually want it. With IGMP Snooping turned on, the switch “listens” to IGMP messages and learns which devices joined the multicast group.

Then it forwards the multicast traffic only to those specific ports, not the whole network.

You can statically configure an interface as an IGMP Snooping multicast-router interface—meaning an interface that connects toward a multicast router or another IGMP querier. The interface can be a physical device port (for example, port1.0.2), a static channel group (such as sa3), or a dynamic LACP channel group (such as 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 the **Edit** icon, then in the **Edit Interface** window:

- Click the **Multicast Router Ports** arrow to access the port list.
- 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.

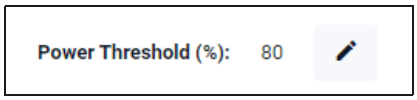
View detailed port information

If the device supports PoE, you can view detailed PoE port information. In the example shown, the device has 380 W of nominal power available, with 90 W allocated across its 48 ports. The two active ports are currently using 20 W, and the power threshold is set to the default 80%.

Configure the PoE power threshold for a device

Use the power threshold settings to trigger an alert when a device's total PoE power consumption exceeds a configured limit. This threshold determines when the switch will report that the combined power usage of all Powered Devices (PDs) has reached a critical level relative to its nominal power rating. The threshold is set as a percentage of the total available power

To change the power threshold setting, click on the **Edit** icon next to **Power Threshold** (%).



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

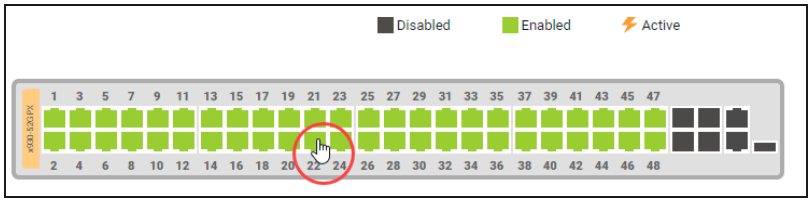
Configure the power priority per interface

If the Powered Devices (PDs) connected to a switch require more power than the switch can supply, the switch will deny power to some ports. Port prioritization determines which ports continue receiving power when total PD demand exceeds the switch's available power—for example, if one of the power supplies fails. The switch removes power based on priority: ports set to Low lose power first, followed by High, and finally Critical.

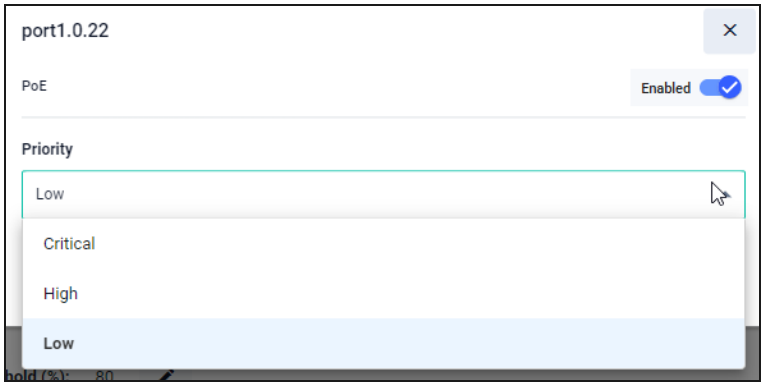
If there is not enough power to support all the ports set for a given priority level, power is provided to the ports based on the switch port number.

To set 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.

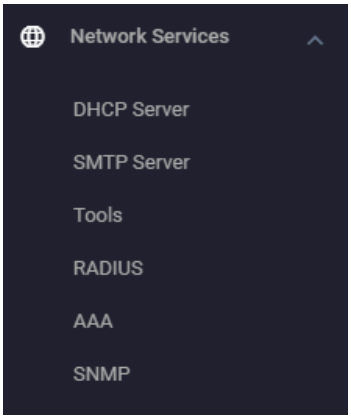
Low: The lowest priority level. This is the default setting. Ports set to Low level only receive power if all the ports assigned to the other two levels are already receiving power.

- Click **Apply**.

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

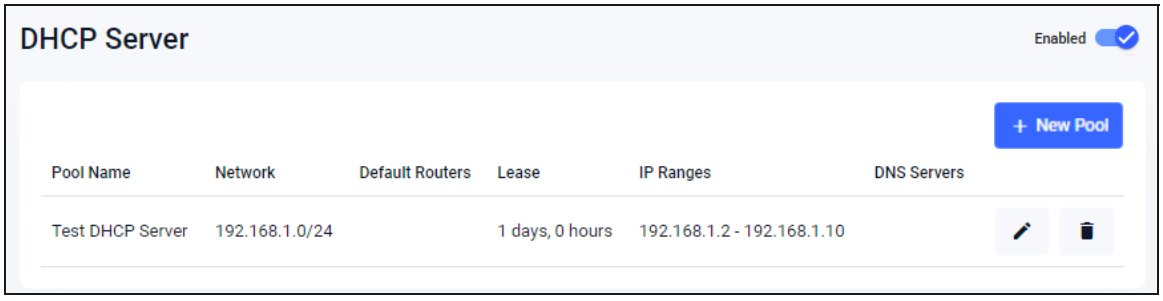
Network Services menu

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



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.

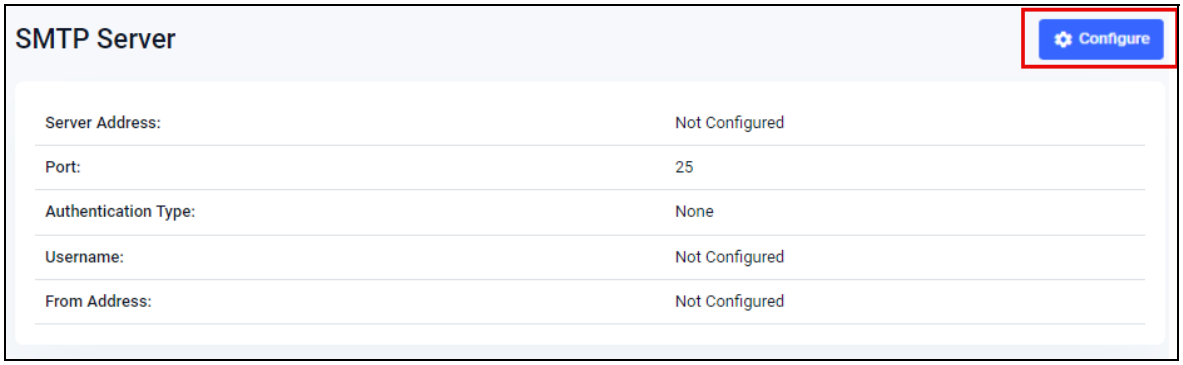
1. Use the Enable/Disable toggle at the top right of the page to enable DHCP server functionality.
2. Click **+New Pool** to add a new pool.

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

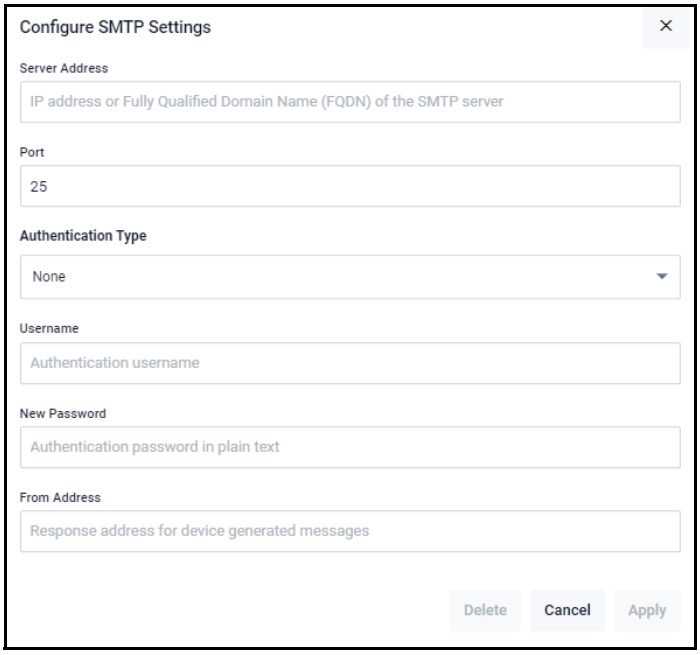
   - Click **Edit** to edit an existing pool.
   - Click **Delete** to remove an existing pool.

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**.

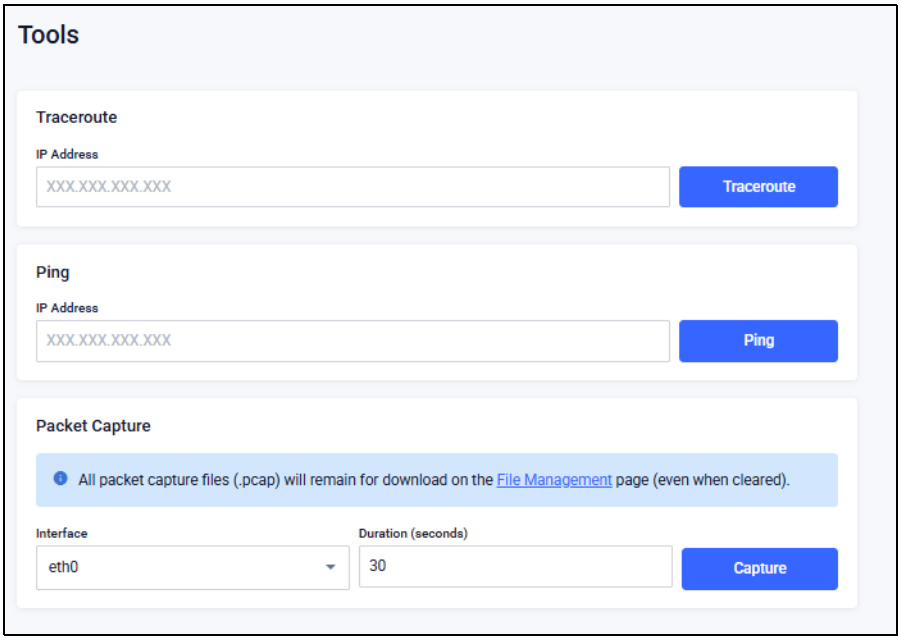


- Type in the **server address** and **port number**. The other fields are not mandatory.
- Click **Apply**.

To add email filters, see "Logging" on page 56.

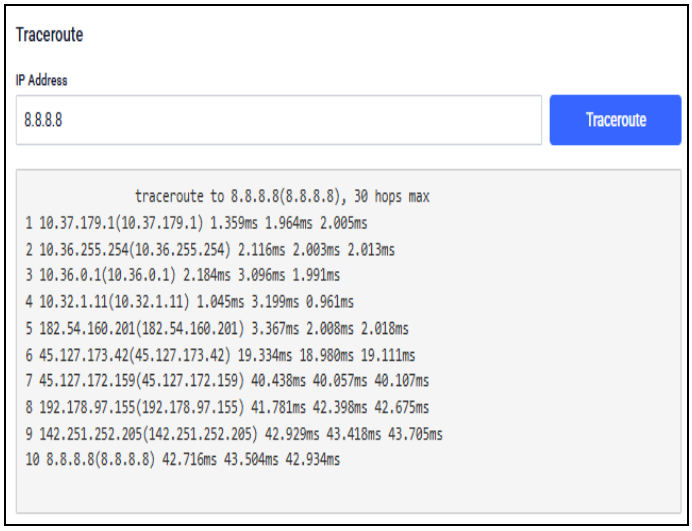
Tools

The Tools menu provides Ping and Traceroute which are useful for checking network connectivity and remote site reachability, plus the Packet Capture feature.



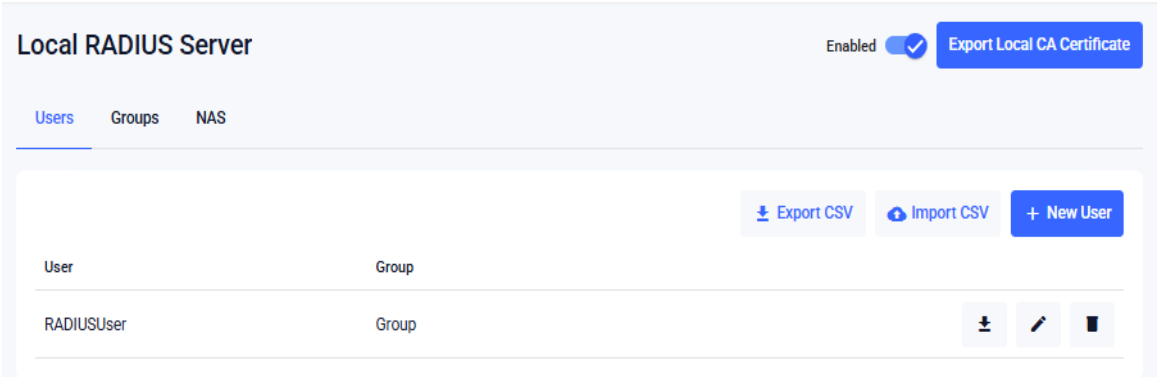
For example, here is a Ping of the IP address 8.8.8.8 (the Google public DNS service), and the results of 5 ICMP packets sent and received.

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 page 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

The AAA (Authentication, Authorization, and Accounting) page provides a central location for configuring how the device authenticates users and, if required, external authentication servers. This page is used to define the authentication methods applied to device logins and privileged (“enable”) access, as well as to manage authentication server entries and groups.

AlliedWare Plus enables you to specify three different types of device authentication: 802.1X-authentication, Web-authentication, and MAC-authentication. You can use these forms of device authentication separately or in combination, creating a powerful authentication feature set.

- 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.

Service Method Lists

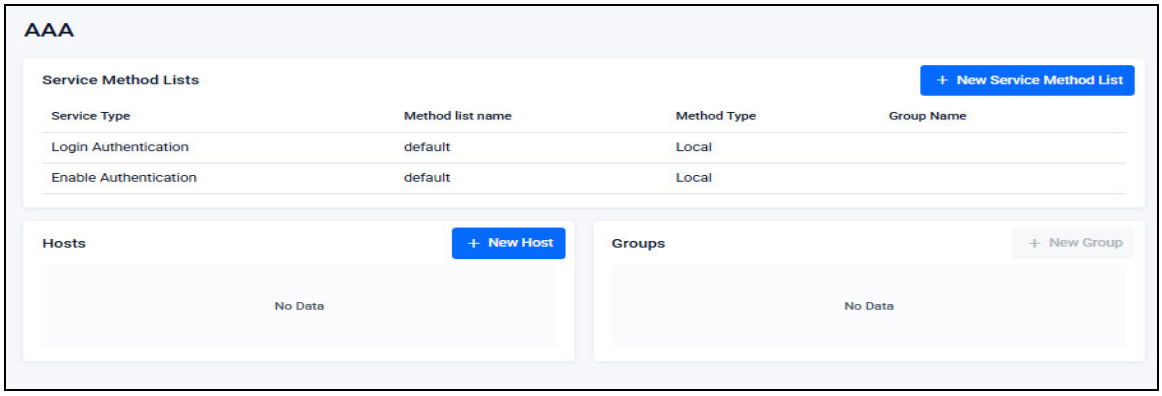
This section shows the authentication methods assigned to each service type. Each method list defines how the device performs authentication—for example, using Local accounts or external servers. Click **+New Service Method List** to create custom authentication sequences.

Hosts

The Hosts panel is where you add external authentication servers (e.g., RADIUS or TACACS+). Click New Host to define server details. Hosts can be assigned to method lists or grouped for redundancy.

Groups

The Groups panel lets you create server groups made of one or more authentication servers. Groups can be linked to method lists to control which servers are used for authentication.



For more detailed information on AAA, see the AAA and Port Authentication Feature Overview and Configuration Guide.

SNMP

In simple terms, when you **Enable SNMP Traps** you are turning on alerts that the device can automatically send when something important happens.

- SNMP is a system that lets network devices report their status.
- Traps are automatic notifications sent from the device to a monitoring system.
- When you enable SNMP traps, the device will send alerts—like “a port went down” or “power usage is too high”—so your monitoring software can catch problems quickly.

To configure SNMP and SNMP traps

This process guides you through configuring SNMP settings on the device, including specifying identification details, defining SNMP views to control access to MIB (Management Information Base) data, and enabling the SNMP traps you want the system to send. It ensures that your device provides the right level of SNMP visibility and notifications for effective network monitoring.

1. Click **Configure** to add a Source Interface.
2. Click **Apply** to save the Location and Contact details. These details will subsequently appear on the **About** > **System Information** page.
3. Enable specific **SNMP Traps** using the Trap Status Enabled/Disabled toggle buttons.
4. Add **SNMP Views** by clicking **+ New View**. The button is located at the bottom of the page.

SNMP Views

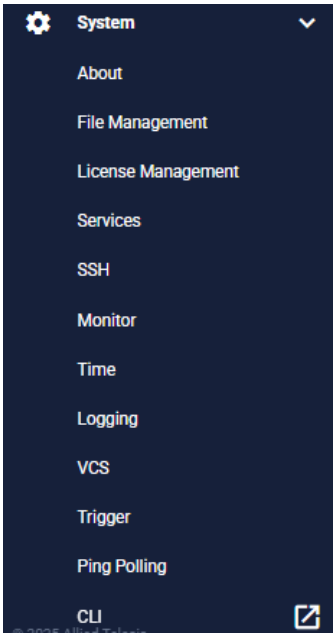
SNMP Views define which parts of the MIB an SNMP group or user is allowed to see or modify.

User Management menu

The User Management menu allows you to add new users and configure their passwords and privilege levels. Levels 1–14 provide limited access, while level 15 provides full access

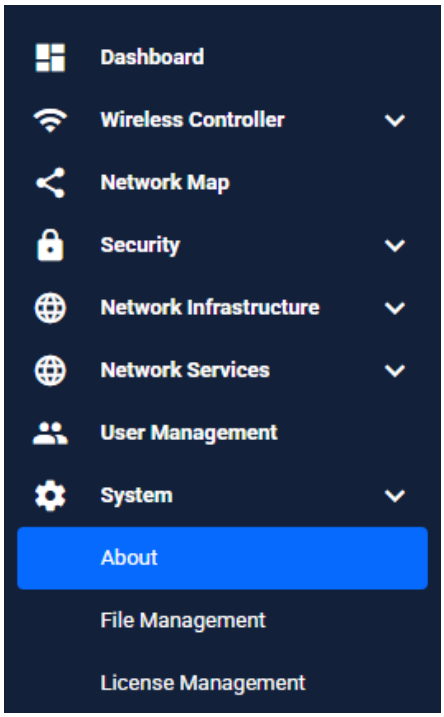
System menu

The System menu provides access to information about your device, file management, license management, services, SSH, time, logging, VCS, trigger settings, and the CLI.



About

The **About** page provides details of your switch, or switches if stacked.



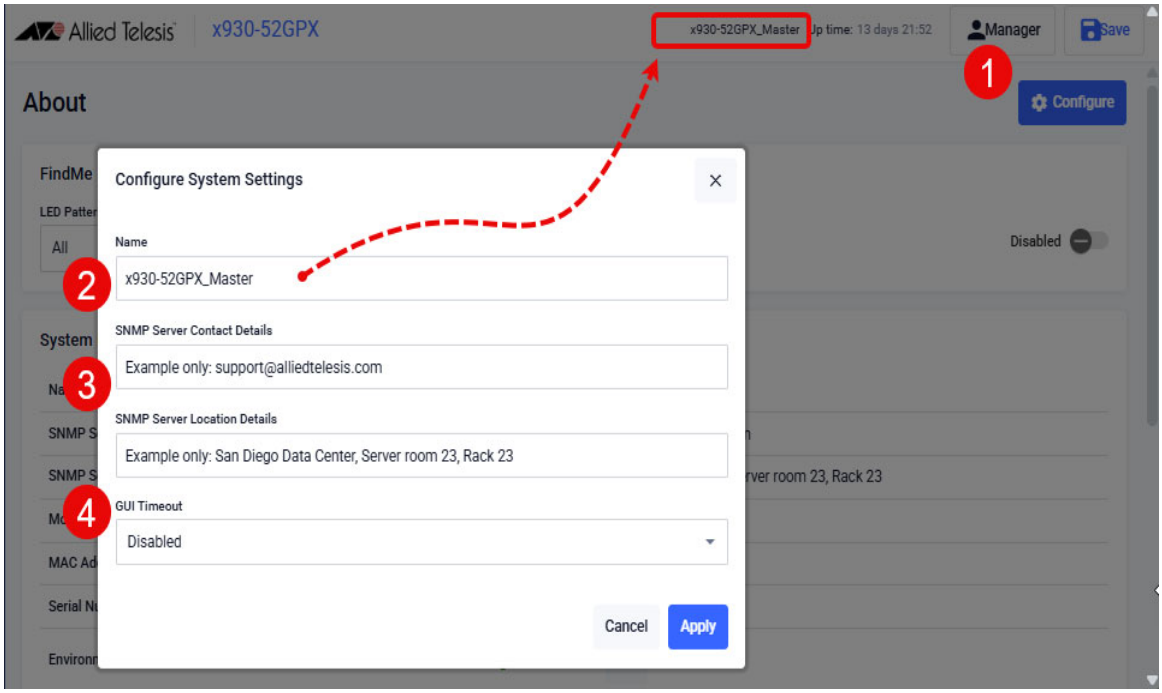
This includes:

- The device's Hostname
- SNMP Server Contact and Location details
- Model
- MAC Address
- Serial Number
- Environment
- Current Software file
- Software Version
- Bootloader
- GUI Version
- GUI Build

Note: Capturing a screenshot of this information can be extremely helpful in the event of an issue, as it provides valuable details for Allied Telesis support.

Configuring the System settings

1. Click Configure
2. You can change your device's Name. The name change will be reflected on the Device GUI's header at the top of the page.
3. Edit the SNMP server contact and location details
4. You can change the GUI timeout period to 5 or 30 minutes, 1 hour, or disabled.The default setting for the GUI timeout is 5 minutes.



Finding a device in a server room

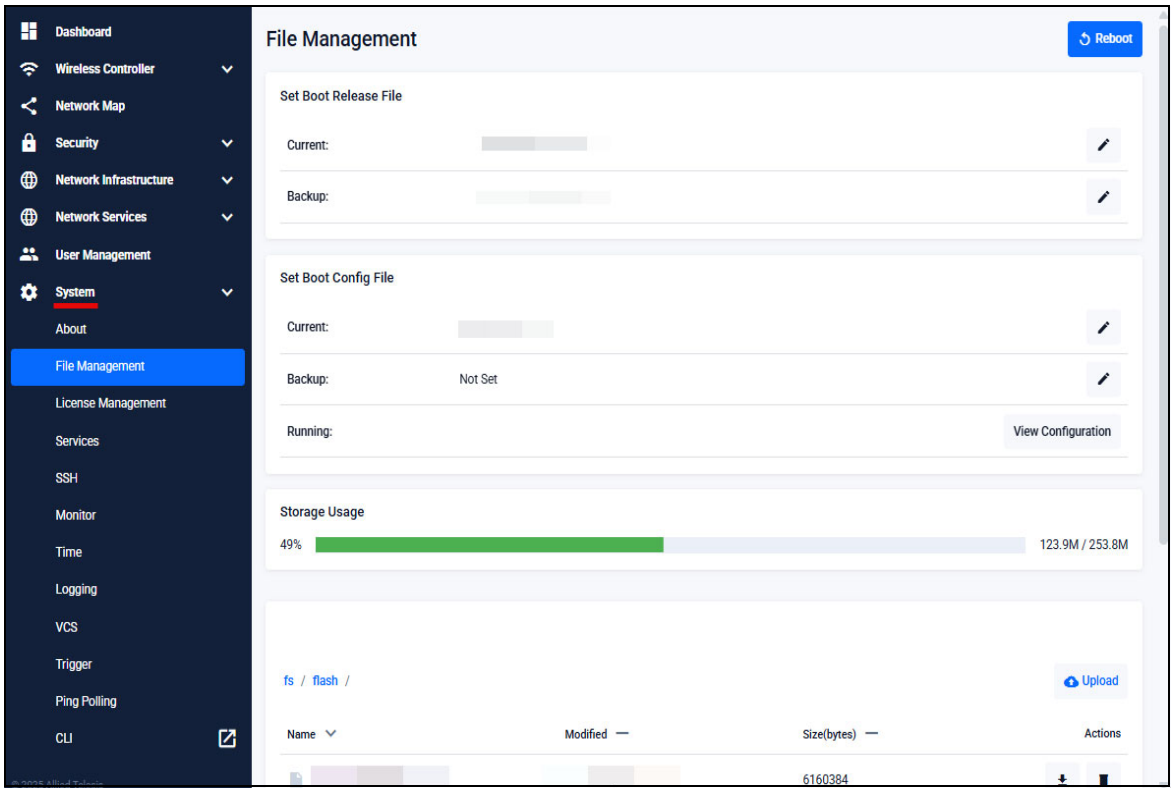
FindMe helps you locate a specific device by flashing all of its port LEDs in a selected pattern.

- First, choose the LED flash pattern and set a timeout period to help identify which device you are working with.
- Then enable **FindMe**.

Note: FindMe operates on the entire device. You cannot select individual ports or individual VCStack members.

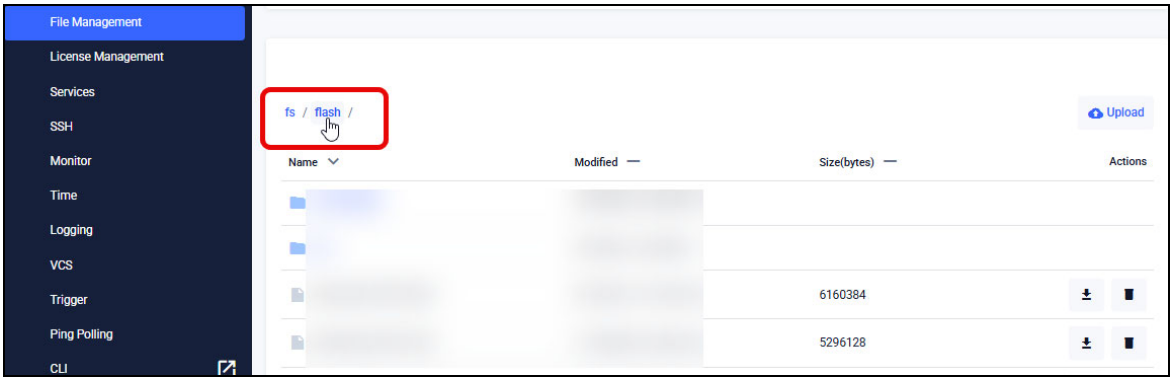
File Management

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



At a glance, File Management shows you the settings for configuring boot release and configuration files. You can easily upload, download, or delete any file, as well as set the current and backup software release for the switch, as well as the current and backup configuration files.

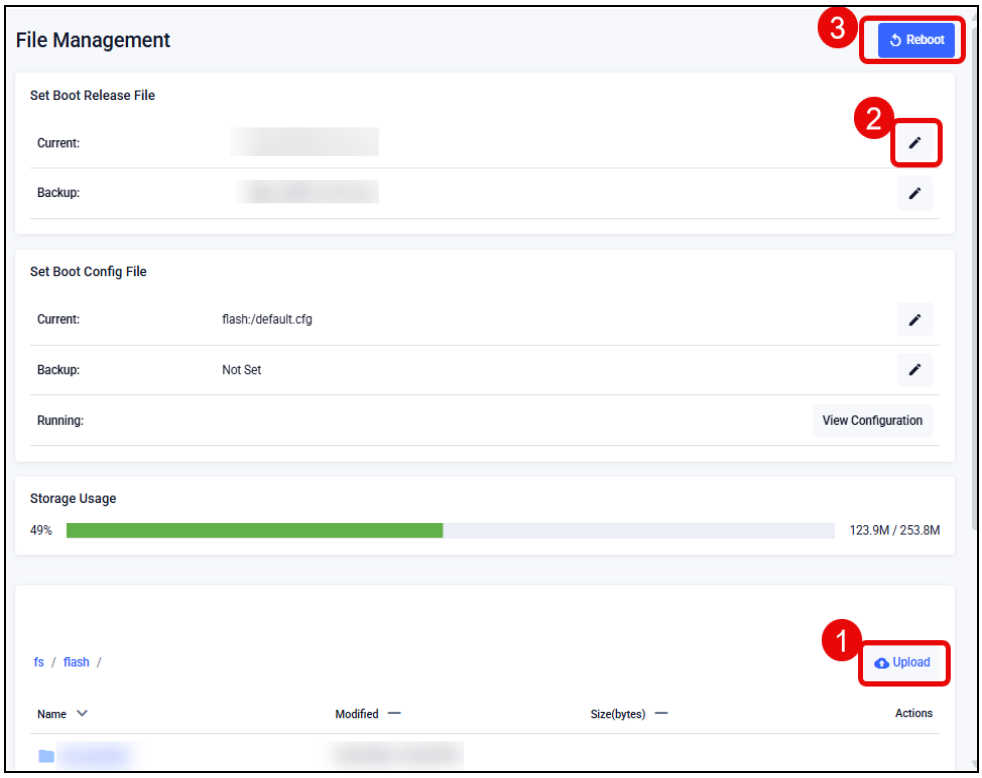
Click on the file breadcrumb bar to navigate through the different storage locations. Flash memory files are displayed by default.



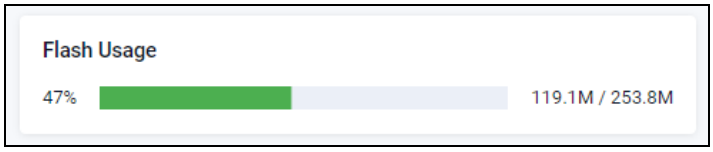
How to upgrade software

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.



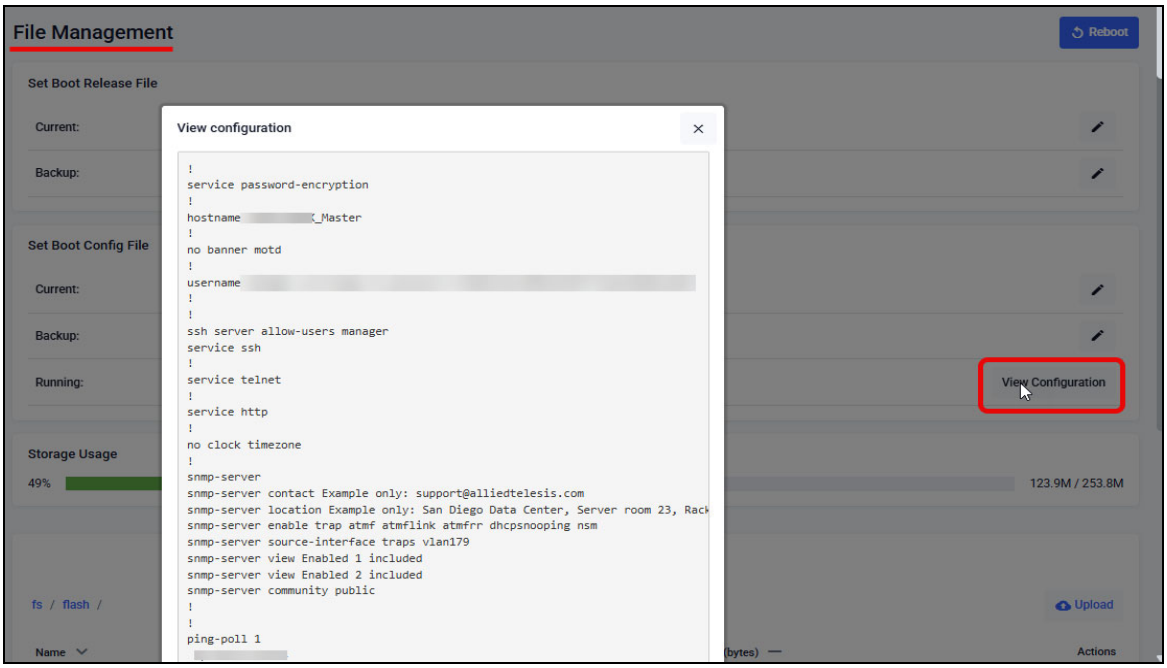
Tip Use the **Flash Usage** panel to check you have enough available space prior to uploading any large files.



Display the running configuration

You can view the device's current running configuration from the Device GUI. Keep in mind that the running configuration may be different from the configuration the device loads at startup. To display it, go to the File Management page and click View Configuration in the Set Boot Config File section.

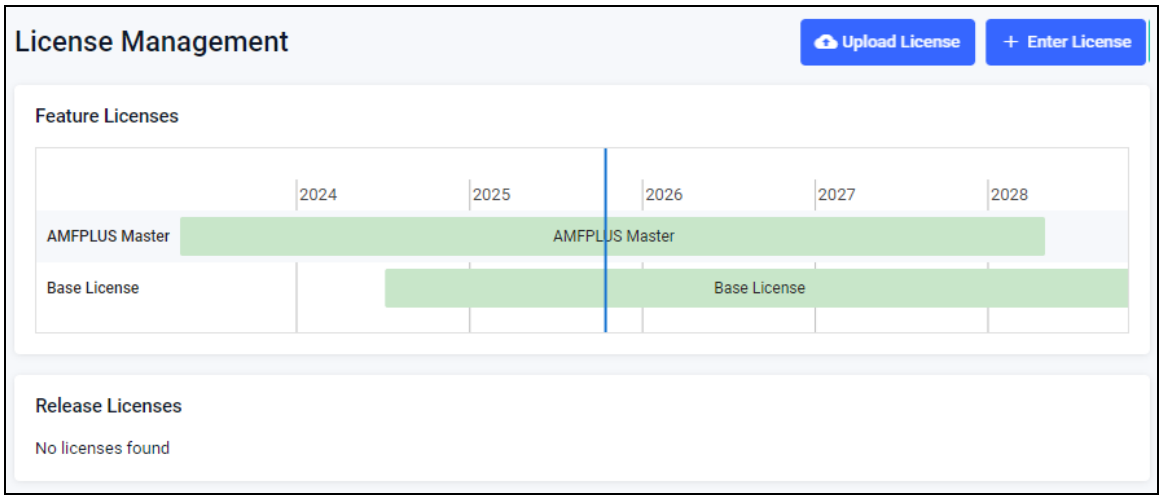
The running configuration will appear in a dialog box.



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.

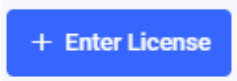
Hover your mouse over a license to show details, including duration and included features.



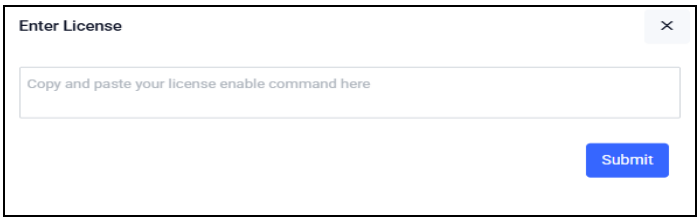
Adding a new permanent feature license

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

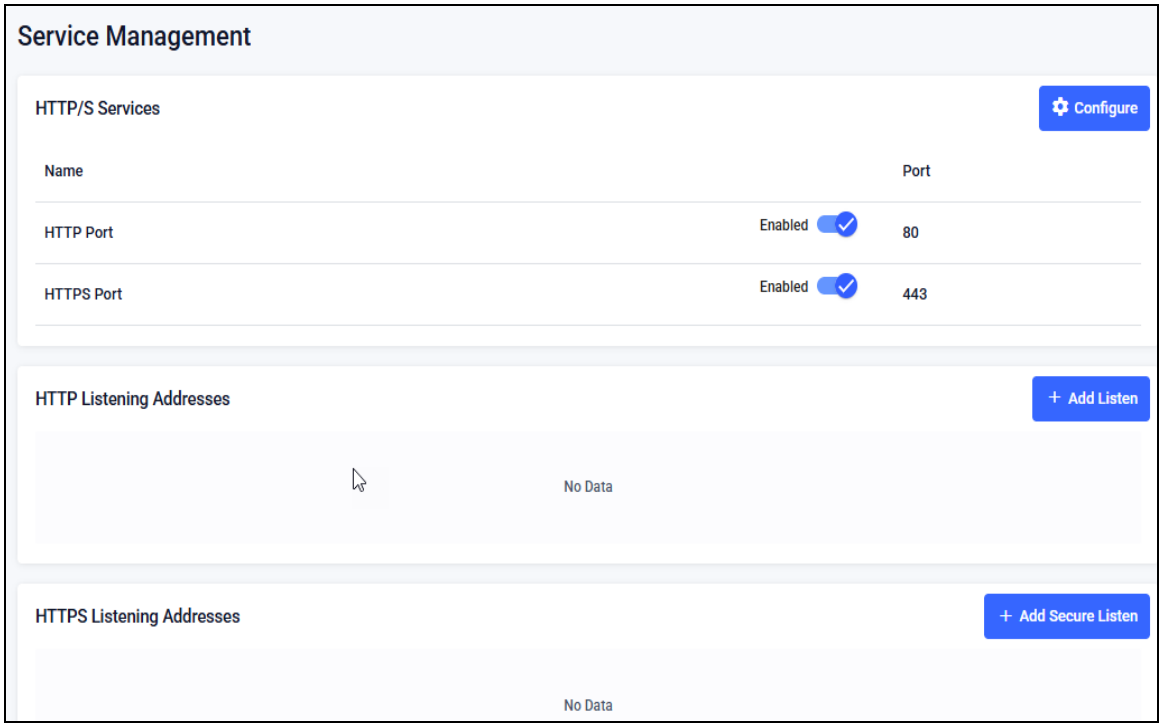
Once you have purchased your new subscription license (for example, a 1 year OpenFlow license), here's how to add it to your device:

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

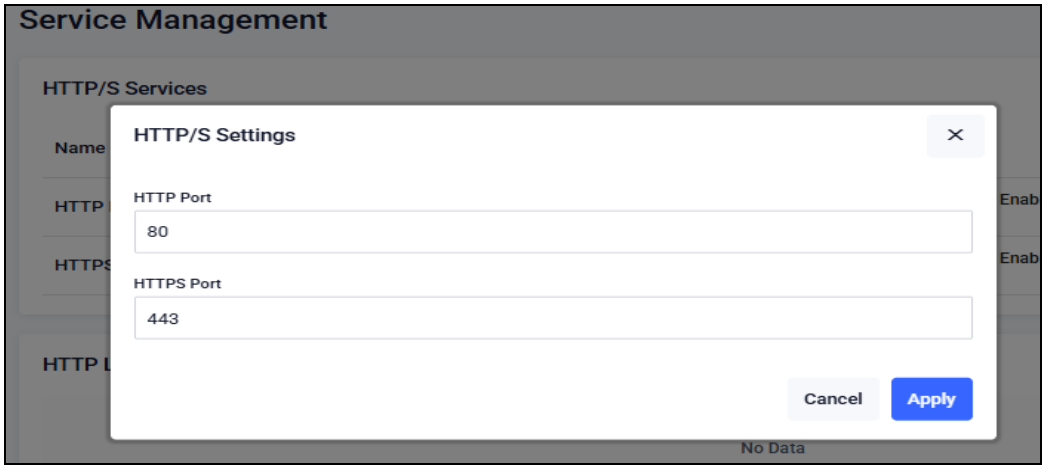
Use the Services page to enable or disable HTTP and HTTPS.



- Click the toggle next to an HTTP or HTTPS port to enable or disable that port.
  If the toggle is set to disabled, the port value will reset to none.

Enabling or disabling the HTTP or HTTPS ports is only available from version 2.17.0 onwards.

Click the **Configure** button on the HTTP/S Services table to change the HTTP or HTTPS port.



- You cannot use the same ports for both HTTP and HTTPS.
- If you configure a port currently in use (for example, the same http port you are using to log into the GUI), then a warning message will display.

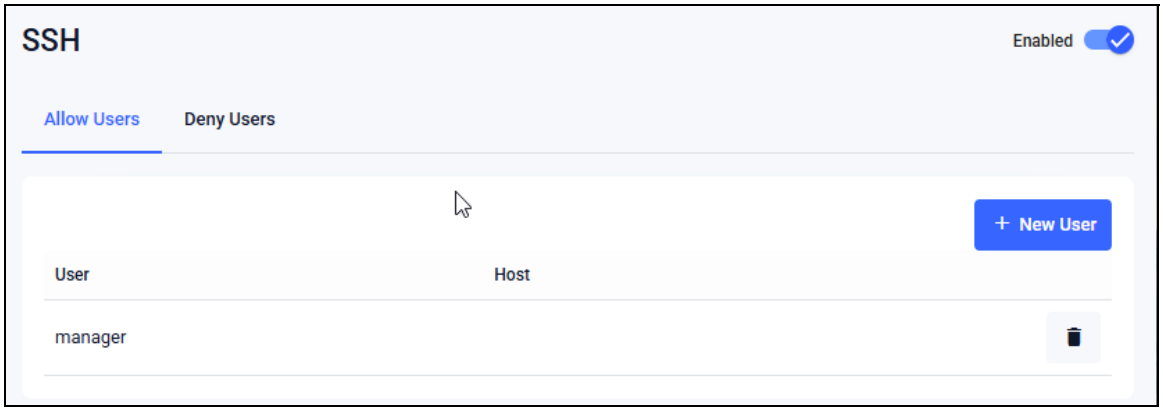
Note: Changing the HTTP or HTTPS settings will result in loss of connection.

SSH

Use the SSH page to enable or disable SSH and manage SSH access.

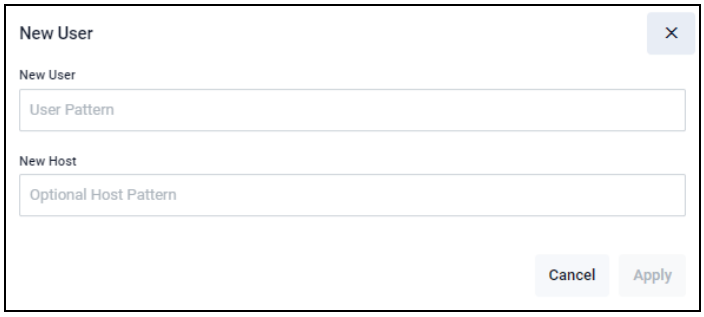
You can:

- Toggle SSH on or off by clicking the switch next to SSH.
- Allow specific users by selecting + New User in the Allow Users tab.
- Deny specific users by selecting + New User in the Deny Users tab.



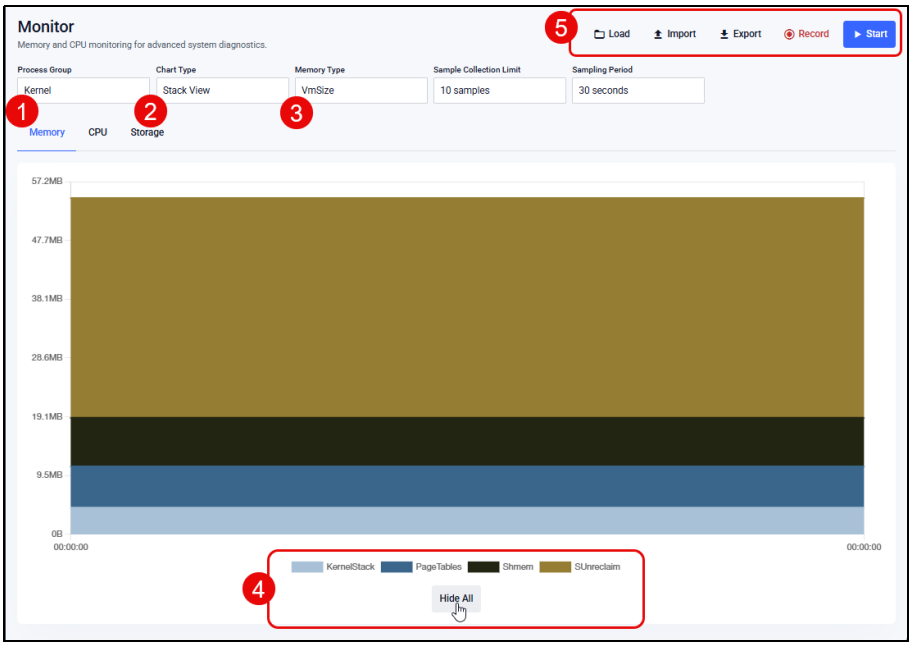
When you click **+ New User** in either the Allow or Deny tab, the New User window opens, allowing you to enter a user and host pattern. The host pattern can be either an IP address or a domain name.

You can use an asterisk as a wildcard character to match any string of characters.
For example, 192.168.1.* will match a range (from 192.168.1.1 to 192.168.1.255) of IP addresses as hosts.



Monitor

Use the Monitor page to visualize usage statistics for CPU, memory, and storage I/O. This can help identify processes that are consuming more (or less) resources than expected.



1. **Process Group -** Overview (a combination of Kernel and System), Kernel, or System
2. **Chart Type** - Stack, Line, or Data
3. **Memory Type**:
   - **VmSize** - the amount of virtual memory available to a process. Note that this is not the amount of memory that the process is actively consuming in memory, but instead the amount a process has requested to be potentially use. This can provide insight into the memory patterns of a process.
   - **VmRSS** -the amount of physical memory the process has consumed. This is useful when determining if a process is over consuming memory and therefore starving other processes of memory.
   - **Shared** - the amount of memory a process shares with other processes.
   - **Data** - measures size of the global, static, and stack variables. High usage can indicate issues like high recursion depth. Deep recursion refers to a situation where a function keeps calling itself many times.
4. **Programs** - each program is shown as a coloured square. Hover your mouse over a square to see more information, or click it to show or hide that program.
5. **Managing and Recording Sample Sets**:

   Use the tools at the top of this page to load, import, export, and record sample sets.

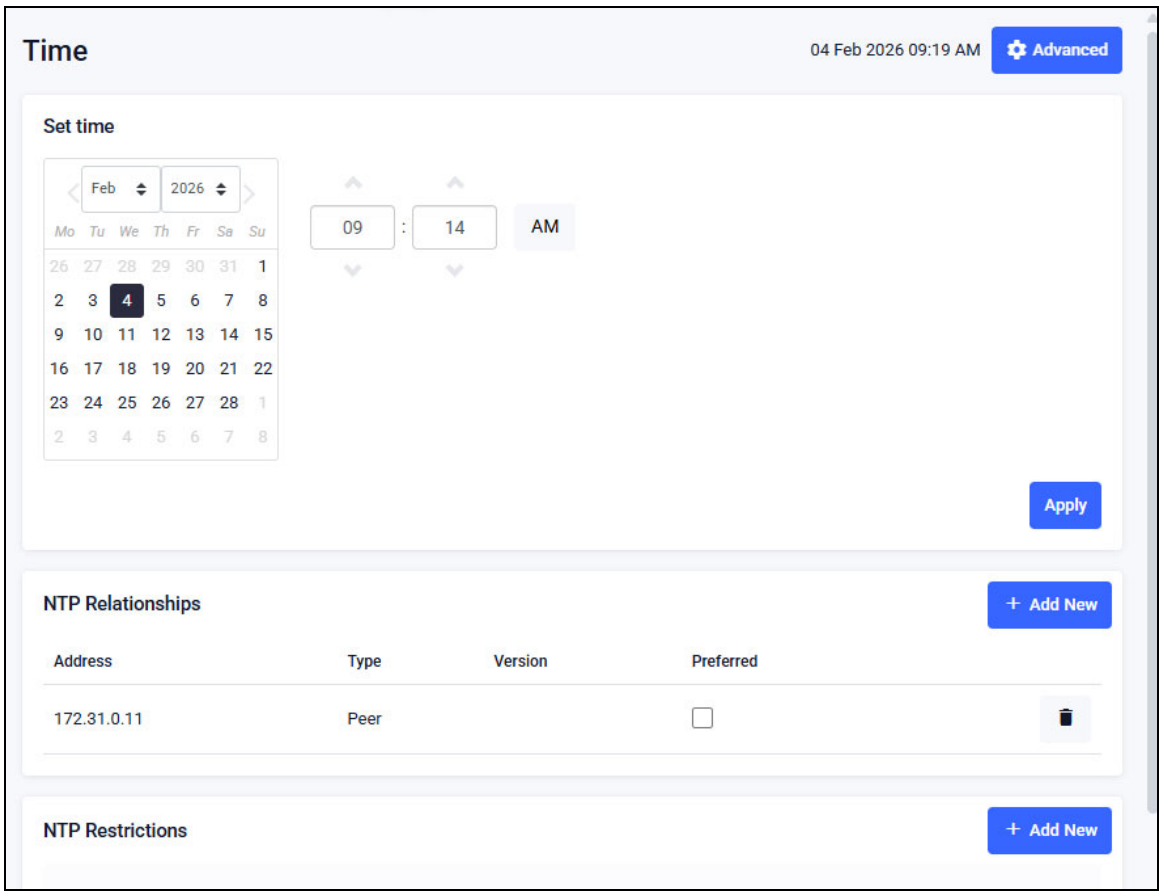
   Tip: Hover your mouse over each tool to view additional information.

Time

You can change the System time and date using the **Time** page.

The Time page also allows you to configure NTP settings, including:

- NTP relationships
- NTP restrictions



NTP Relationships

We recommended you use more than one NTP server for redundancy.

- Click the **+ Add New** button to add an NTP relationship
- Enter an address, type, version, and the preferred server.

Address types include the following:

- Server
- Peer
- Pool

The NTP version can be set from 1-4

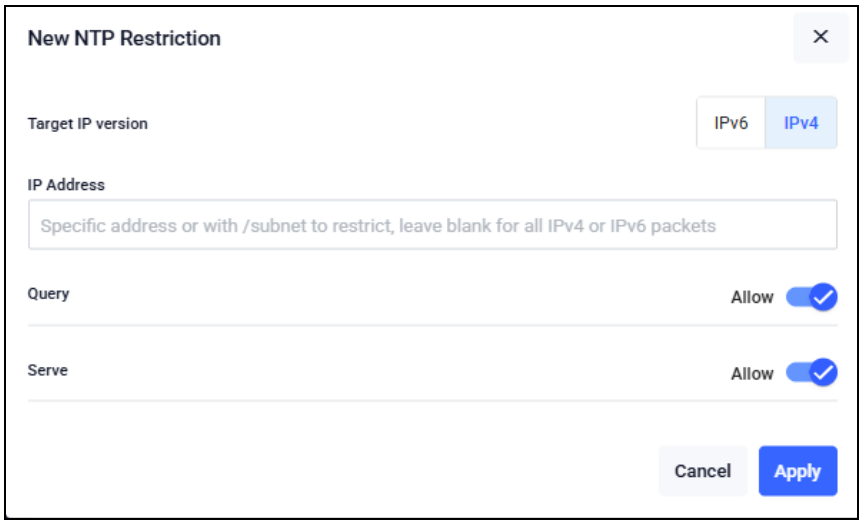
NTP Restrictions

To add an NTP restriction, click the **+ Add New** button next to the title.

You can deny or allow the ability for NTP to send queries or serve network time stamps to the target IP.

You might use NTP restriction for hierarchy purposes, for example, if an organization has a main office with a data center, and several remote sites.

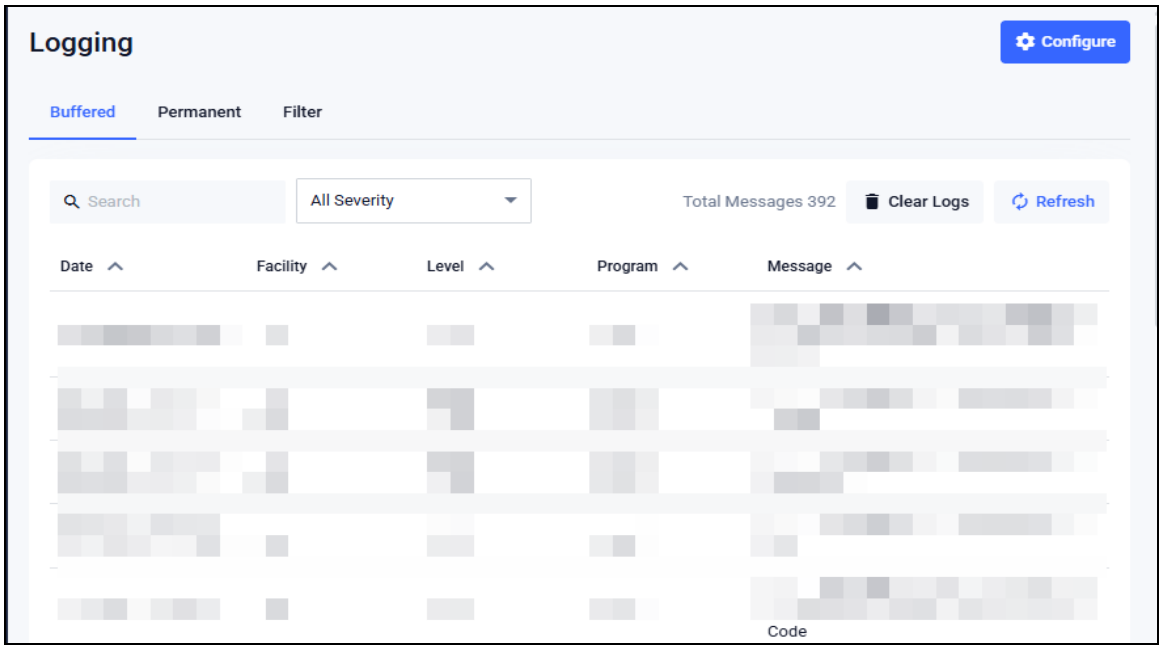
- Restrictions can help if you want to serve NTP times to remote sites, but don't want to sync time from them.
- You can allow or deny specific IPs from being able to query or serve network time information, in order to secure your network.



Logging

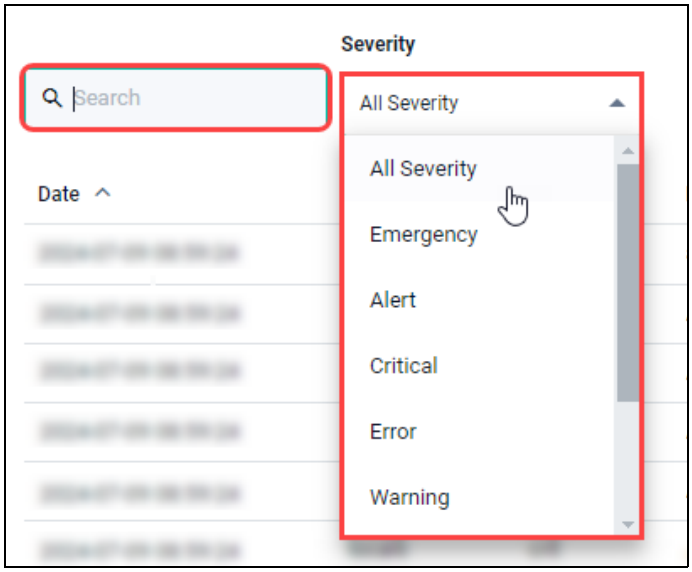
The Logging page shows buffered and permanent log messages stored on the device. The buffered logs tab is displayed by default.

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



1. Click the name of a category to sort by that type:
2. Search for any text string found in the logs with the search function.
3. Select the level of logs to display from the drop-down next to the search.

Logging Filters

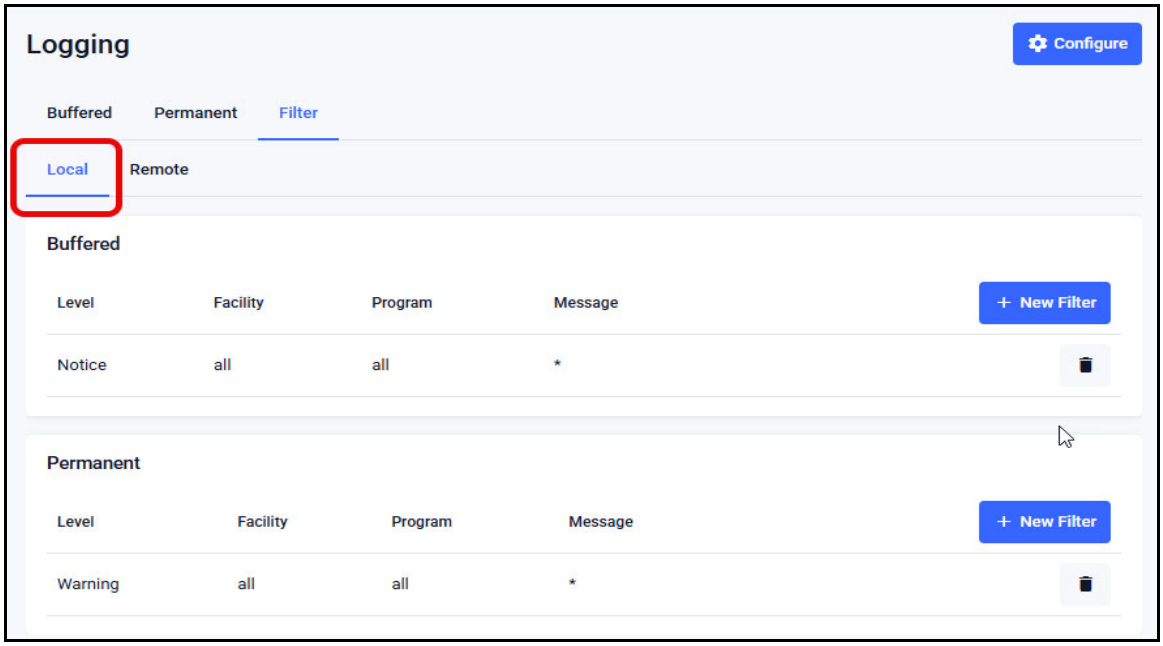


Filters allow you to manage which logs are stored on the switch and also set up a Syslog server(s) for remote log storage.

- Use the **Local** tab to create filters to manage the level of logs that are on the switch.

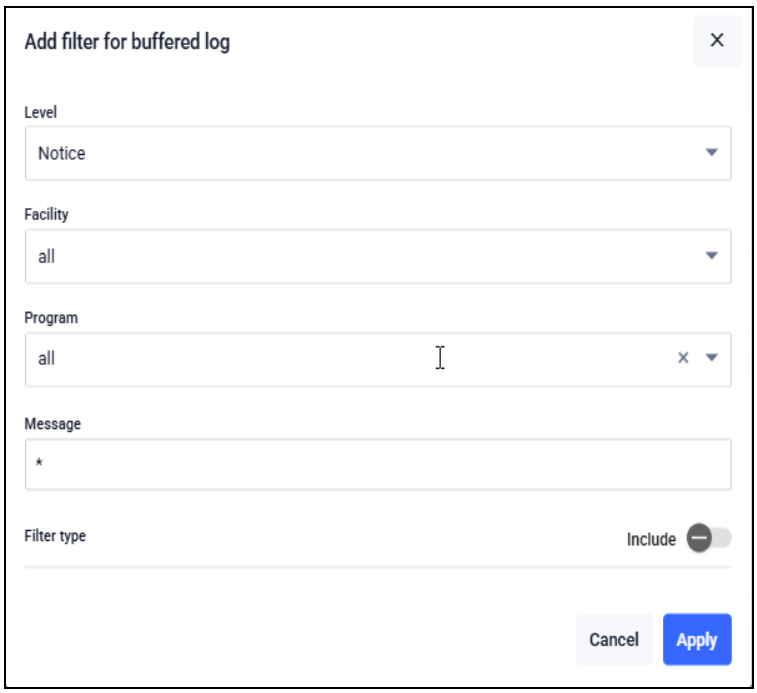
Local Filters

From the **Filter** > **Local** tab, you can add New Filters for Buffered and Permanent logs.



To create local buffered and permanent logging filters, click the **+ New Filter** button.

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.



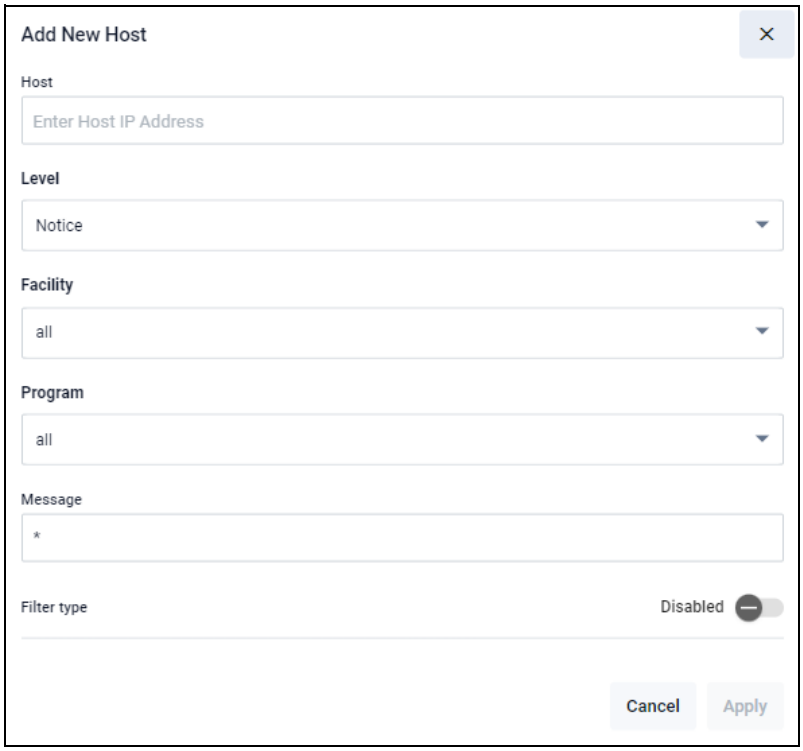
Remote Filters

From the **Remote** tab, you can create filters for email addresses or hosts. You can set up a host, such as a syslog server, to send log messages to for storage and analysis.

To add a new email or host, click the **+ New Email** or **+ New Host** buttons.

To add a new Host:

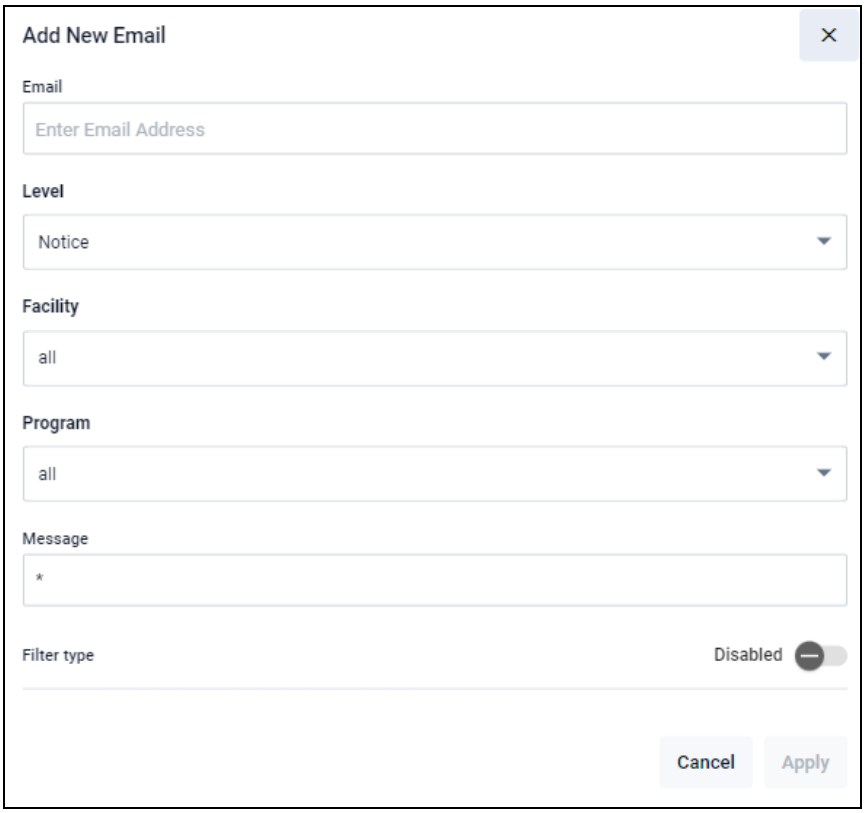
1. Navigate to the **Filter** > **Remote** tab on the Logging page.
2. Click the **+New Host** button
3. Enter your syslog server information.



Similarly to hosts, you can also add an email address for logging messages to be forwarded to.

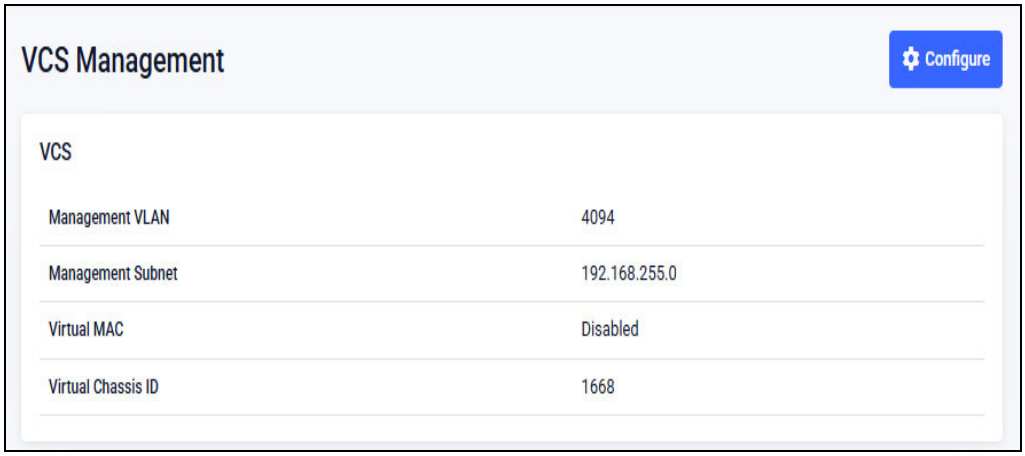
To add an email filter:

1. Navigate to the **Filter** > **Remote** tab on the Logging page.
2. Click on the **+New Email** button
3. Type in a destination email address.
4. 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.



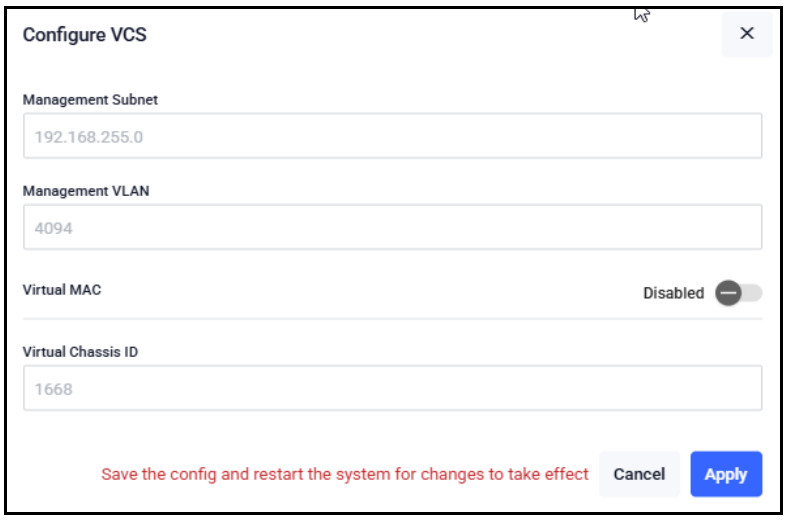
By default, the VLAN and subnet used are:

- 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.

Trigger

You can create triggers through the Device GUI. When you create a trigger, you can fill out different fields depending on the type of trigger you select.

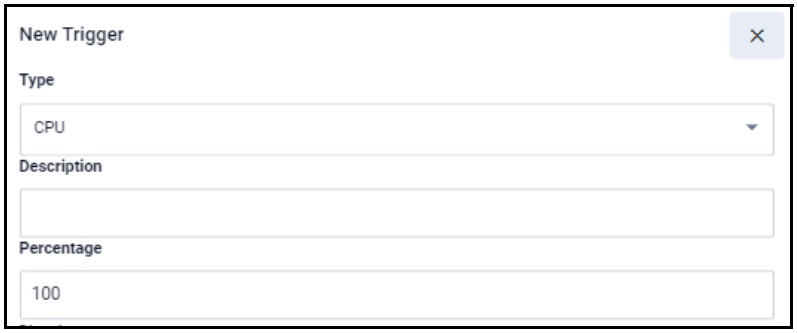
For more information about Triggers, see the Triggers Feature Overview Guide.

- A **trigger** is an ordered sequence of scripts that is executed when a certain event occurs.
- A **script** is a sequence of commands stored as a plain text file on a file subsystem accessible to the device, such as Flash memory.

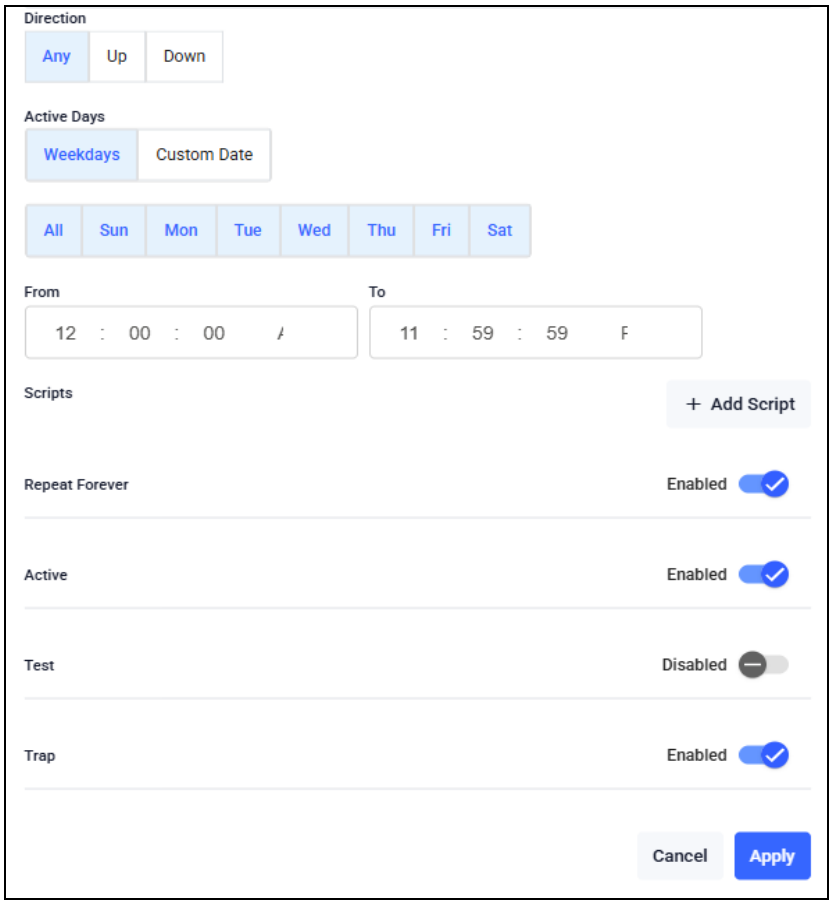
Note: You cannot edit an existing trigger. Instead, please delete and re-create a new trigger.

- To create a trigger, click the **New Trigger** button.
- To delete a trigger, click the **Delete** button next to the trigger.

For example, if you create a **CPU trigger**, you can select the percentage from 0 - 100 that the trigger will enable at.



The following fields may change based on the trigger type you select:



Select the type of trigger you would like. What you can configure in the Direction/Event section depends on the type of trigger you have selected.

For example, you can select a percentage for CPU, a port for Interface, a stack event based on a member joining or leaving for Stack Member, etc.

- **Description** - You can add a description to help identify a trigger. This is useful if there are a lot of triggers in the list.
- **Direction** - Either Up or Down. This may change depending on what trigger type you have selected.

Active days - Depending on if you select Daily or custom from the Date/Time section, different options will display.

- Daily - you can select any of the days you would like the trigger to activate.
- Custom - you can set a custom day/month/year setting.

For the **Time** category, you can select the time the trigger should be active between.

In the **Scripts** section, you can add a script to run when the trigger activates. To see more information about how scripts work with triggers, see the Triggers Feature Overview and Configuration Guide.

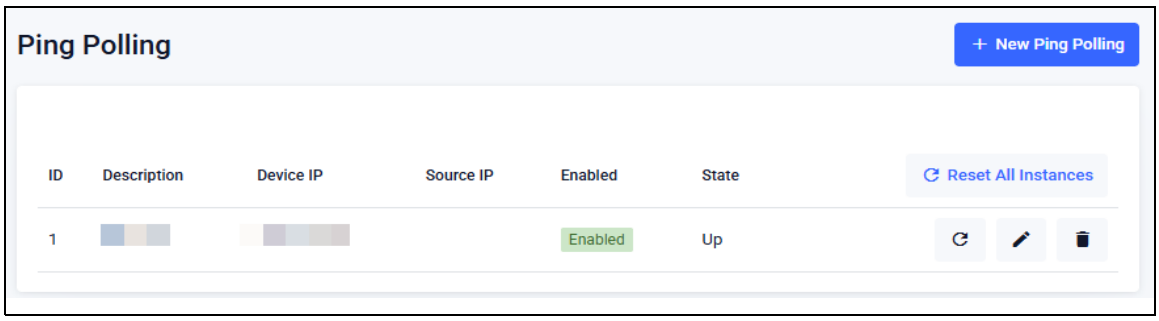
You can select the times that a trigger is repeated by toggling the **Repeat** button.

The following Toggles are available to configure at the end of the Create Trigger dialogue. They can be enabled or disabled.

- **Active** - Turns the trigger on or off
- **Test Mode** - enable/disable the trigger to operate in diagnostic mode.
  In this mode the trigger may activate, but when it does it will not run any of the trigger's scripts.
- **Trap** - enable/disable the ability to send SNMP traps.

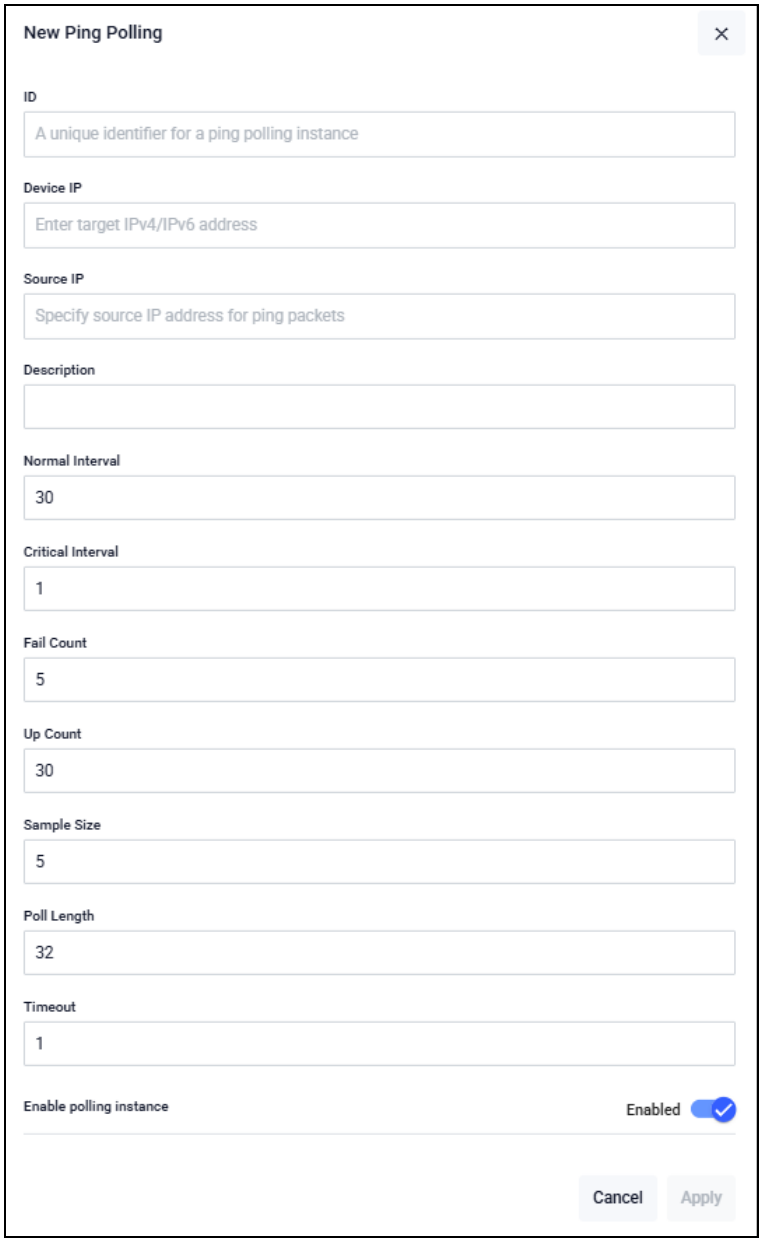
Ping Polling

Create a Ping Polling instance from the Device GUI in order to check your device's connectivity. You can configure Ping Polling to send ping requests from your switch, pinging a device, and the request will reply letting you know if it can reach other devices in the network.



You might set up a Ping Polling trigger on a device to ping another device's IP. For more information on how Ping Polling works, see the Ping Polling Feature Overview and Configuration Guide.

- To set up a new Ping Polling instance, click the **+ New Ping Polling** button in the top right.
- Enter the details to configure the ping instance in the newly opened New Ping Polling window.

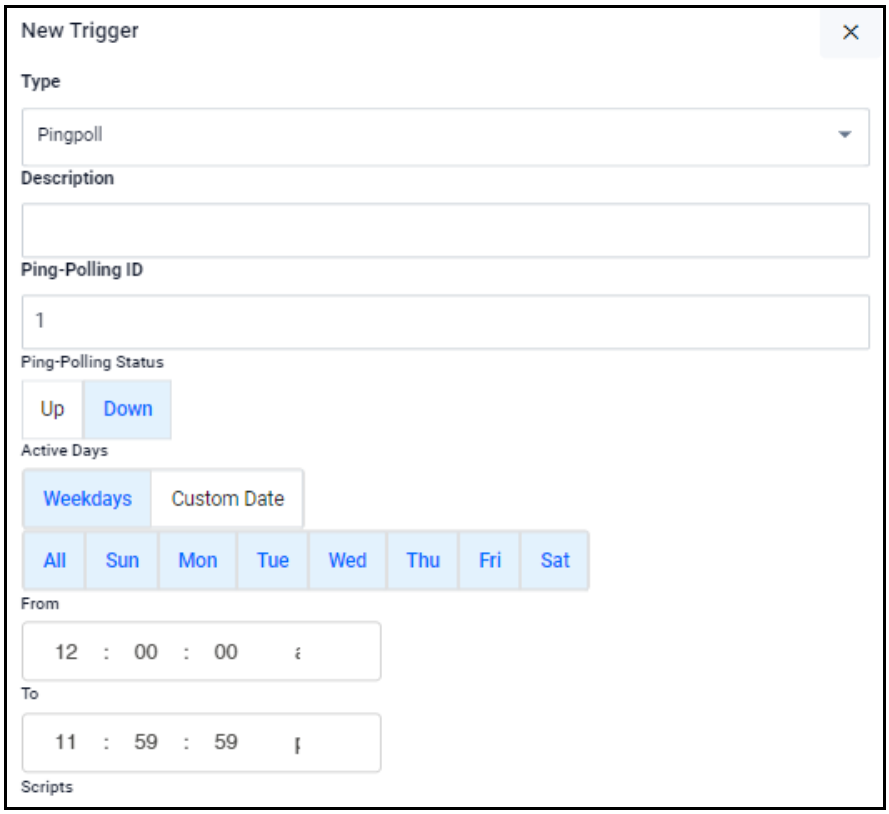


Automatically triggering ping polling

You can set up a Trigger from the trigger menu to run the ping command when a source IP is down. To do this:

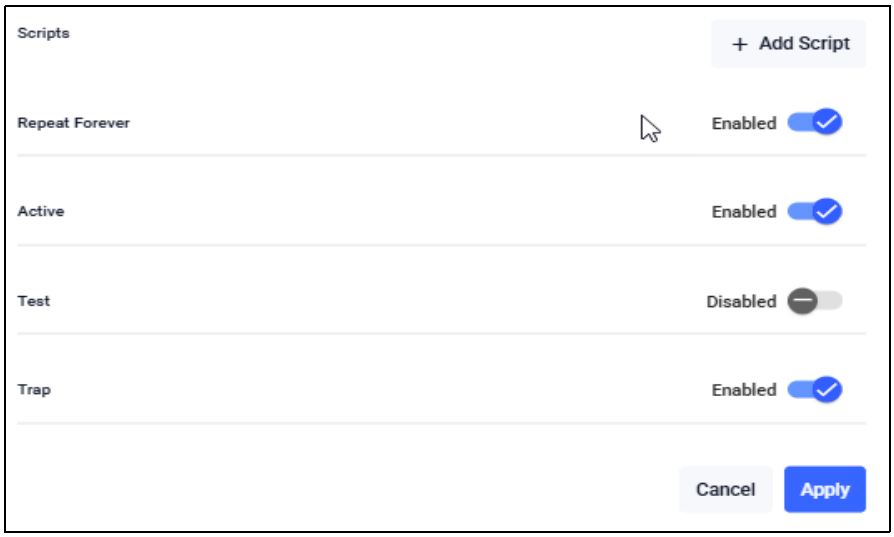
Make sure you have an existing Pingpoll entry set up on the Ping Polling page.

1. Go to the **System** > **Trigger** menu.
2. Click **+ New Trigger.**
3. Scroll down through the Type menu and select Pingpoll.



4. Enter the Ping-Polling ID from your existing Pingpoll entry.
5. Select a status.
6. Enter the time and frequency for the trigger.

7. Add a script to the trigger to run after the trigger is executed.



8. Enable or disable toggles as necessary.
9. Click **Apply** to create the Pingpoll trigger.

CLI

Allied Telesis devices running the AlliedWare Plus operating system use an industry-standard command-line interface (CLI) for configuring all features and functionality.

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