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

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™

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
```

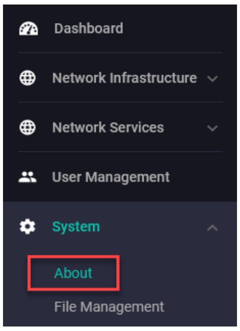
Alternatively, on unconfigured devices you can use the default address, which is 169.254.42.42.

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

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 Download 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.

Step 1. Obtain the latest GUI file.

You can 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.

Step 2. Log into the GUI.

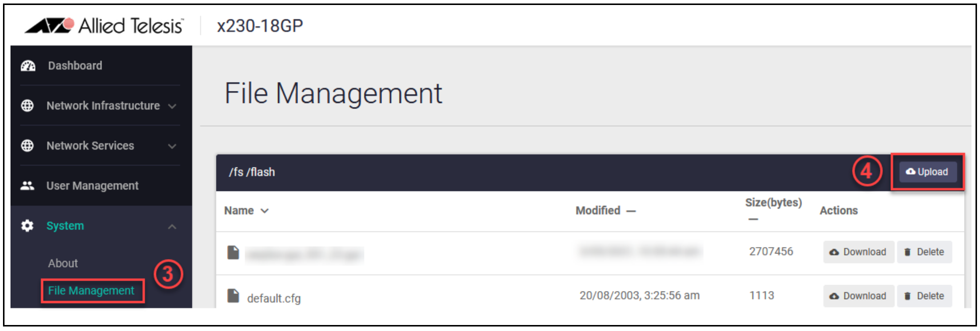
Start a browser and browse to the device's IP address by typing it into the address bar. You can access the GUI via any reachable IP address on any interface.

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.***

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

Step 4. Click **Upload** to upload the GUI file.



Name	Modified	Size(bytes)	Actions
[redacted]	[redacted]	2707456	Download Delete
default.cfg	20/08/2003, 3:25:56 am	1113	Download Delete

Step 5. Locate and select the GUI file

Note: You can download the latest GUI file from our Software Download centre.

The new GUI file is then 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**.

Step 6. 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, then use the following commands to stop and restart the HTTP service. You can access the CLI in a browser window by clicking the CLI button in the System sidebar.

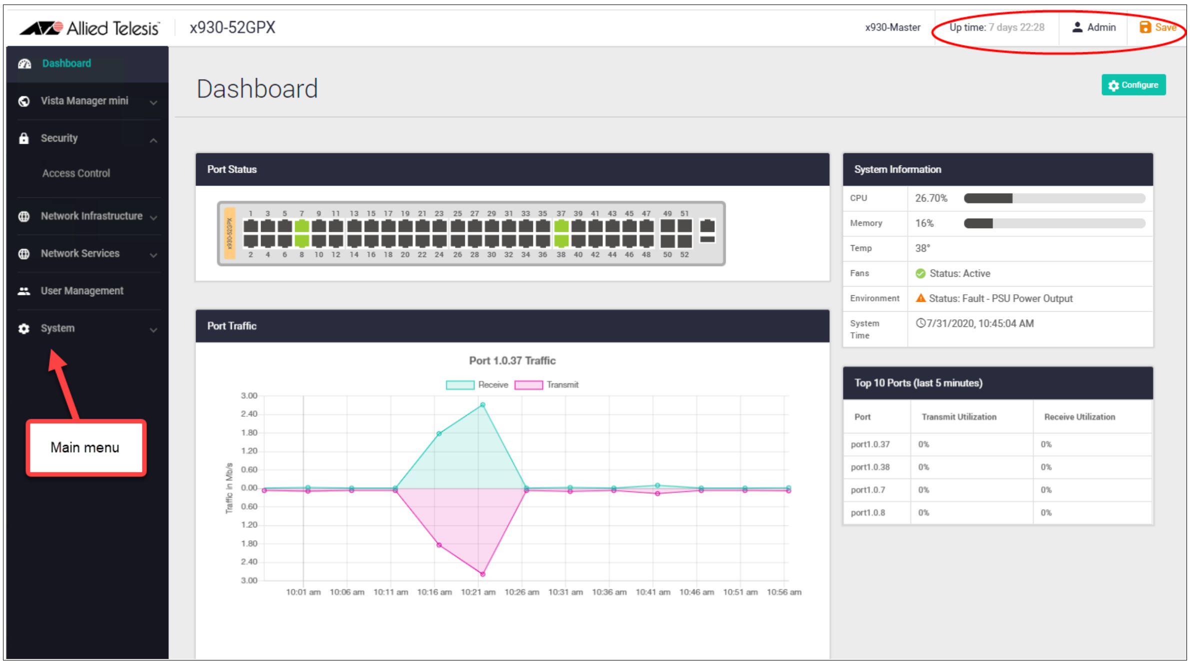
```
awplus> enable
awplus# configure terminal
awplus(config)# no service http
awplus(config)# service http
```

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.



System Information

CPU	26.70%
Memory	16%
Temp	38°
Fans	Status: Active
Environment	Status: Fault - PSU Power Output
System Time	7/31/2020, 10:45:04 AM

Top 10 Ports (last 5 minutes)

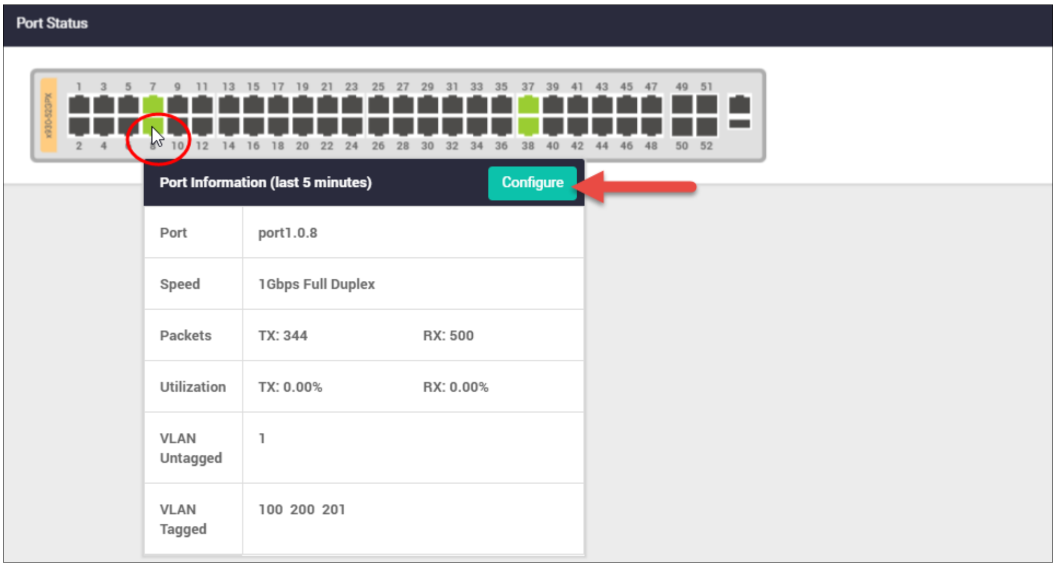
Port	Transmit Utilization	Receive Utilization
port1.0.37	0%	0%
port1.0.38	0%	0%
port1.0.7	0%	0%
port1.0.8	0%	0%

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



Port Information (last 5 minutes)

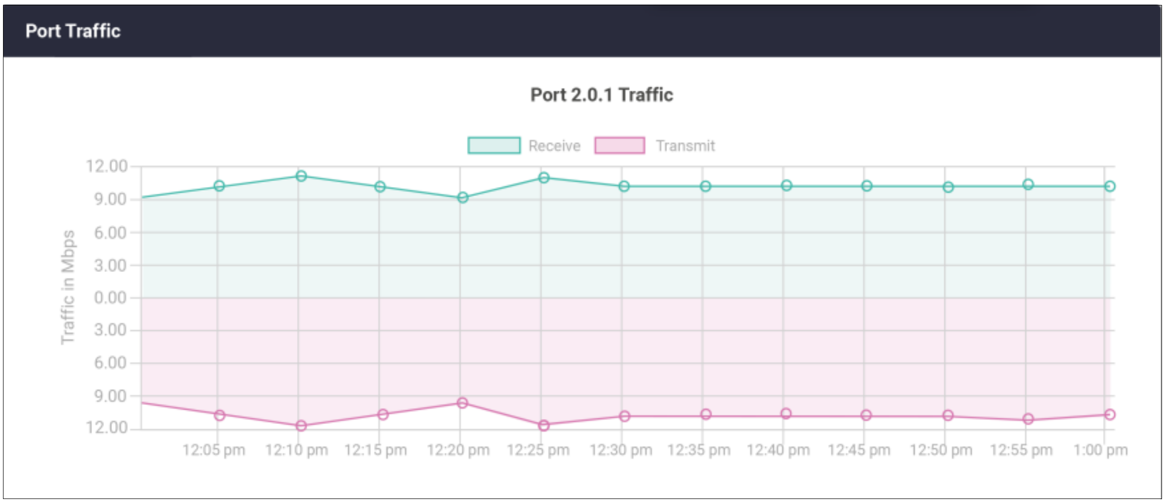
Port	port1.0.8	
Speed	1Gbps Full Duplex	
Packets	TX: 344	RX: 500
Utilization	TX: 0.00%	RX: 0.00%
VLAN Untagged	1	
VLAN Tagged	100 200 201	

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.

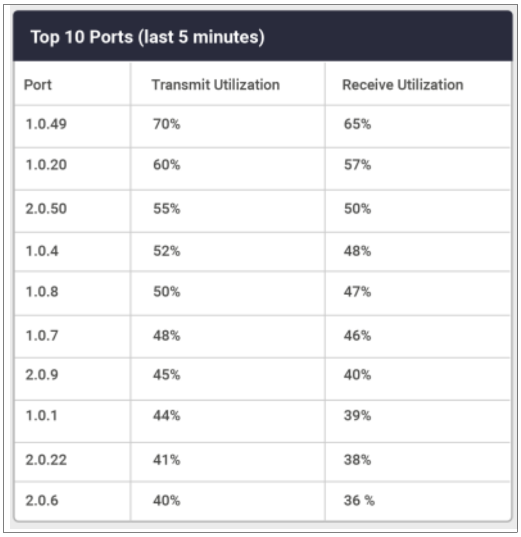
Port Traffic widget



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

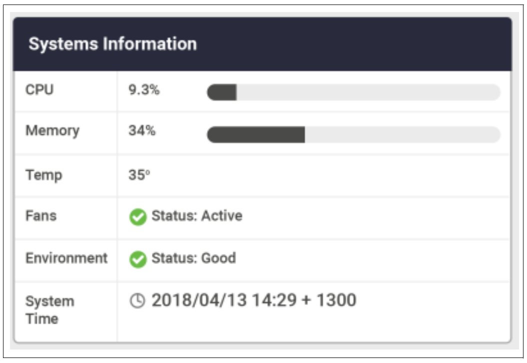


Top 10 Ports (last 5 minutes)

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



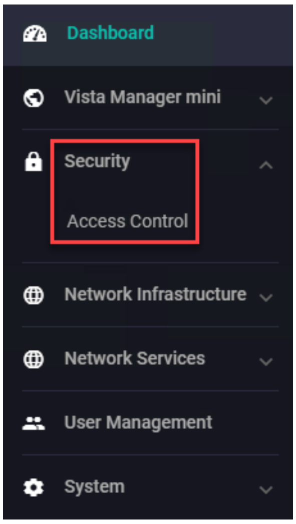
Systems Information

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.

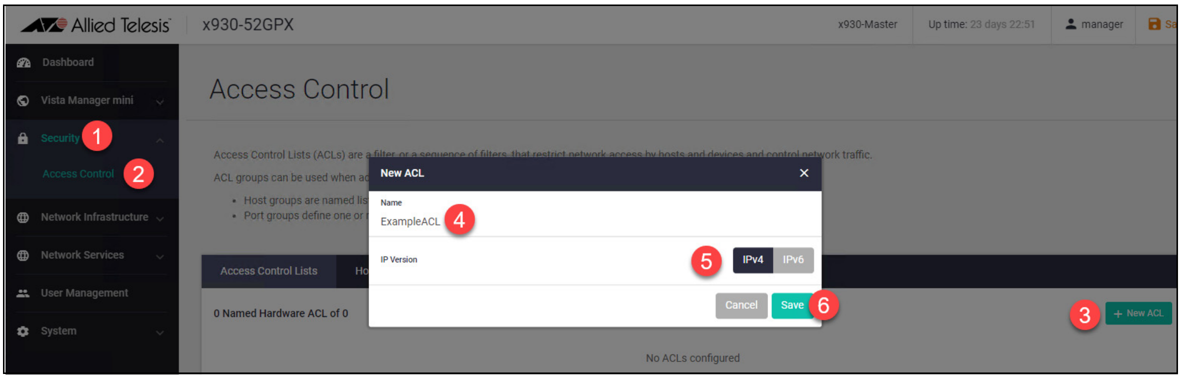
Security menu

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**.:



Access Control Lists (ACLs) are a filter or a sequence of filters, that restrict network access by hosts and devices and control network traffic.

ACL groups can be used when ac

- Host groups are named lis
- Port groups define one or r

Name: ExampleACL

IP Version: IPv4

0 Named Hardware ACL of 0

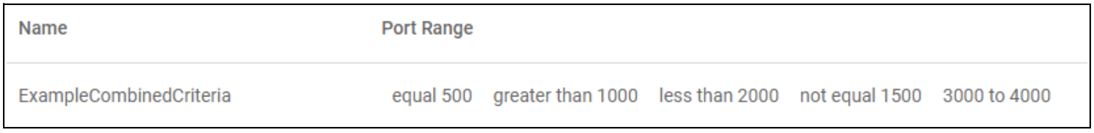
No ACLs configured

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:

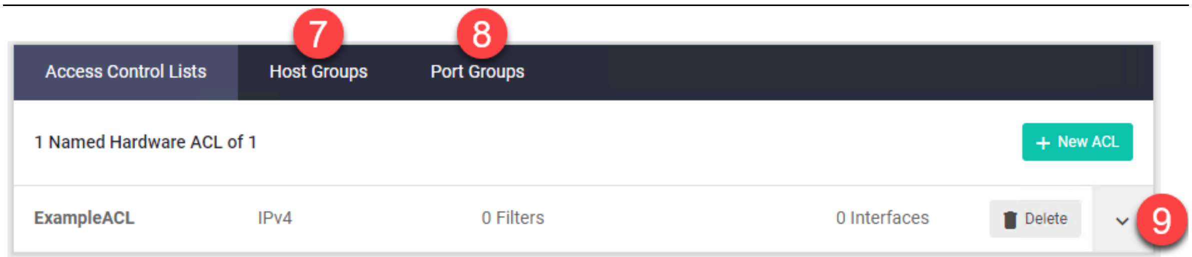
   - They let filters match on multiple addresses or port matching criteria. For example, you can use a port group to match all ports greater than a given port number. You can use a mix of criteria in one group, like this:

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.

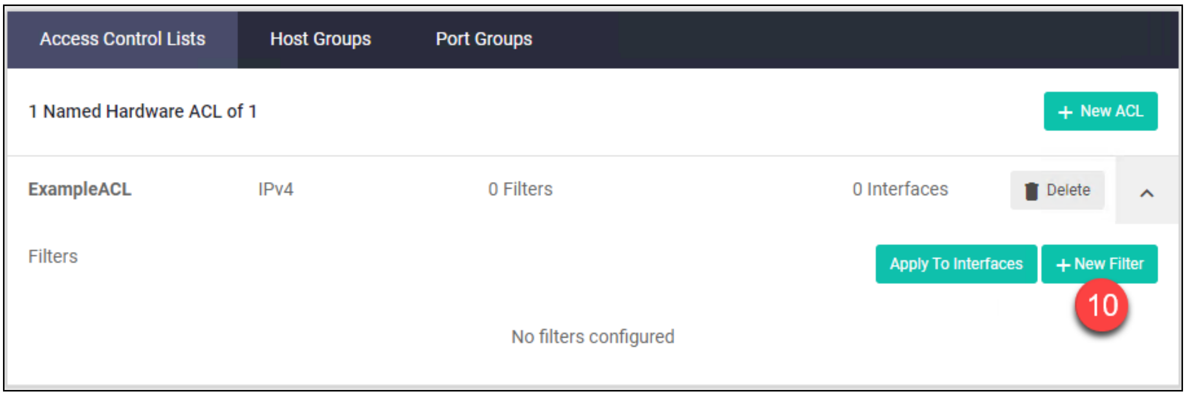
9. Return to the Access Control lists tab and select the down-arrow button at the end of your ACL's row to edit it.



1 Named Hardware ACL of 1

ExampleACL IPv4 0 Filters 0 Interfaces

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



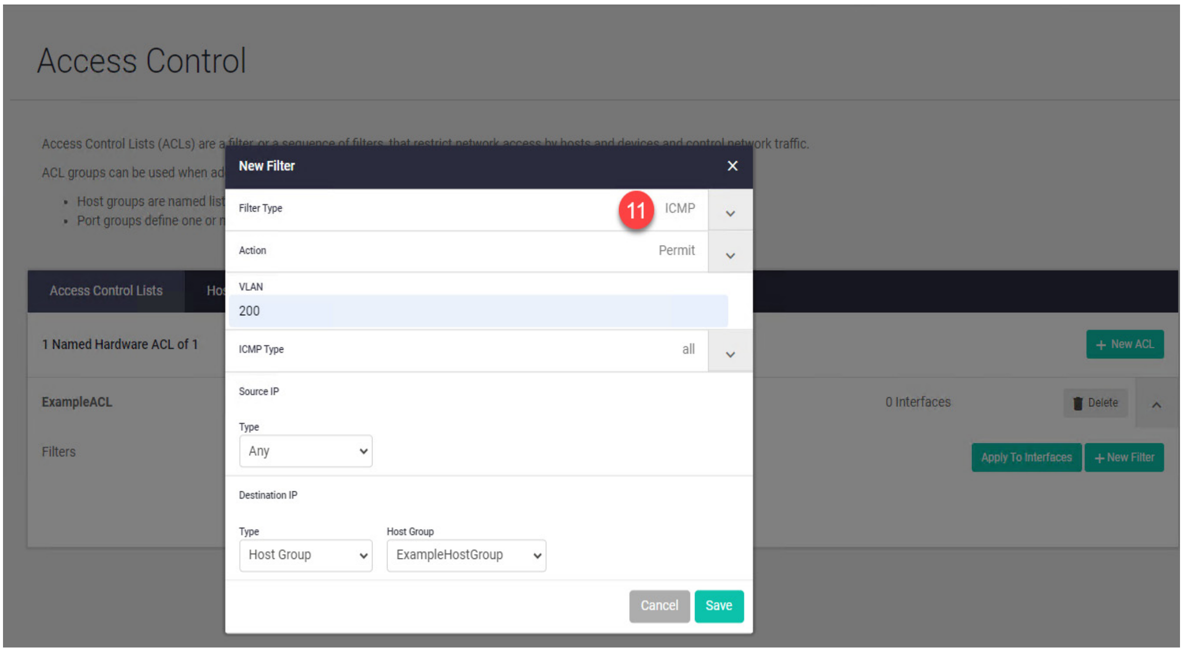
1 Named Hardware ACL of 1

ExampleACL IPv4 0 Filters 0 Interfaces

Filters

No filters configured

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.



Access Control

Access Control Lists (ACLs) are a filter, or a sequence of filters, that restrict network access by hosts and devices and control network traffic.

ACL groups can be used when ad

- Host groups are named list
- Port groups define one or m

New Filter

Filter Type: ICMP

Action: Permit

VLAN: 200

ICMP Type: all

Source IP

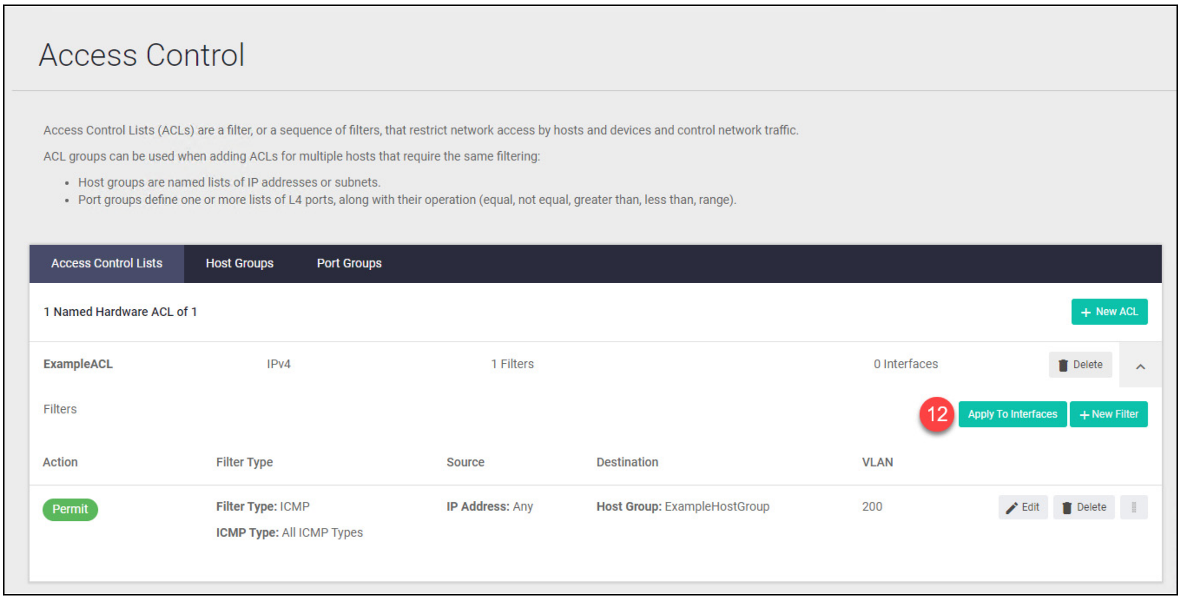
Type: Any

Destination IP

Type: Host Group

Host Group: ExampleHostGroup

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.



Access Control

Access Control Lists (ACLs) are a filter, or a sequence of filters, that restrict network access by hosts and devices and control network traffic.

ACL groups can be used when adding ACLs for multiple hosts that require the same filtering:

- Host groups are named lists of IP addresses or subnets.
- Port groups define one or more lists of L4 ports, along with their operation (equal, not equal, greater than, less than, range).

1 Named Hardware ACL of 1

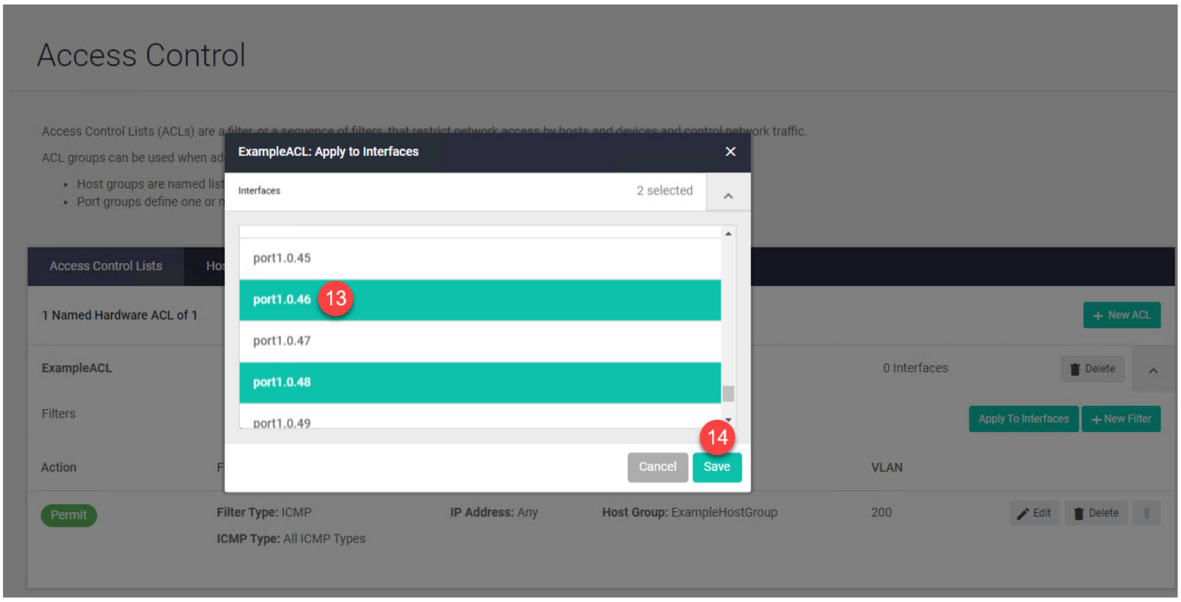
ExampleACL IPv4 1 Filters 0 Interfaces

Filters

Action	Filter Type	Source	Destination	VLAN
Permit	**Filter Type:** ICMP **ICMP Type:** All ICMP Types	**IP Address:** Any	**Host Group:** ExampleHostGroup	200

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**.



Access Control

Access Control Lists (ACLs) are a filter, or a sequence of filters, that restrict network access by hosts and devices and control network traffic.

ACL groups can be used when ad

- Host groups are named list
- Port groups define one or n

ExampleACL: Apply to Interfaces ×

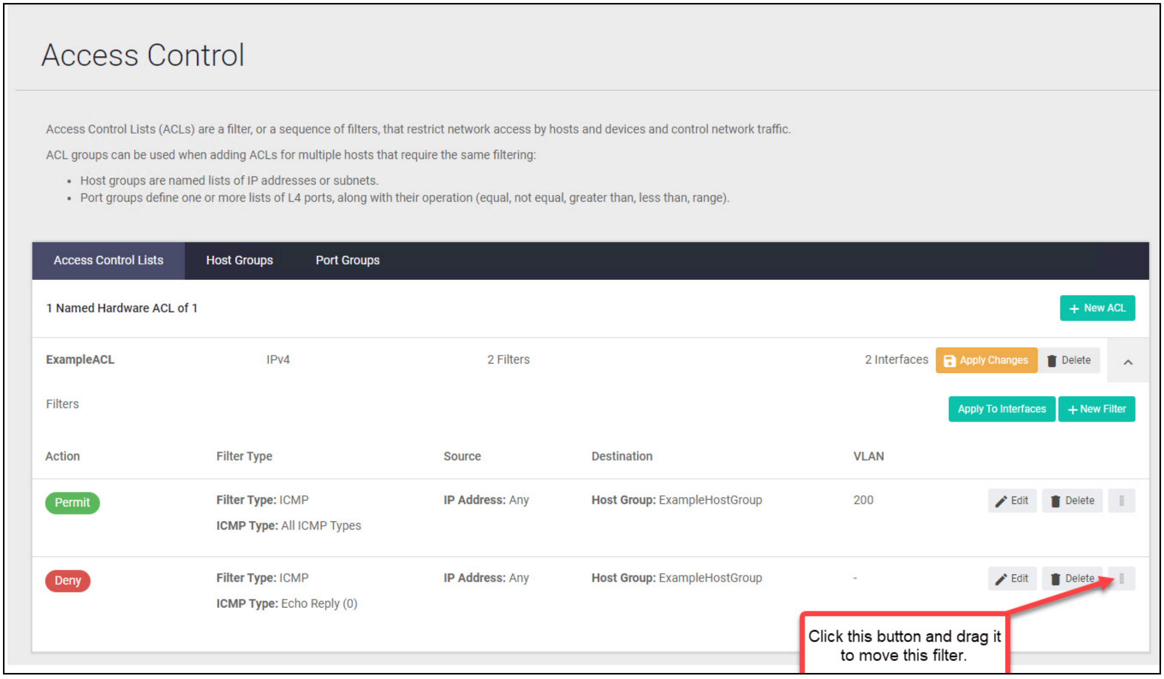
Interfaces — 2 selected

- port1.0.45
- port1.0.46
- port1.0.47
- port1.0.48
- port1.0.49

Action	F			VLAN	
Permit	**Filter Type:** ICMP **ICMP Type:** All ICMP Types	**IP Address:** Any	**Host Group:** ExampleHostGroup	200	Edit Delete

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.



Access Control

Access Control Lists (ACLs) are a filter, or a sequence of filters, that restrict network access by hosts and devices and control network traffic.

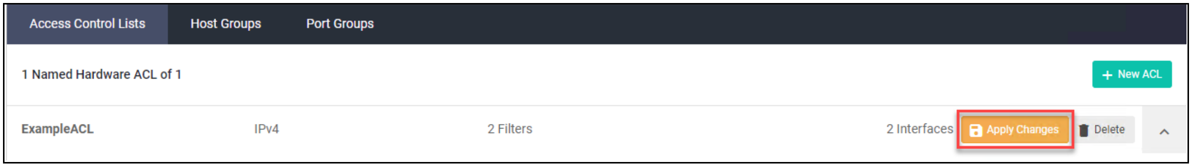
ACL groups can be used when adding ACLs for multiple hosts that require the same filtering:

- Host groups are named lists of IP addresses or subnets.
- Port groups define one or more lists of L4 ports, along with their operation (equal, not equal, greater than, less than, range).

Action	Filter Type	Source	Destination	VLAN	
Permit	**Filter Type:** ICMP **ICMP Type:** All ICMP Types	**IP Address:** Any	**Host Group:** ExampleHostGroup	200	Edit Delete
Deny	**Filter Type:** ICMP **ICMP Type:** Echo Reply (0)	**IP Address:** Any	**Host Group:** ExampleHostGroup	-	Edit Delete

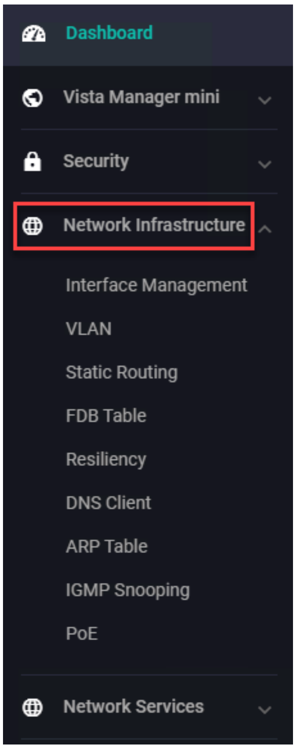
Click this button and drag it to move this filter.

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.



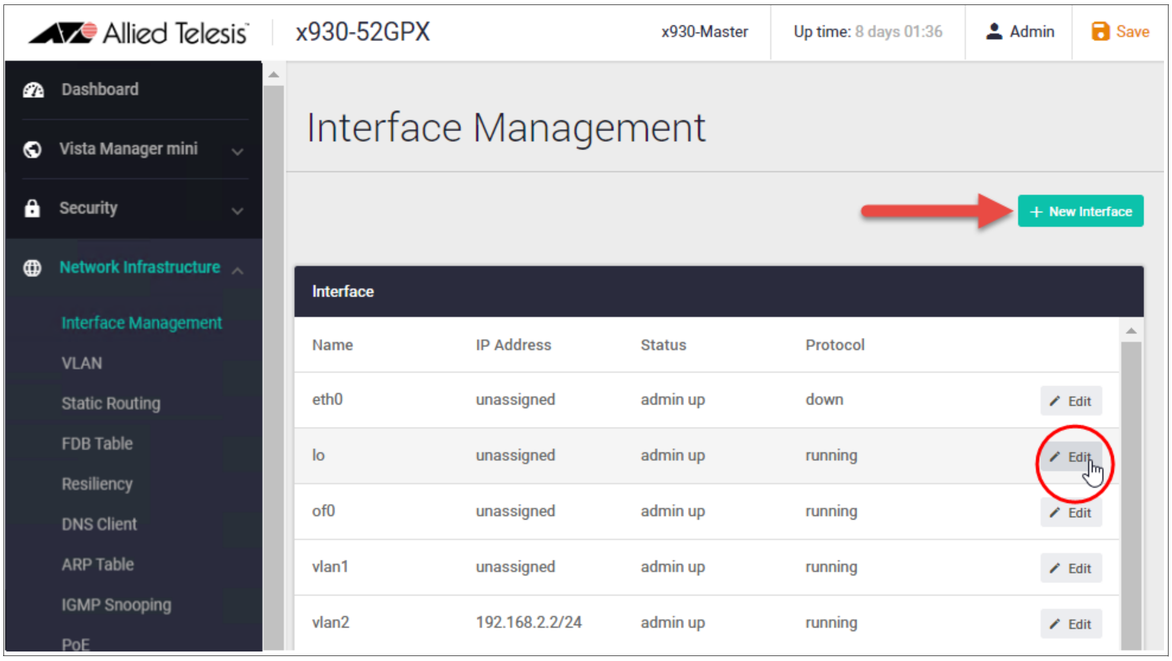
Network Infrastructure menu

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:

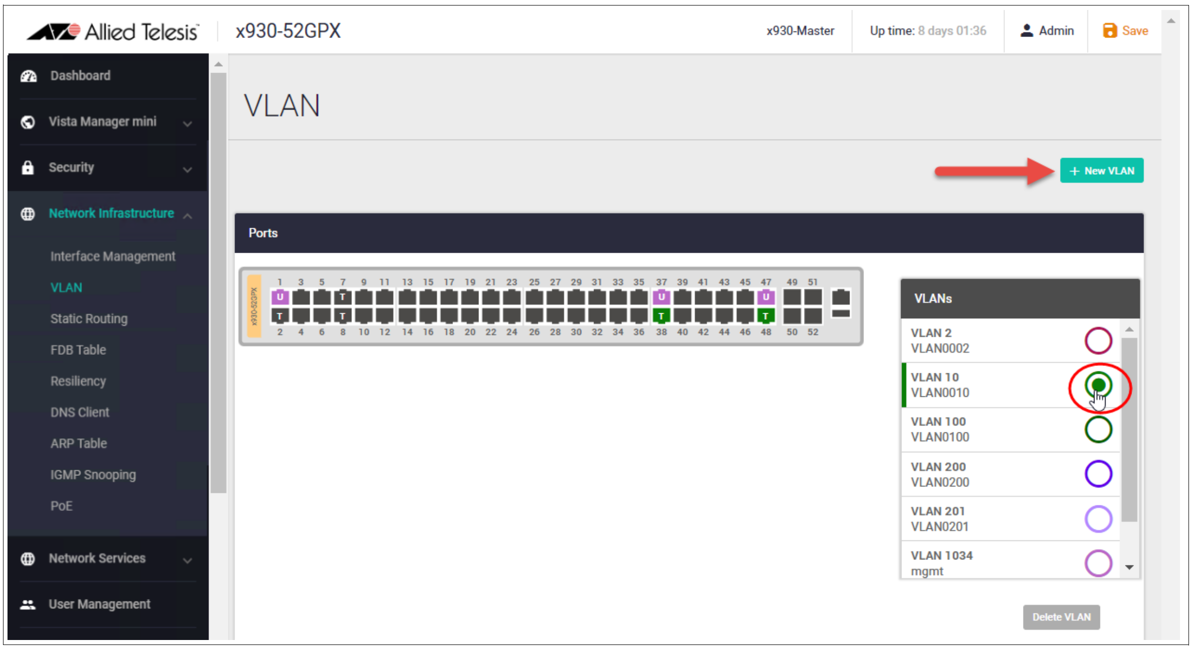
Interface Management



Name	IP Address	Status	Protocol	
eth0	unassigned	admin up	down	Edit
lo	unassigned	admin up	running	Edit
of0	unassigned	admin up	running	Edit
vlan1	unassigned	admin up	running	Edit
vlan2	192.168.2.2/24	admin up	running	Edit

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.

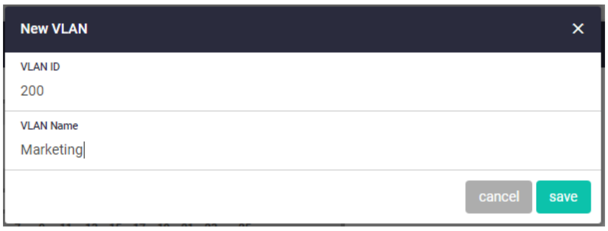
VLAN



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**.



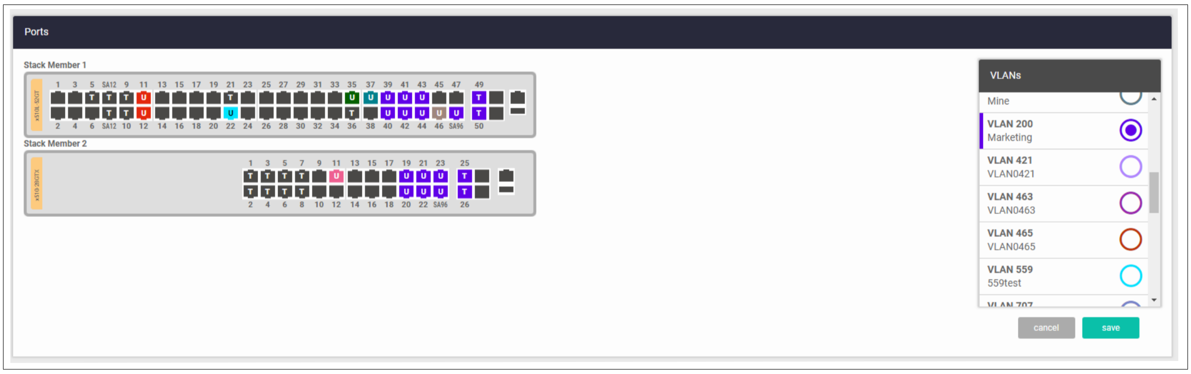
New VLAN

VLAN ID
200

VLAN Name
Marketing

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.

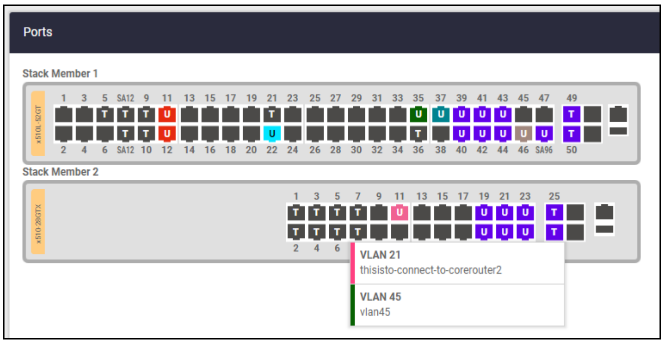
In the example below, VLAN 200 is selected, and it has the color purple assigned to it. When VLAN 200 is selected, all the ports that belong to VLAN 200 are also colored purple in the device images.



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.

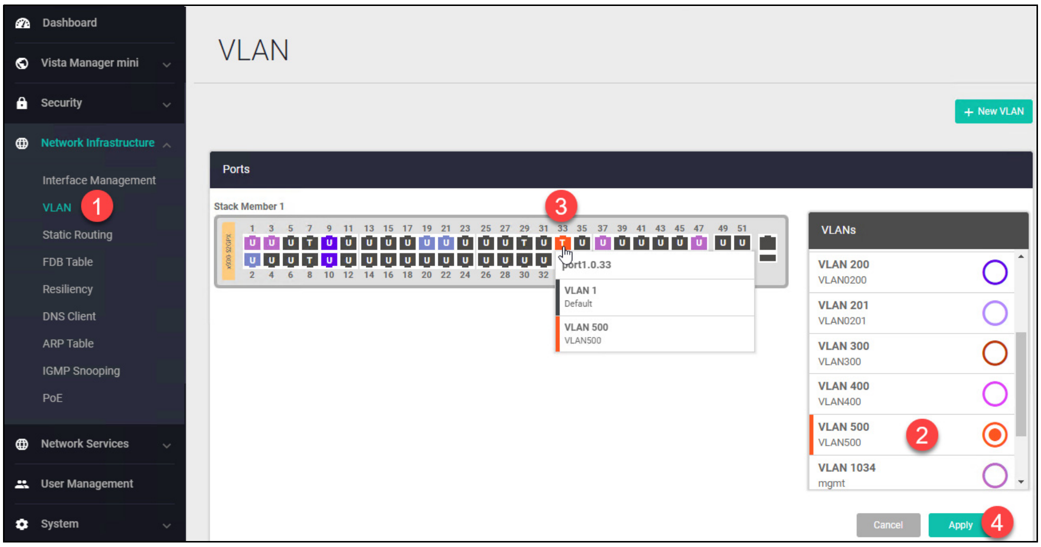
Once a port has a native VLAN, any packets received on the switchport without a VLAN tag are placed into the native VLAN. Packets leaving a switchport on the native VLAN will not be tagged.

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).

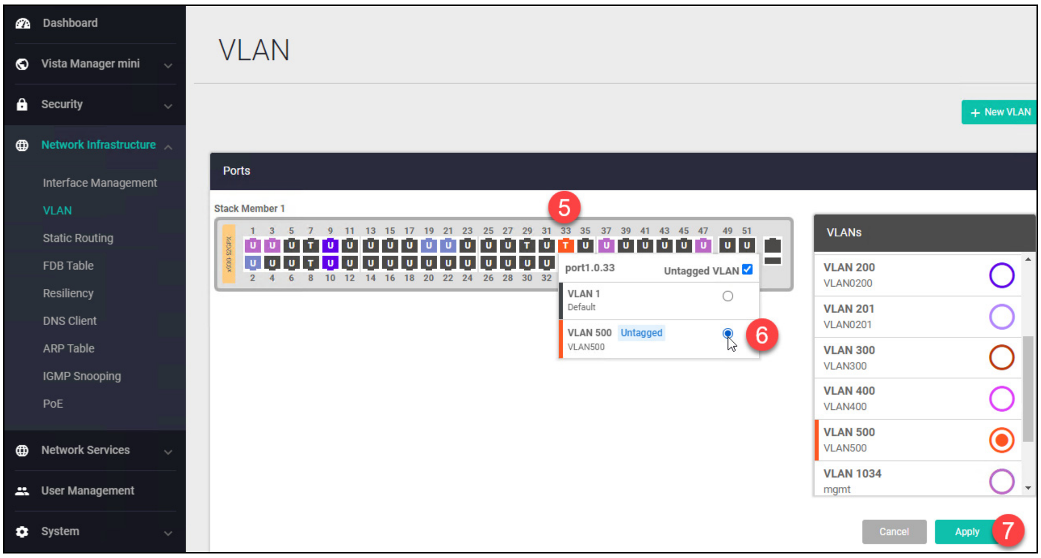
4. Click **Apply** to set the port mode to Trunk.



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.

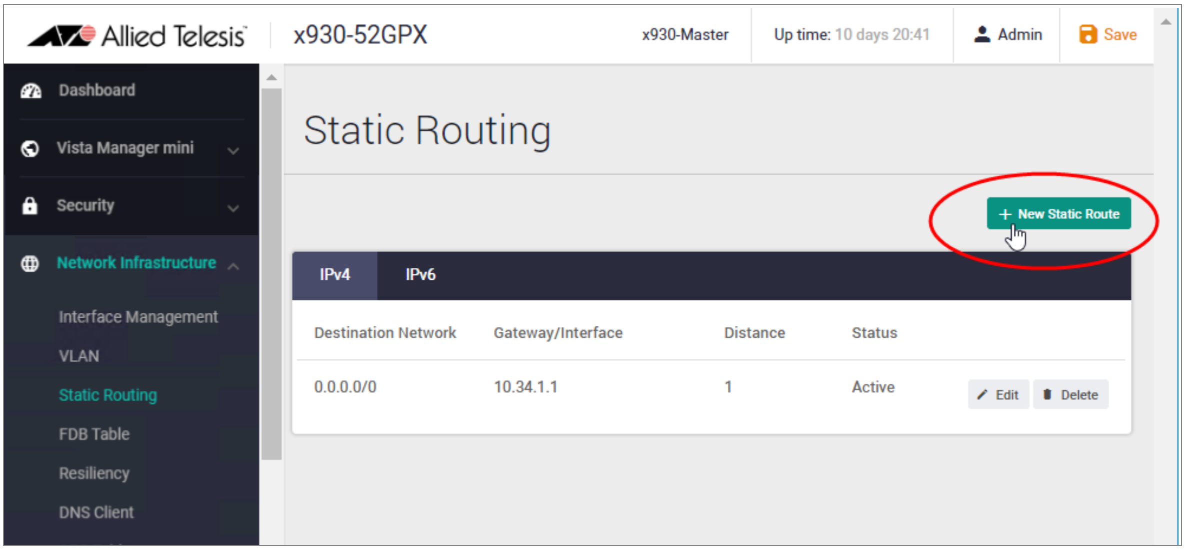
6. In the pop-up, select the VLAN that you want to make the native VLAN.

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.

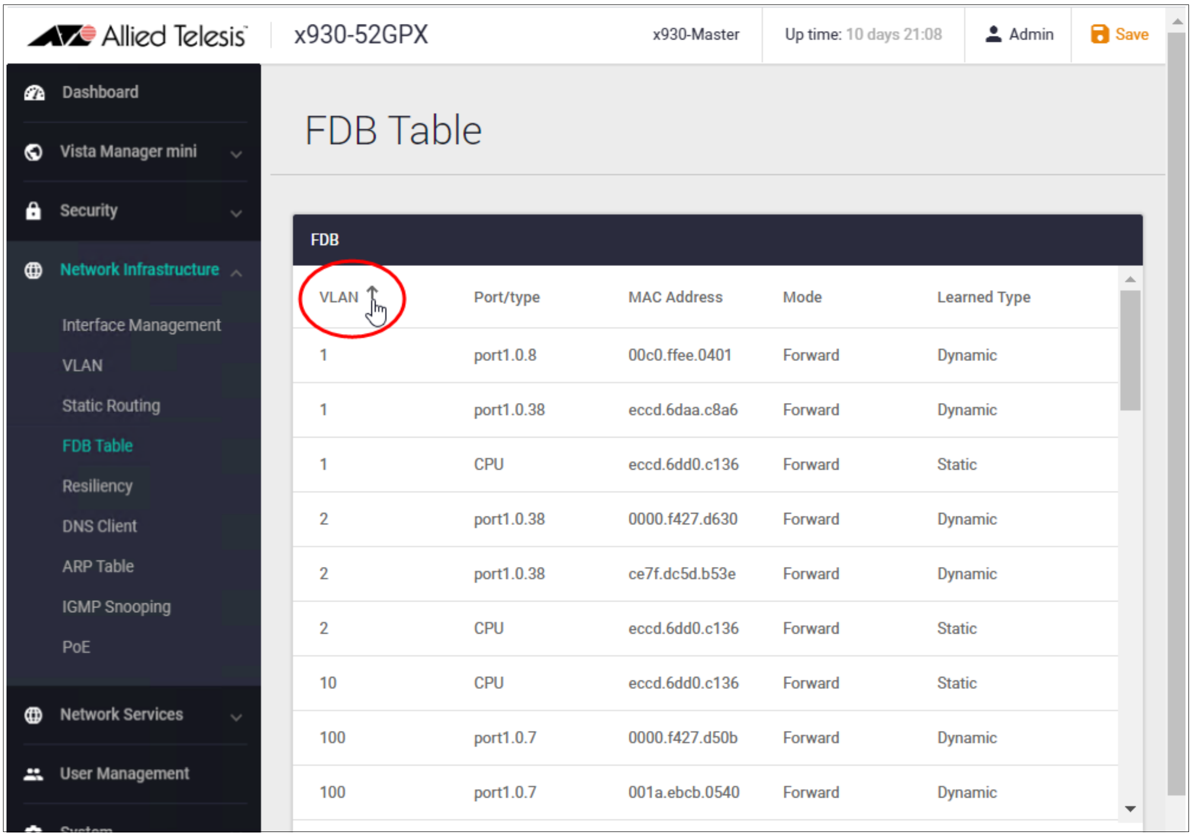


Static Routing

Destination Network	Gateway/Interface	Distance	Status
0.0.0.0/0	10.34.1.1	1	Active

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.



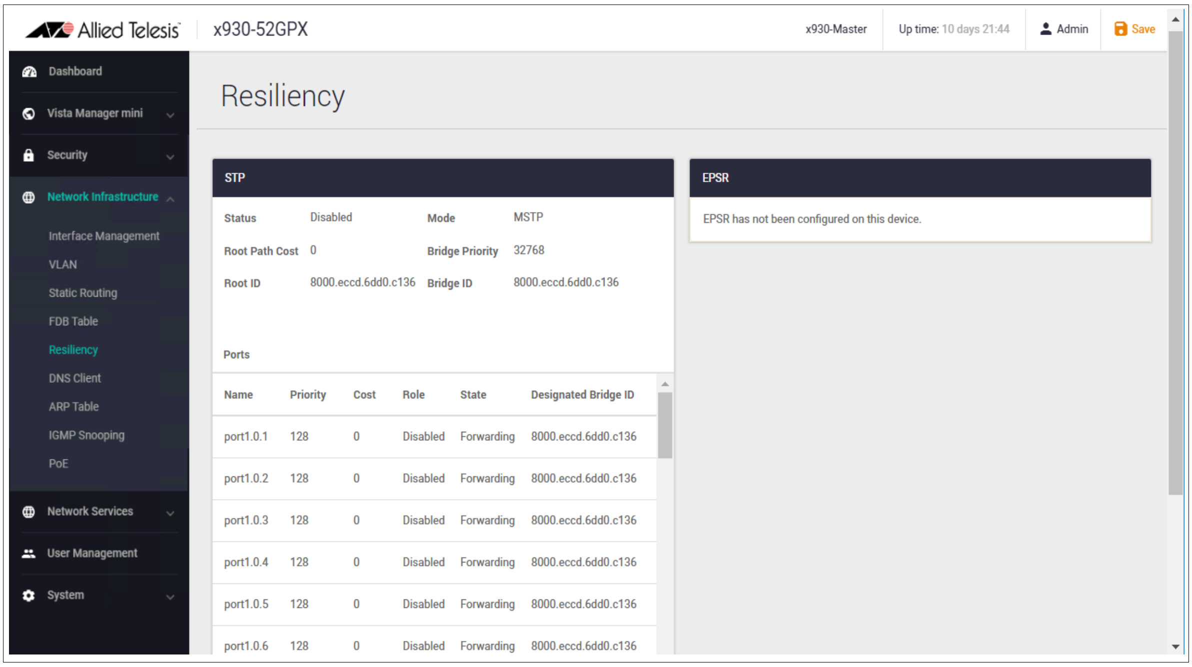
FDB Table

FDB

VLAN	Port/type	MAC Address	Mode	Learned Type
1	port1.0.8	00c0.ffee.0401	Forward	Dynamic
1	port1.0.38	eccd.6daa.c8a6	Forward	Dynamic
1	CPU	eccd.6dd0.c136	Forward	Static
2	port1.0.38	0000.f427.d630	Forward	Dynamic
2	port1.0.38	ce7f.dc5d.b53e	Forward	Dynamic
2	CPU	eccd.6dd0.c136	Forward	Static
10	CPU	eccd.6dd0.c136	Forward	Static
100	port1.0.7	0000.f427.d50b	Forward	Dynamic
100	port1.0.7	001a.ebcb.0540	Forward	Dynamic

Resiliency

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



Resiliency

STP

Status	Disabled	Mode	MSTP
Root Path Cost	0	Bridge Priority	32768
Root ID	8000.eccd.6dd0.c136	Bridge ID	8000.eccd.6dd0.c136

Ports

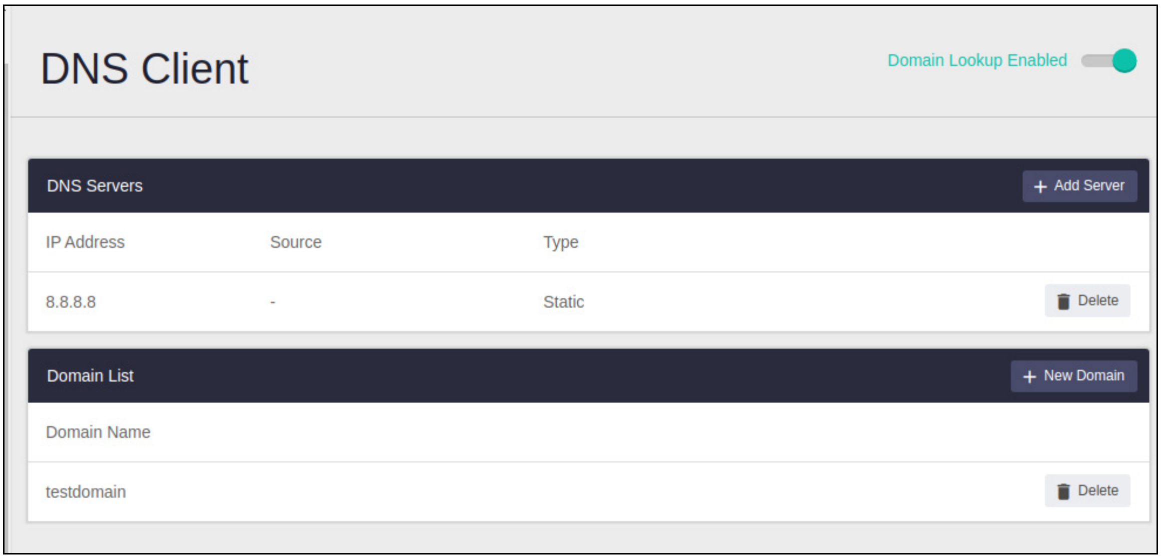
Name	Priority	Cost	Role	State	Designated Bridge ID
port1.0.1	128	0	Disabled	Forwarding	8000.eccd.6dd0.c136
port1.0.2	128	0	Disabled	Forwarding	8000.eccd.6dd0.c136
port1.0.3	128	0	Disabled	Forwarding	8000.eccd.6dd0.c136
port1.0.4	128	0	Disabled	Forwarding	8000.eccd.6dd0.c136
port1.0.5	128	0	Disabled	Forwarding	8000.eccd.6dd0.c136
port1.0.6	128	0	Disabled	Forwarding	8000.eccd.6dd0.c136

EPSR

EPSR has not been configured on this 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.



DNS Client

Domain Lookup Enabled

DNS Servers

IP Address	Source	Type
8.8.8.8	-	Static

Domain List

Domain Name
testdomain

Domain List

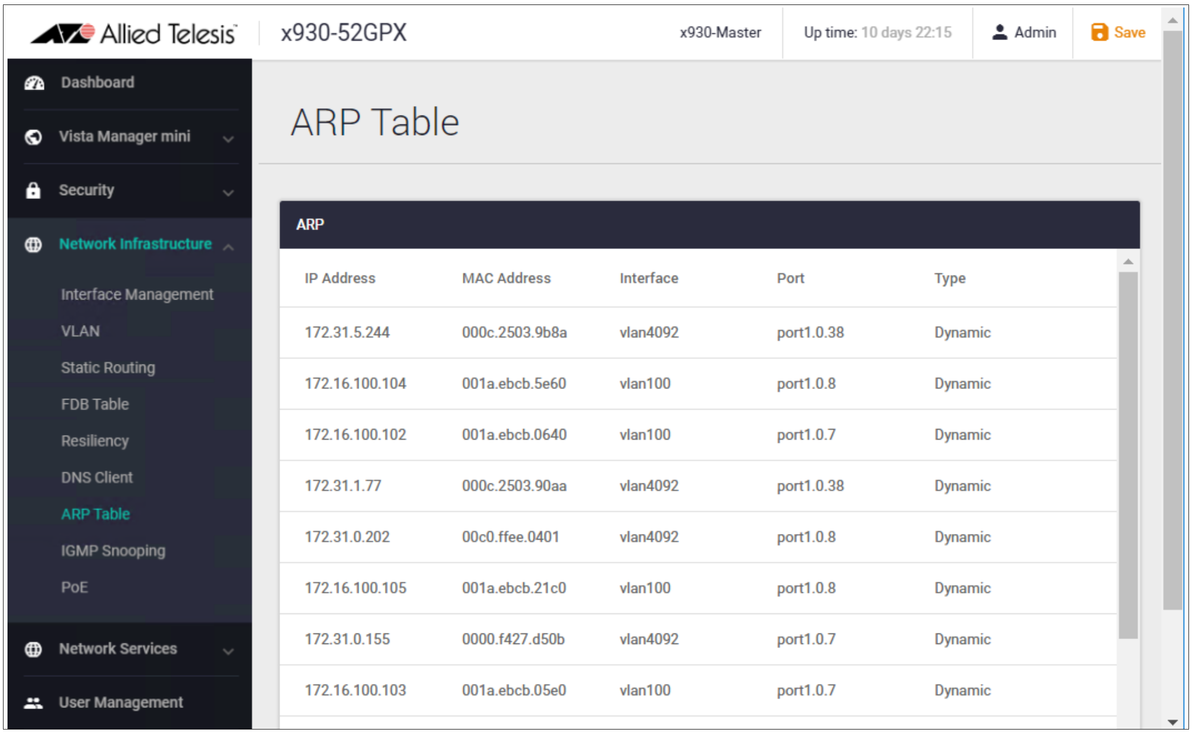
From version 2.16.0 onwards, the **Domain List** category is visible under the DNS Servers table on the **DNS Client** page. You can add and delete domains on this table.

The **DNS Servers** table now shows the **Source** column, which is the source that the DNS server's IP is learned from.

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.



ARP Table

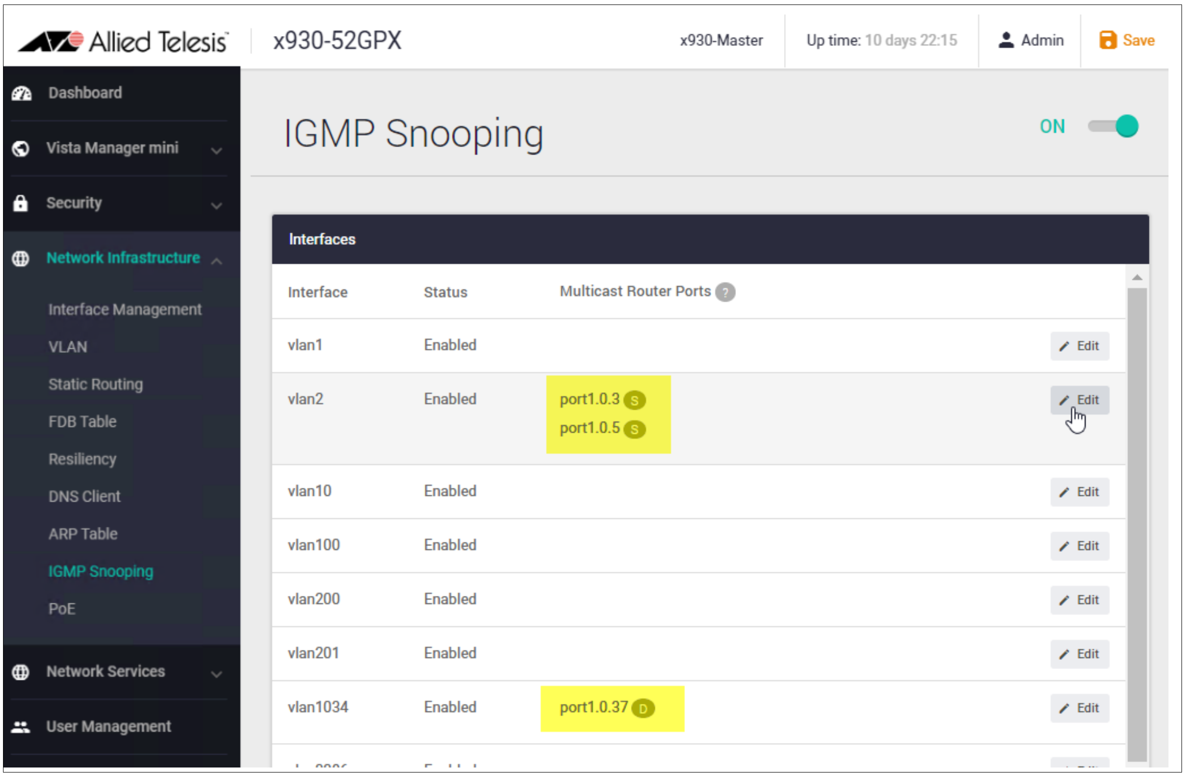
ARP

IP Address	MAC Address	Interface	Port	Type
172.31.5.244	000c.2503.9b8a	vlan4092	port1.0.38	Dynamic
172.16.100.104	001a.ebcb.5e60	vlan100	port1.0.8	Dynamic
172.16.100.102	001a.ebcb.0640	vlan100	port1.0.7	Dynamic
172.31.1.77	000c.2503.90aa	vlan4092	port1.0.38	Dynamic
172.31.0.202	00c0.ffee.0401	vlan4092	port1.0.8	Dynamic
172.16.100.105	001a.ebcb.21c0	vlan100	port1.0.8	Dynamic
172.31.0.155	0000.f427.d50b	vlan4092	port1.0.7	Dynamic
172.16.100.103	001a.ebcb.05e0	vlan100	port1.0.7	Dynamic

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).

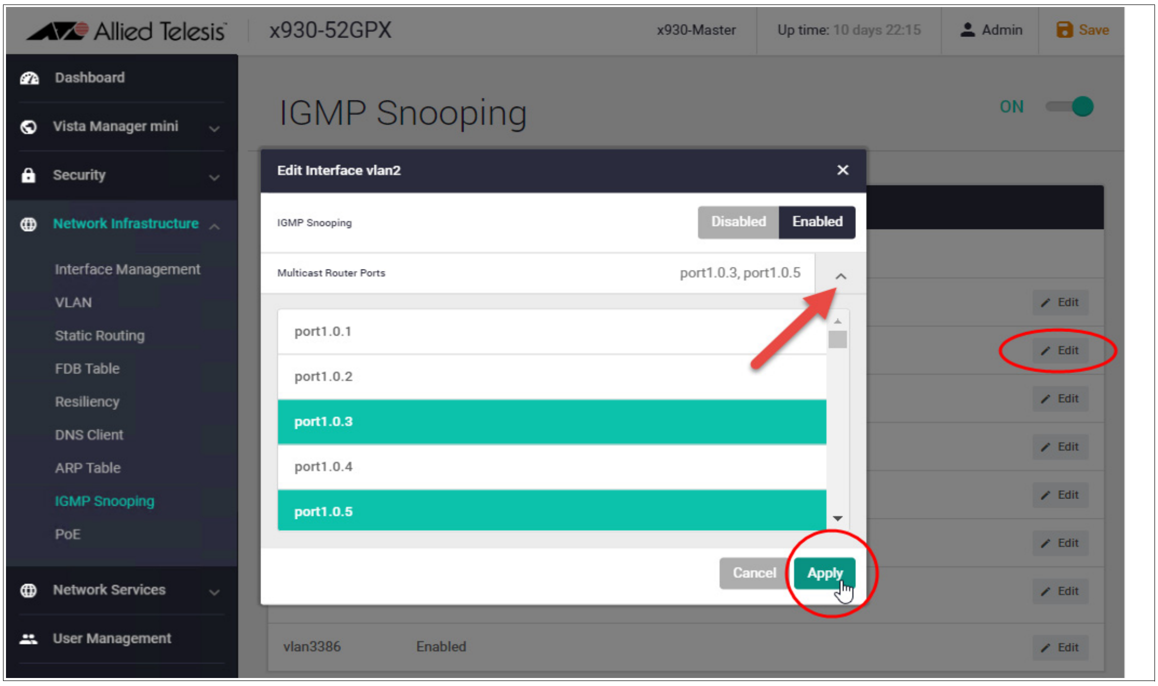
The IGMP Snooping window displays interfaces, their status, and the configured multicast ports.



Interface	Status	Multicast Router Ports	
vlan1	Enabled		Edit
vlan2	Enabled	port1.0.3 S port1.0.5 S	Edit
vlan10	Enabled		Edit
vlan100	Enabled		Edit
vlan200	Enabled		Edit
vlan201	Enabled		Edit
vlan1034	Enabled	port1.0.37 D	Edit

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**.



Edit Interface vlan2

IGMP Snooping: Disabled [✓ Enabled]

Multicast Router Ports: port1.0.3, port1.0.5

PoE

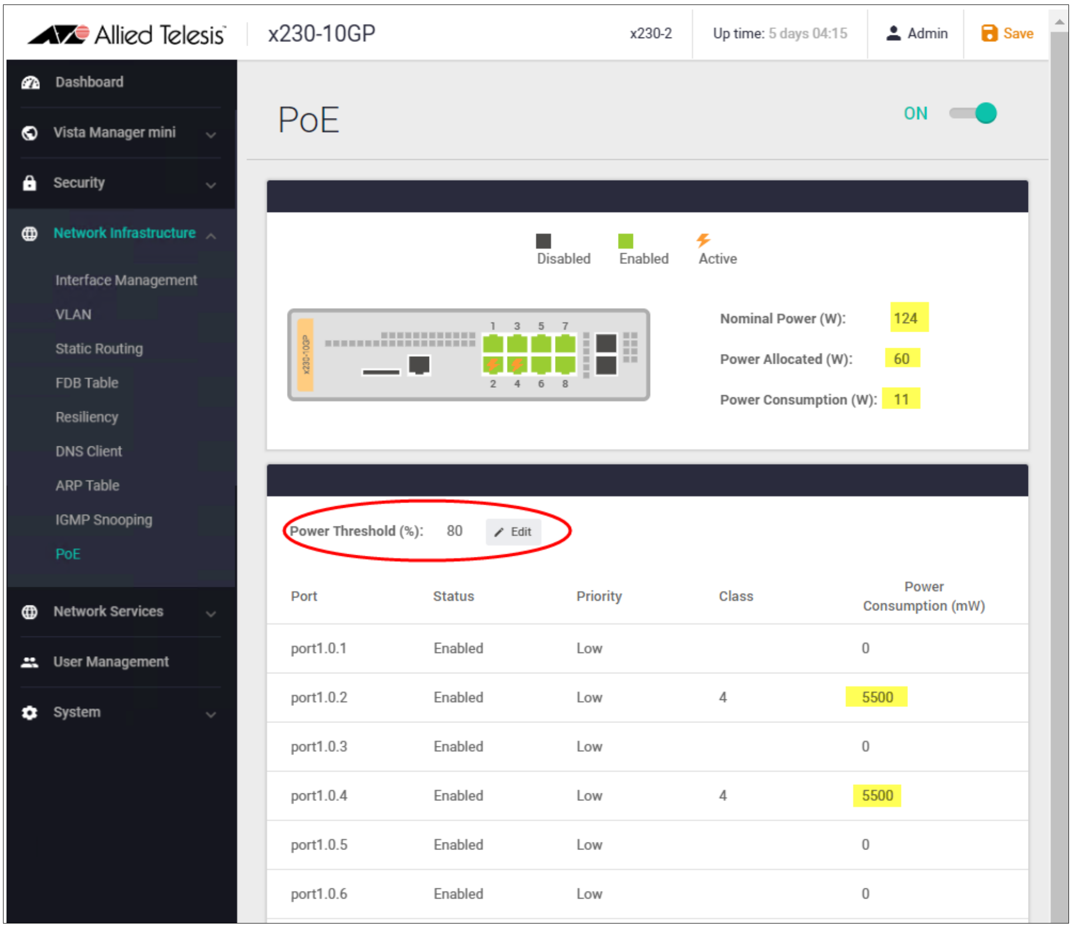
You can use the PoE page to:

- 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%.



Nominal Power (W): 124

Power Allocated (W): 60

Power Consumption (W): 11

Power Threshold (%): 80

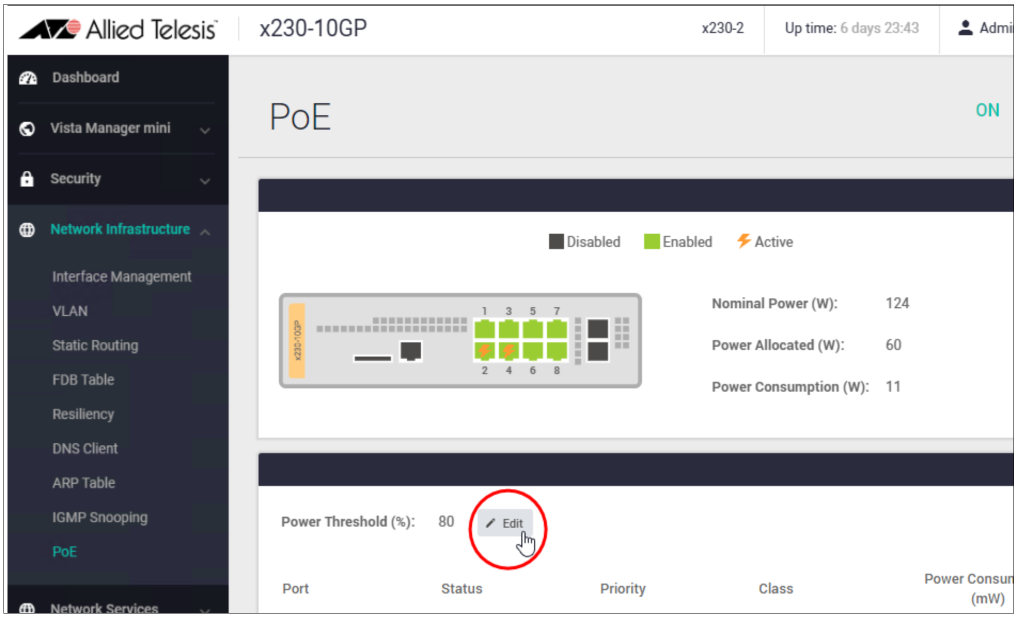
Port	Status	Priority	Class	Power Consumption (mW)
port1.0.1	Enabled	Low		0
port1.0.2	Enabled	Low	4	5500
port1.0.3	Enabled	Low		0
port1.0.4	Enabled	Low	4	5500
port1.0.5	Enabled	Low		0
port1.0.6	Enabled	Low		0

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**.

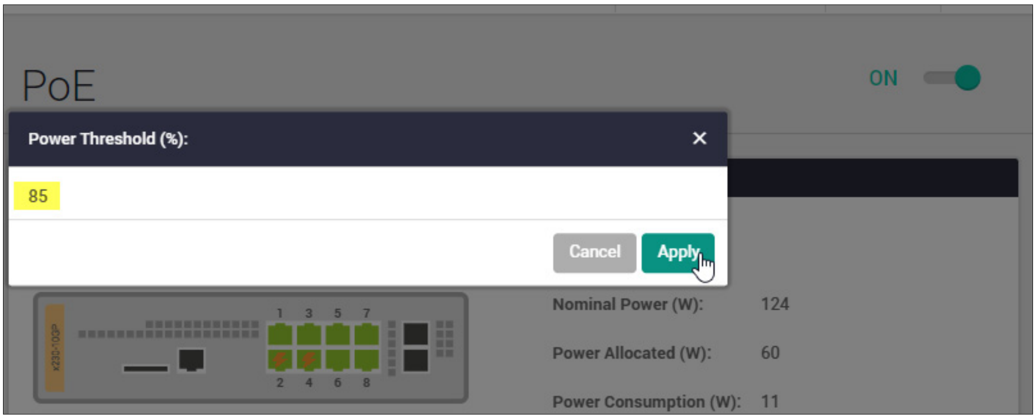
To change the power threshold setting:

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



Nominal Power (W): 124
Power Allocated (W): 60
Power Consumption (W): 11
Power Threshold (%): 80

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



Power Threshold (%): 85

Nominal Power (W): 124
Power Allocated (W): 60
Power Consumption (W): 11

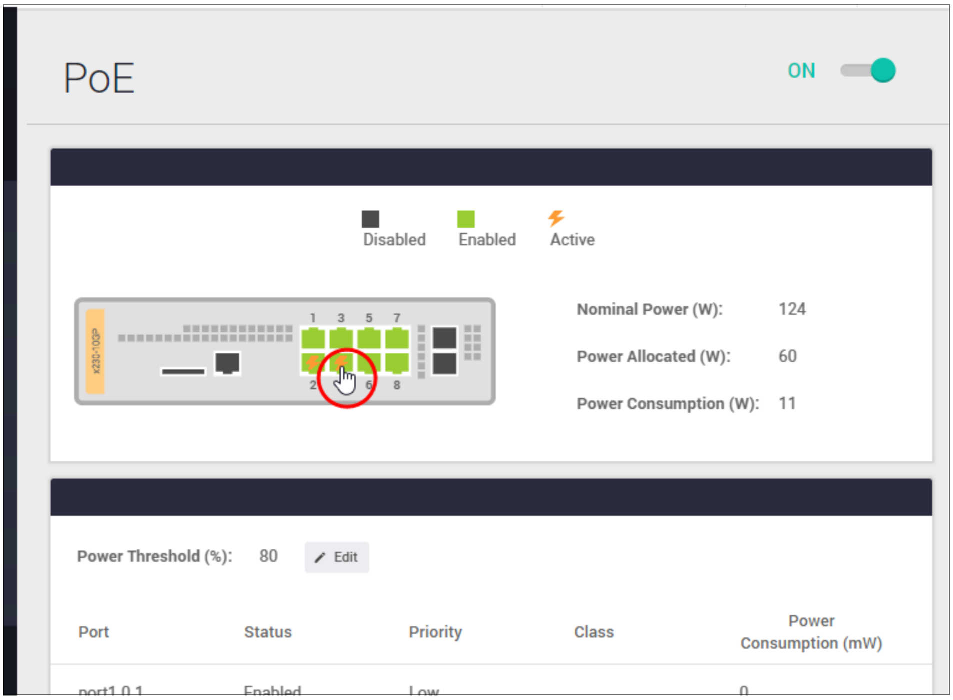
Configure the power priority per interface

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).



PoE

ON

■ Disabled 🟩 Enabled ⚡ Active

Nominal Power (W): 124

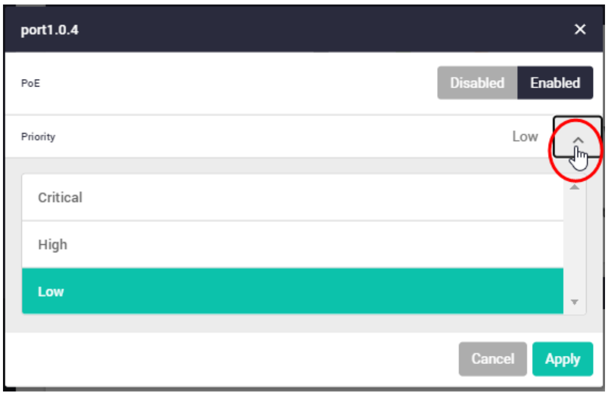
Power Allocated (W): 60

Power Consumption (W): 11

Power Threshold (%): 80

Port	Status	Priority	Class	Power Consumption (mW)
port1.0.1	Enabled	Low		0

- The port detail window opens.



port1.0.4

PoE: Disabled [✓ Enabled]

Priority: Low

- 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.

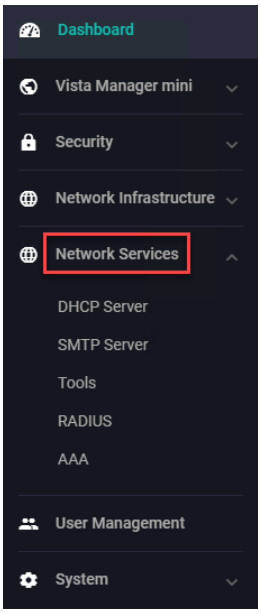
Low: The lowest priority level. This is the default setting. Ports set to Low level only receive power if all the ports assigned to the other two levels are already receiving power.

- Click **Apply**.

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

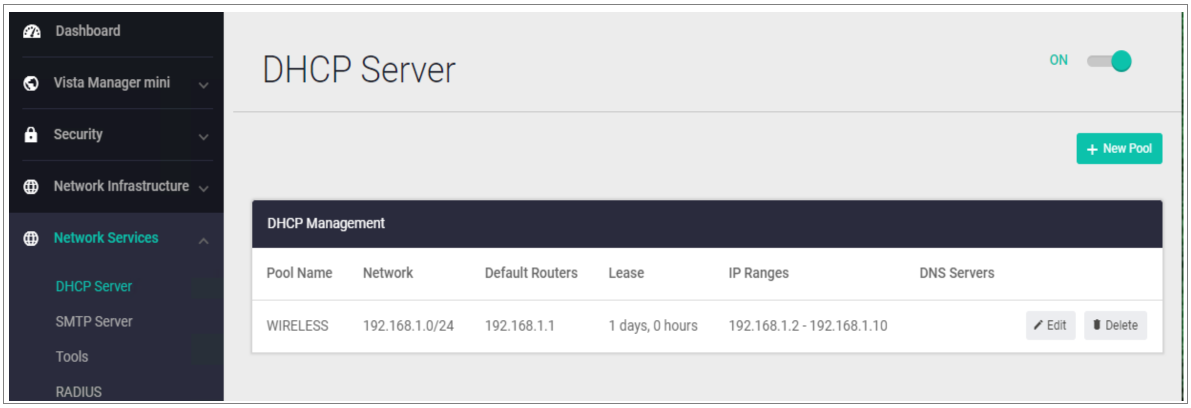
Network Services menu

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.

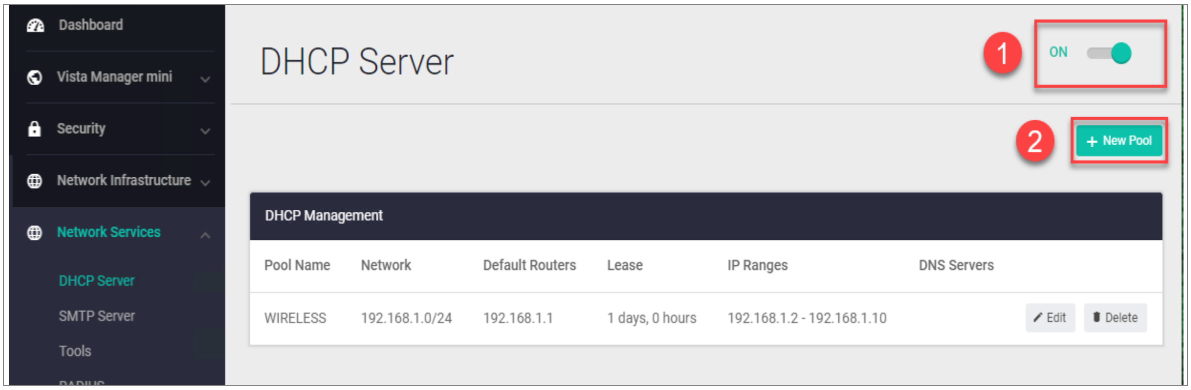


Pool Name	Network	Default Routers	Lease	IP Ranges	DNS Servers	
WIRELESS	192.168.1.0/24	192.168.1.1	1 days, 0 hours	192.168.1.2 - 192.168.1.10		Edit Delete

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.

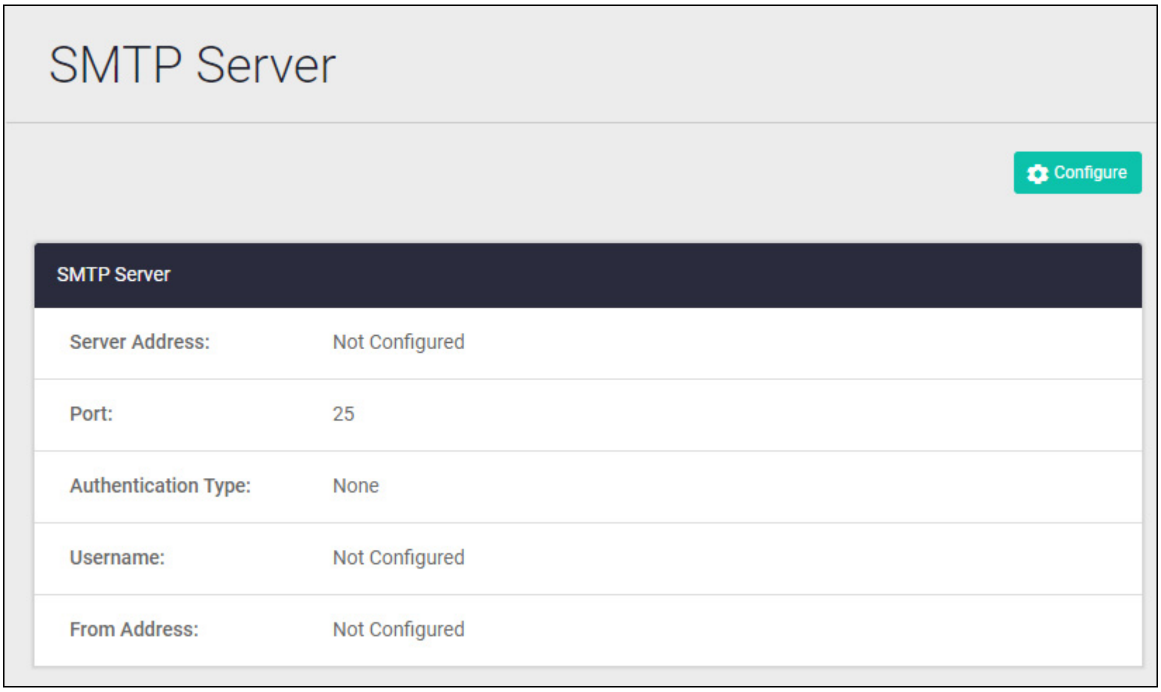


Pool Name	Network	Default Routers	Lease	IP Ranges	DNS Servers	
WIRELESS	192.168.1.0/24	192.168.1.1	1 days, 0 hours	192.168.1.2 - 192.168.1.10		Edit Delete

- 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.

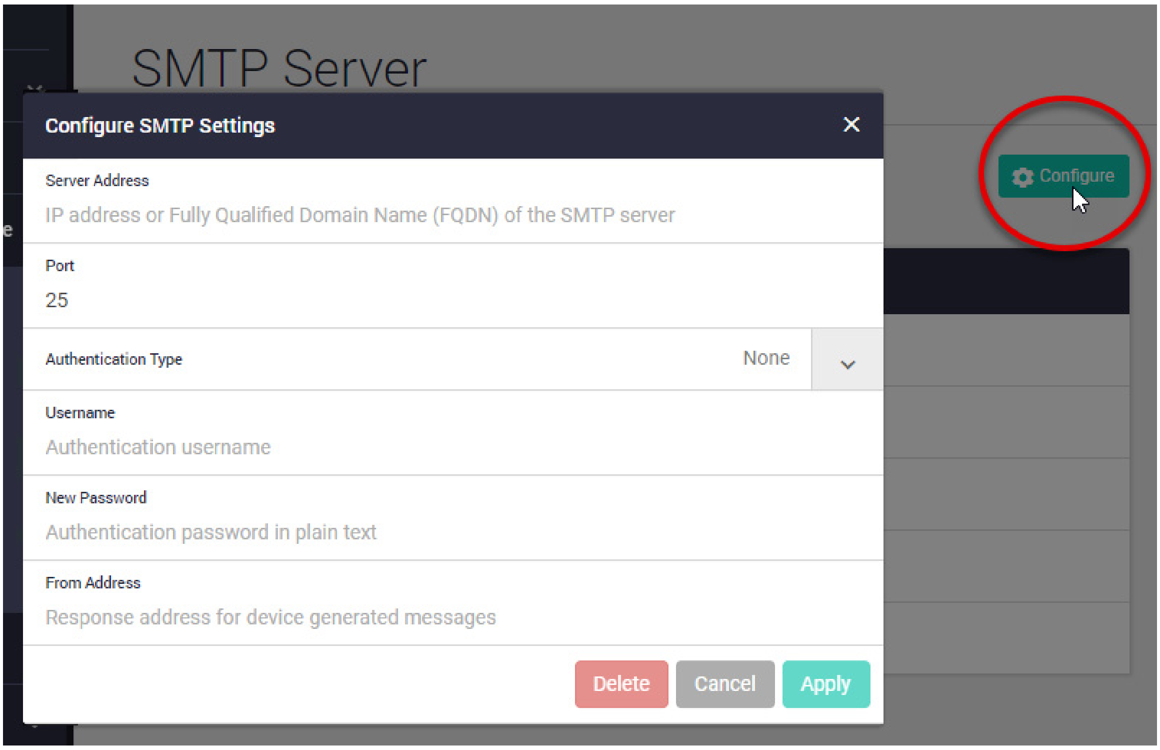


SMTP Server

SMTP Server

Server Address:	Not Configured
Port:	25
Authentication Type:	None
Username:	Not Configured
From Address:	Not Configured

To configure the SMTP settings, click **Configure**.



Configure SMTP Settings

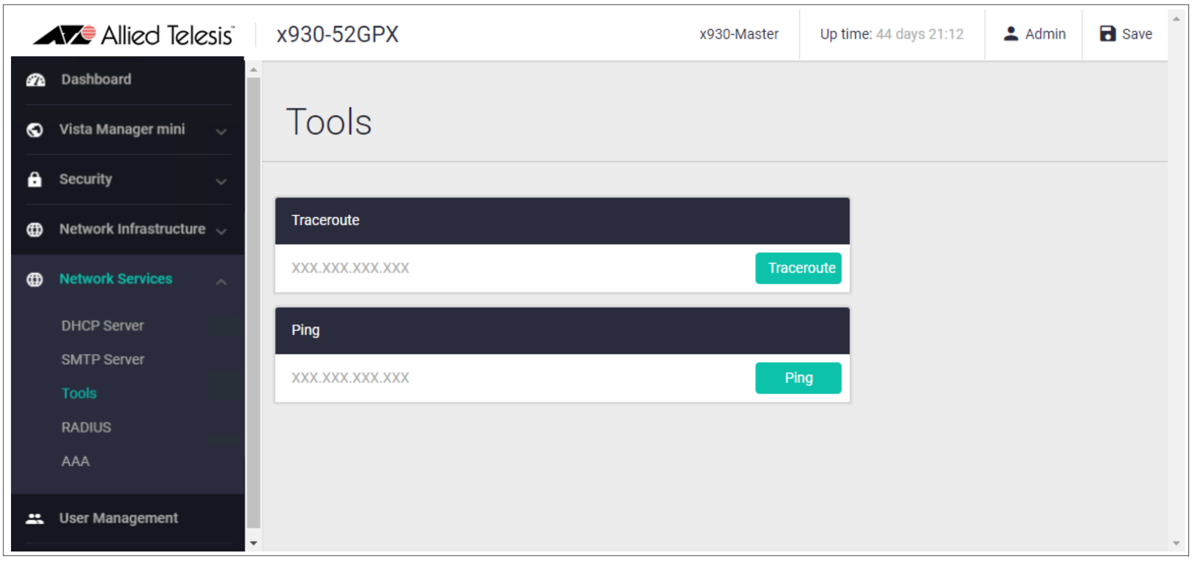
Server Address	IP address or Fully Qualified Domain Name (FQDN) of the SMTP server
Port	25
Authentication Type	None
Username	Authentication username
New Password	Authentication password in plain text
From Address	Response address for device generated messages

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

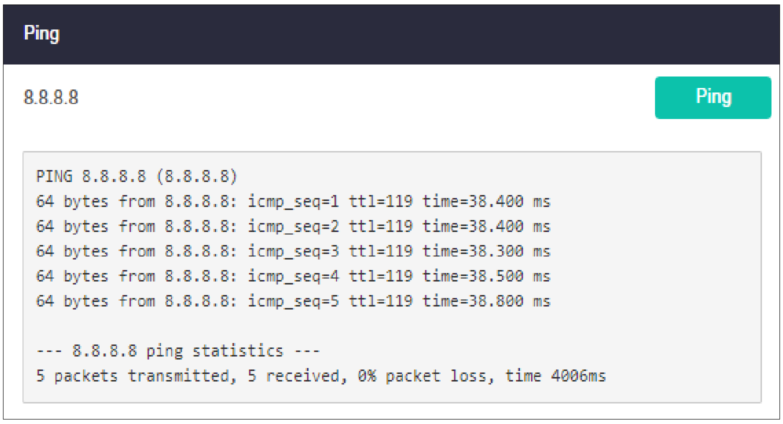
To add email filters, see "Logging" on page 43.

Tools

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

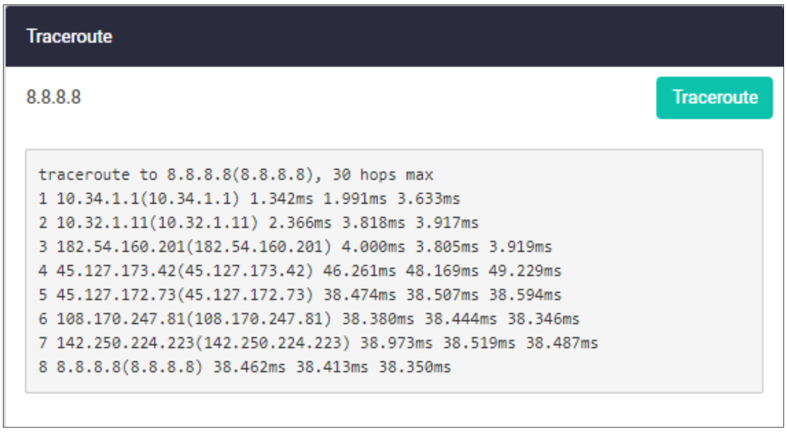


For example, shown here is a Ping of the IP address 8.8.8.8 (the Google public DNS service), and the results of 5 ICMP packets sent and received.



```
PING 8.8.8.8 (8.8.8.8)
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=38.400 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=38.400 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=38.300 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=38.500 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=38.800 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
```

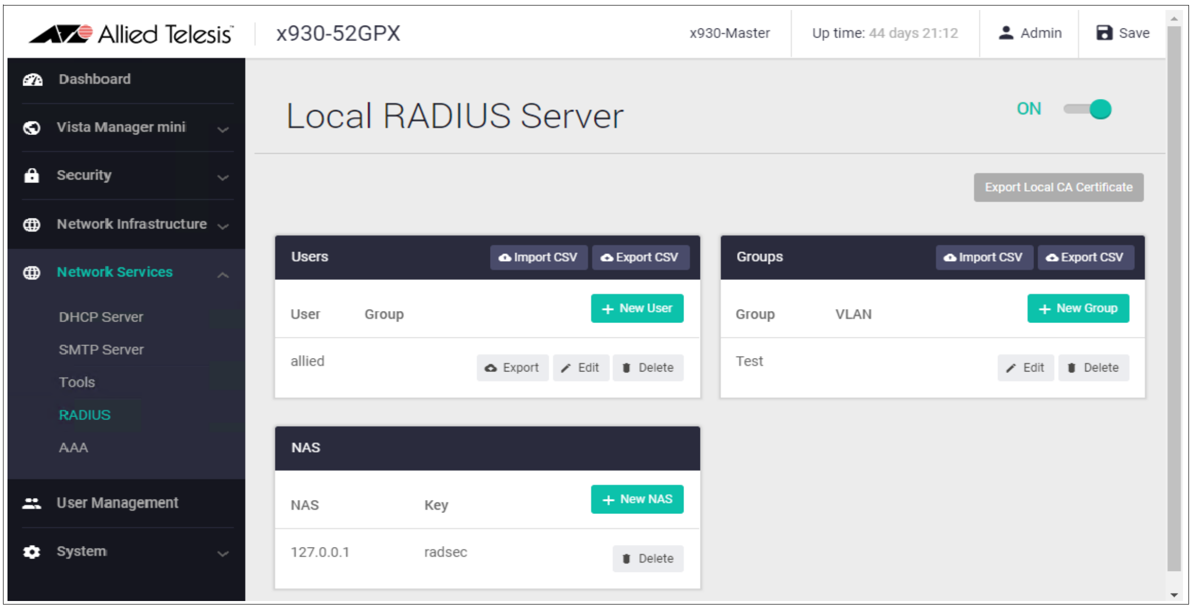
Here is the Traceroute to IP address 8.8.8.8, and the path taken to reach the closest Google DNS server.



```
traceroute to 8.8.8.8(8.8.8.8), 30 hops max
1 10.34.1.1(10.34.1.1) 1.342ms 1.991ms 3.633ms
2 10.32.1.11(10.32.1.11) 2.366ms 3.818ms 3.917ms
3 182.54.160.201(182.54.160.201) 4.000ms 3.805ms 3.919ms
4 45.127.173.42(45.127.173.42) 46.261ms 48.169ms 49.229ms
5 45.127.172.73(45.127.172.73) 38.474ms 38.507ms 38.594ms
6 108.170.247.81(108.170.247.81) 38.380ms 38.444ms 38.346ms
7 142.250.224.223(142.250.224.223) 38.973ms 38.519ms 38.487ms
8 8.8.8.8(8.8.8.8) 38.462ms 38.413ms 38.350ms
```

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.



Users

User	Group
allied	

Groups

Group	VLAN
Test	

NAS

NAS	Key
127.0.0.1	radsec

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.

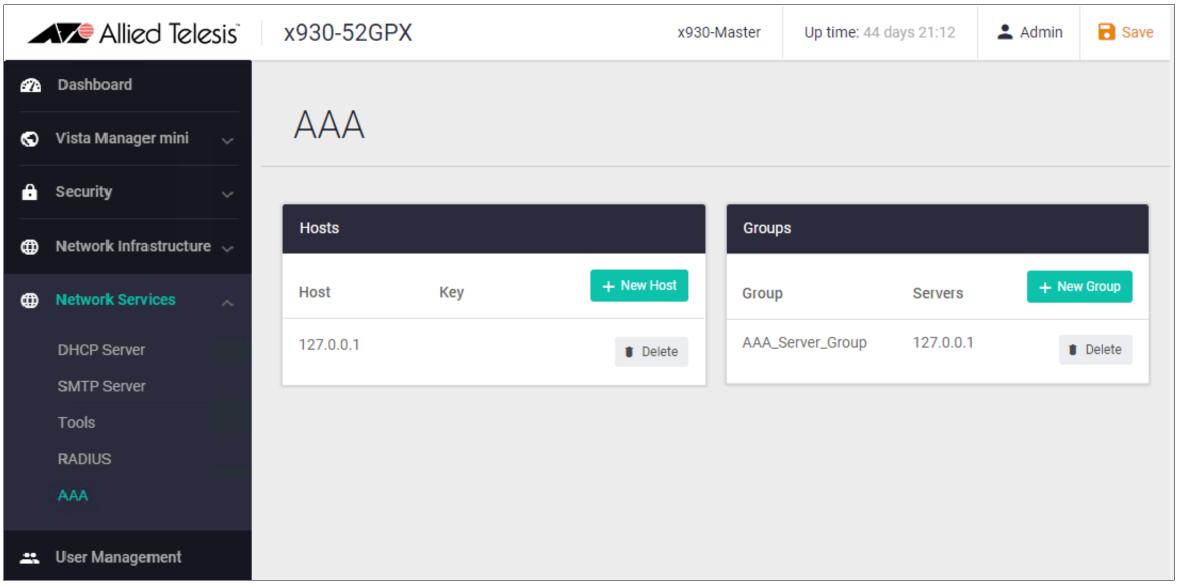
For more detailed information on configuring a local RADIUS server, see the Local RADIUS Server Feature Overview and Configuration Guide.

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.



AAA

Hosts

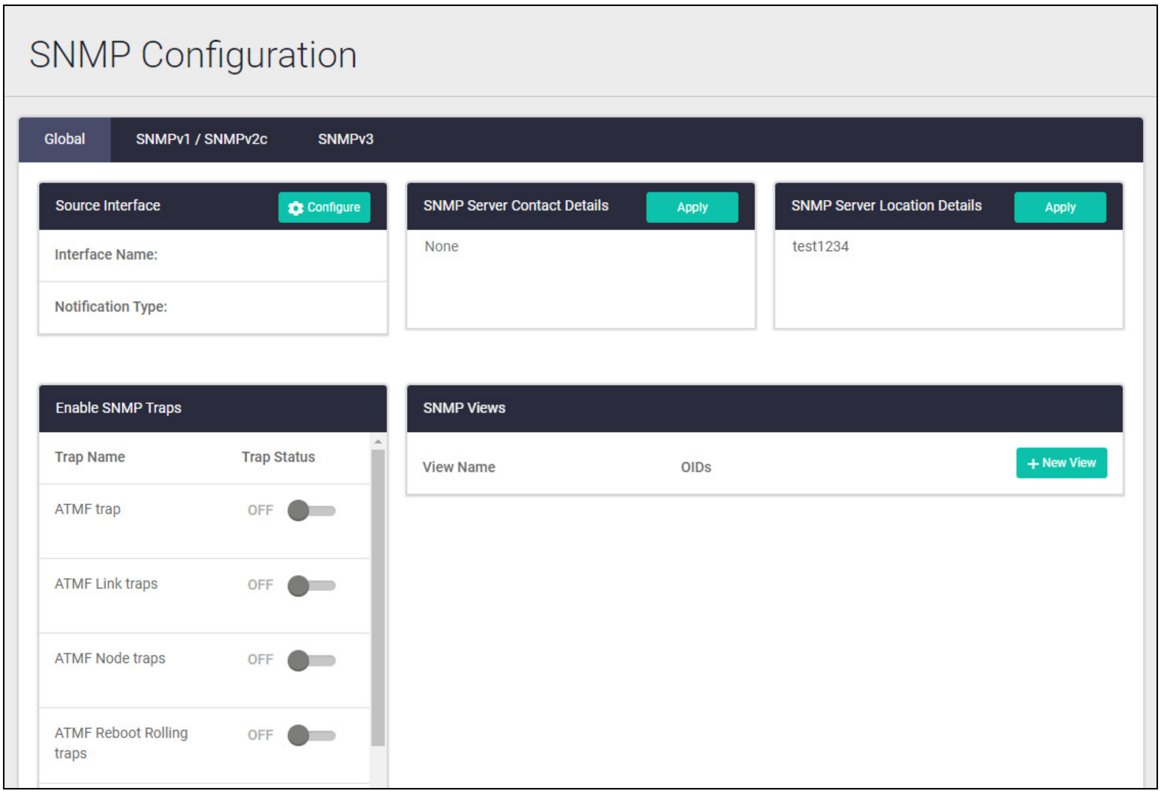
Host	Key
127.0.0.1	

Groups

Group	Servers
AAA_Server_Group	127.0.0.1

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.

SNMP

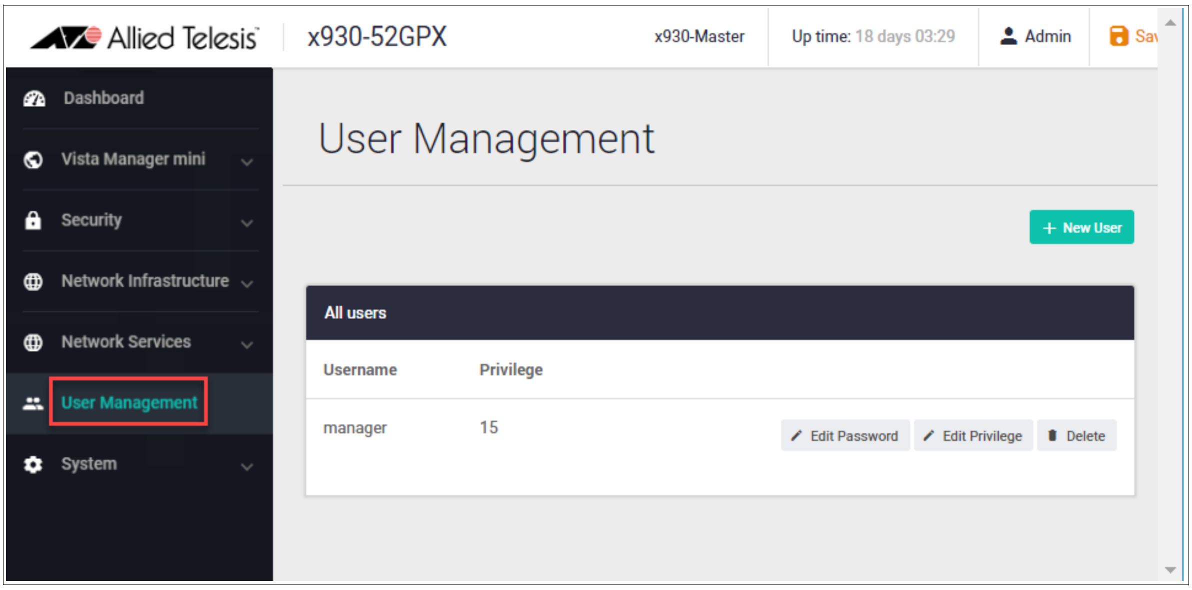


You can configure SNMP and SNMP Traps through this menu.

- Click **Configure** to add a Source Interface.
- Click **Apply** to add either Location or Contact Details.
- Add SNMP Views by clicking **+ New View**
- Toggle specific **SNMP Traps** on/off from this menu using the toggle buttons.

User Management menu

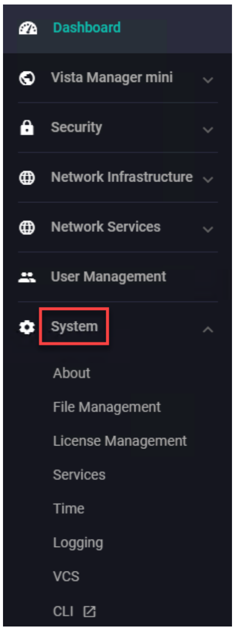
The User Management menu lets you add a new user, and set a user password and privilege level: either 1-14 (limited access) or 15 (full access).



All users

Username	Privilege
manager	15

System menu



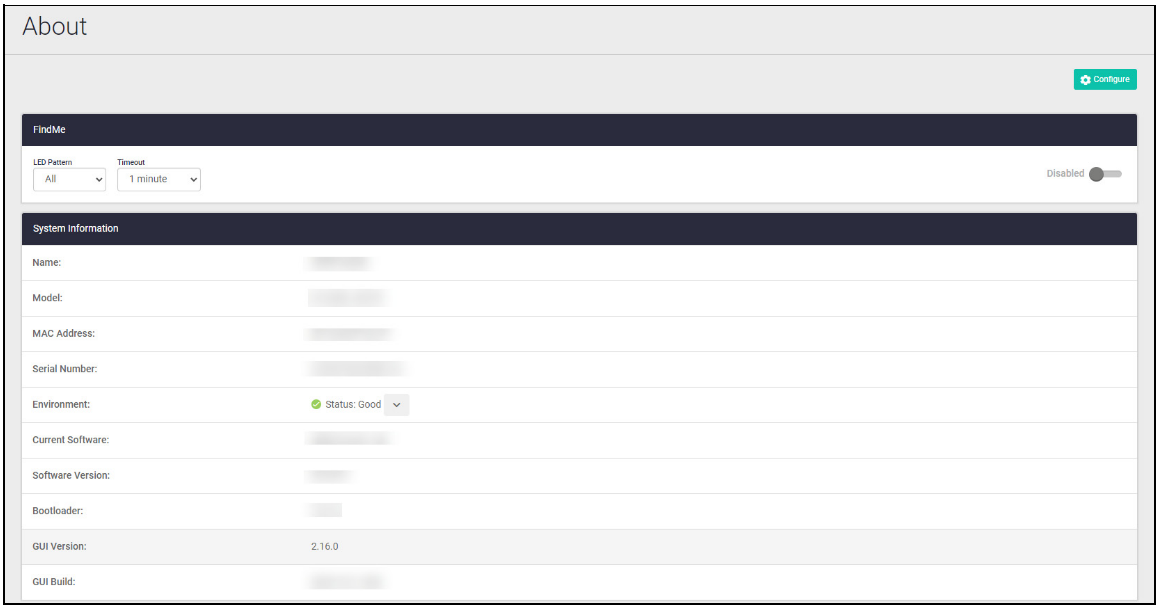
The System menu provides access to information about your device, file management, license management, services, time, logging, VCS, and a CLI window.

About

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

This includes:

- The device’s Hostname
- Model
- MAC Address
- Serial Number
- Environment
- Current Software file
- Software Version
- Bootloader
- GUI Version
- GUI Build



About

FindMe

LED Pattern: All

Timeout: 1 minute

Disabled

System Information

Name:	[redacted]
Model:	[redacted]
MAC Address:	[redacted]
Serial Number:	[redacted]
Environment:	✓ Status: Good
Current Software:	[redacted]
Software Version:	[redacted]
Bootloader:	[redacted]
GUI Version:	2.16.0
GUI Build:	[redacted]

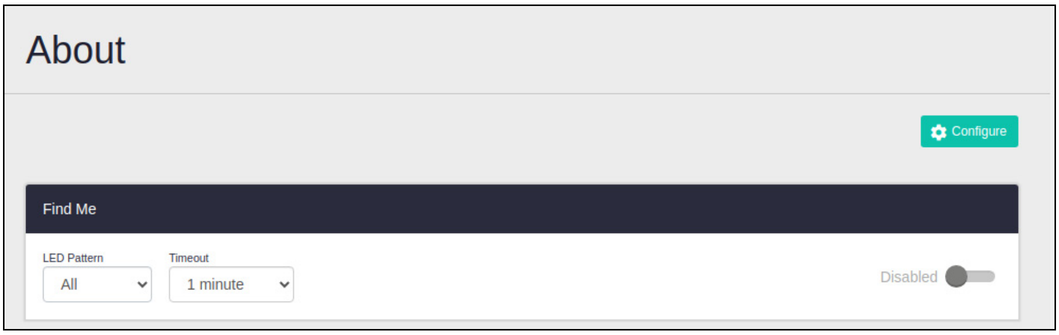
You can optionally use the Configure button to add a device’s contact and server location, and to change the GUI timeout.

Note: Screenshotting this information is very helpful in the event of a problem, to assist Allied Telesis support.

Finding a device in a server room

From version 2.16.0 onwards, you can use the Find Me feature to locate a device. When you enable Find Me, all ports on your device will flash based on the pattern that you select.

On the **About** page, click the toggle next to the Find Me table to enable Find Me.



LED Pattern: All

Timeout: 1 minute

You can set the LED pattern and timeout in order to find what device you are currently using.

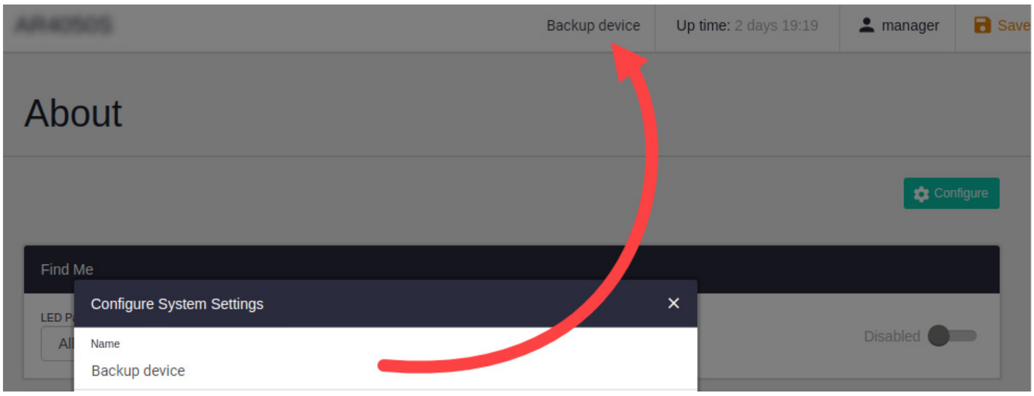
- Note that you cannot specify individual ports or individual VCStack members.

Changing hostname:

From version 2.16.0 onwards, you can change your device's hostname from the About page. The hostname change will be reflected on the Device GUI's header at the top of the page.

To use this feature:

- Navigate to the **About** page from the System menu.
- Select the **Configure** button.



Name: Backup device

This will bring up the Configure System Settings window. You can type a new hostname in the window.

Configuring the contact and server location:

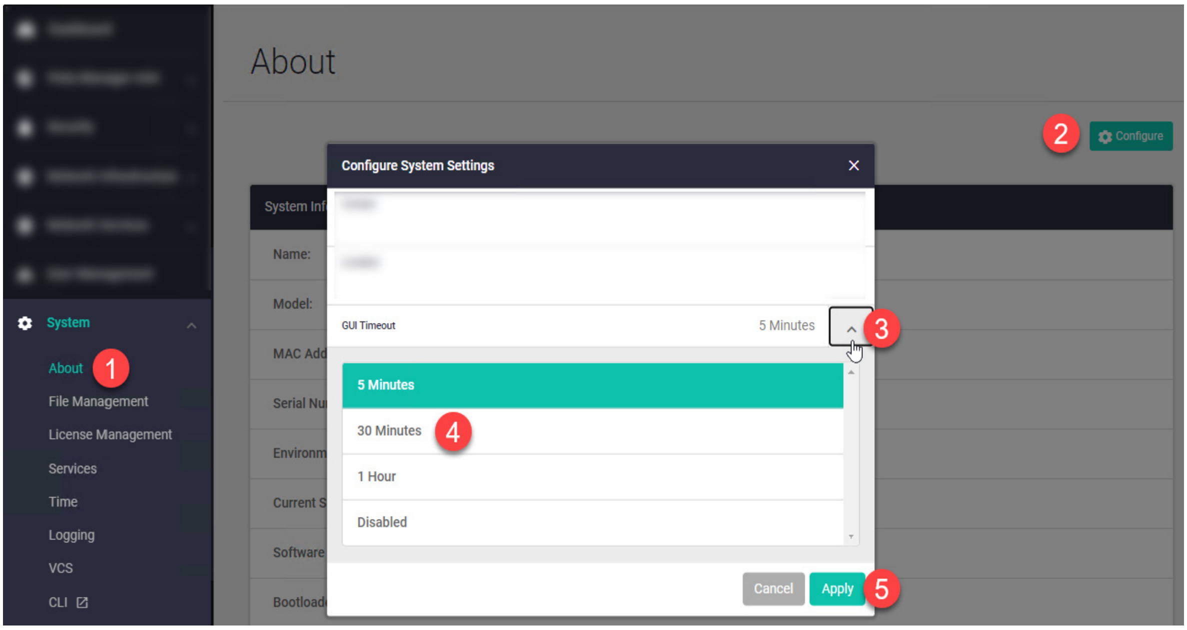
1. Click the green **Configure** button on the top-right.
2. Type in the **Contact** and **Location** details.
3. Click **Apply**.

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**.

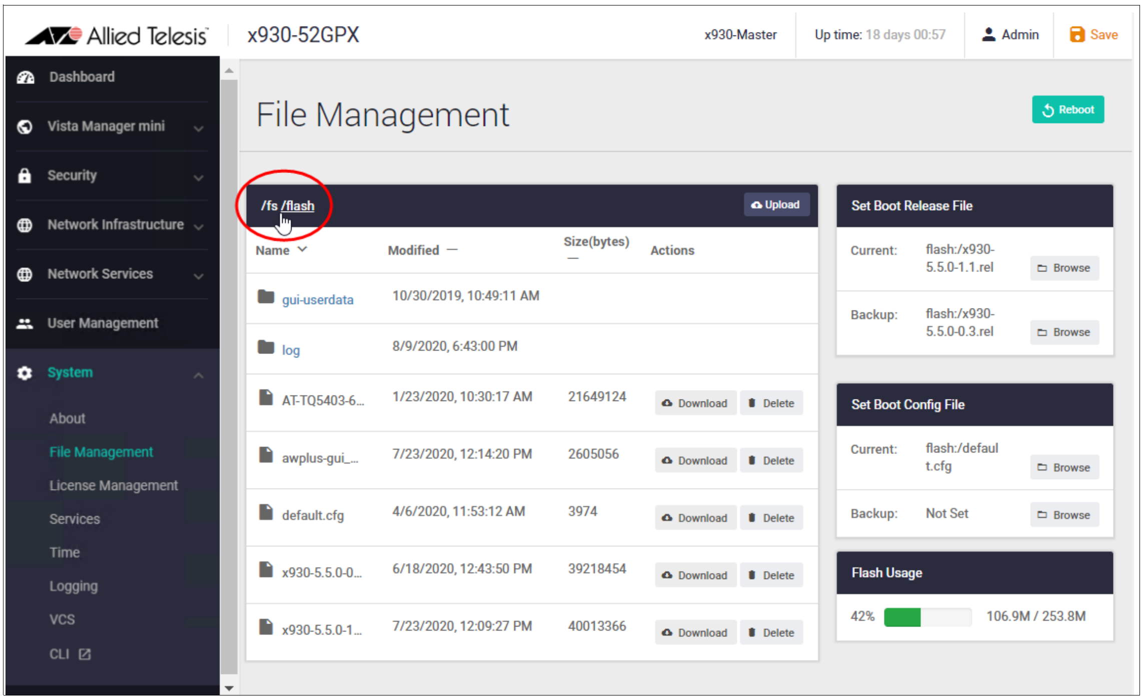


GUI Timeout 5 Minutes

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.



Name	Modified	Size(bytes)	Actions
gui-userdata	10/30/2019, 10:49:11 AM		
log	8/9/2020, 6:43:00 PM		
AT-TQ5403-6...	1/23/2020, 10:30:17 AM	21649124	Download Delete
awplus-gui_...	7/23/2020, 12:14:20 PM	2605056	Download Delete
default.cfg	4/6/2020, 11:53:12 AM	3974	Download Delete
x930-5.5.0-0...	6/18/2020, 12:43:50 PM	39218454	Download Delete
x930-5.5.0-1...	7/23/2020, 12:09:27 PM	40013366	Download Delete

Set Boot Release File
Current: flash:/x930-5.5.0-1.1.rel
Backup: flash:/x930-5.5.0-0.3.rel

Set Boot Config File
Current: flash:/default.cfg
Backup: Not Set

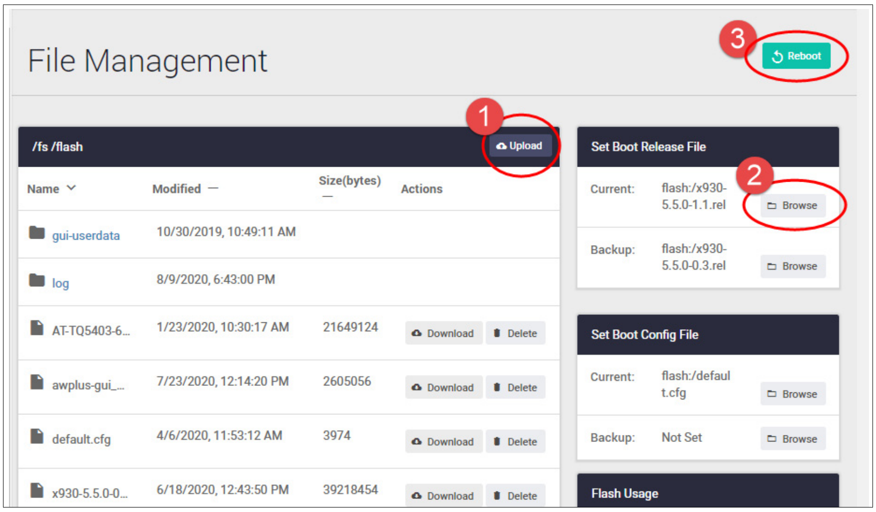
Flash Usage
42% 106.9M / 253.8M

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.

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.

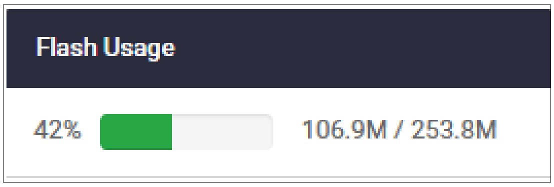


Name	Modified	Size(bytes)	Actions
gui-userdata	10/30/2019, 10:49:11 AM		
log	8/9/2020, 6:43:00 PM		
AT-TQ5403-6...	1/23/2020, 10:30:17 AM	21649124	Download Delete
awplus-gui_...	7/23/2020, 12:14:20 PM	2605056	Download Delete
default.cfg	4/6/2020, 11:53:12 AM	3974	Download Delete
x930-5.5.0-0...	6/18/2020, 12:43:50 PM	39218454	Download Delete

Set Boot Release File
Current: flash:/x930-5.5.0-1.1.rel
Backup: flash:/x930-5.5.0-0.3.rel

Set Boot Config File
Current: flash:/default.cfg
Backup: Not Set

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



Flash Usage

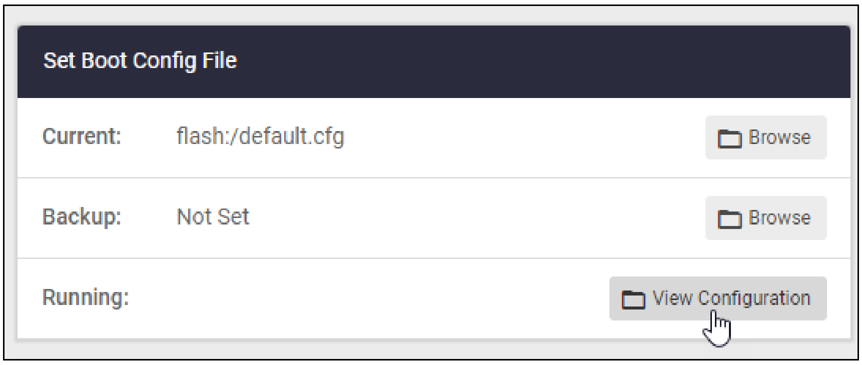
42% 106.9M / 253.8M

Display the running configuration

From version 2.16.0 onwards, you can display the running configuration. This is the configuration that the device is currently running.

- It may be different than the configuration that the device loads on start-up.

You can display the running configuration by clicking the **View Configuration** button in the Set Boot Config File section of the **File Management** page. This will display the running configuration in a dialog box.



Set Boot Config File

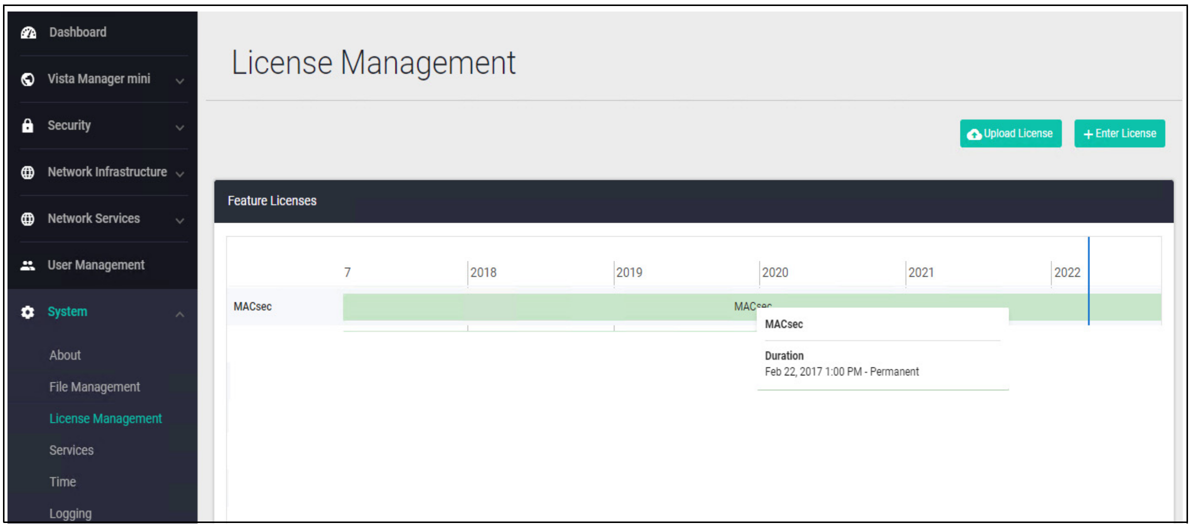
Current: flash:/default.cfg

Backup: Not Set

Running:

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.



License Management

Feature Licenses

MACsec

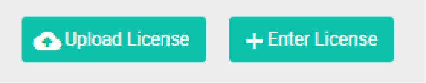
Duration
Feb 22, 2017 1:00 PM - Permanent

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

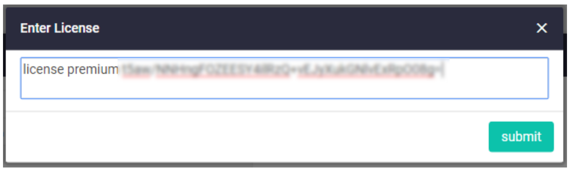
Adding a new permanent feature license

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.

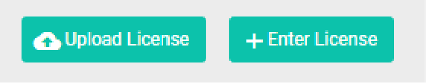


license premium [redacted]

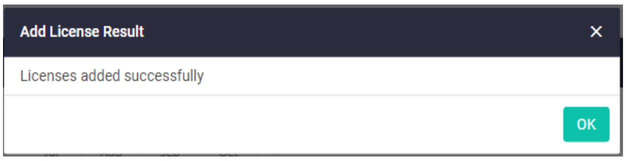
Adding a new subscription feature license

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.



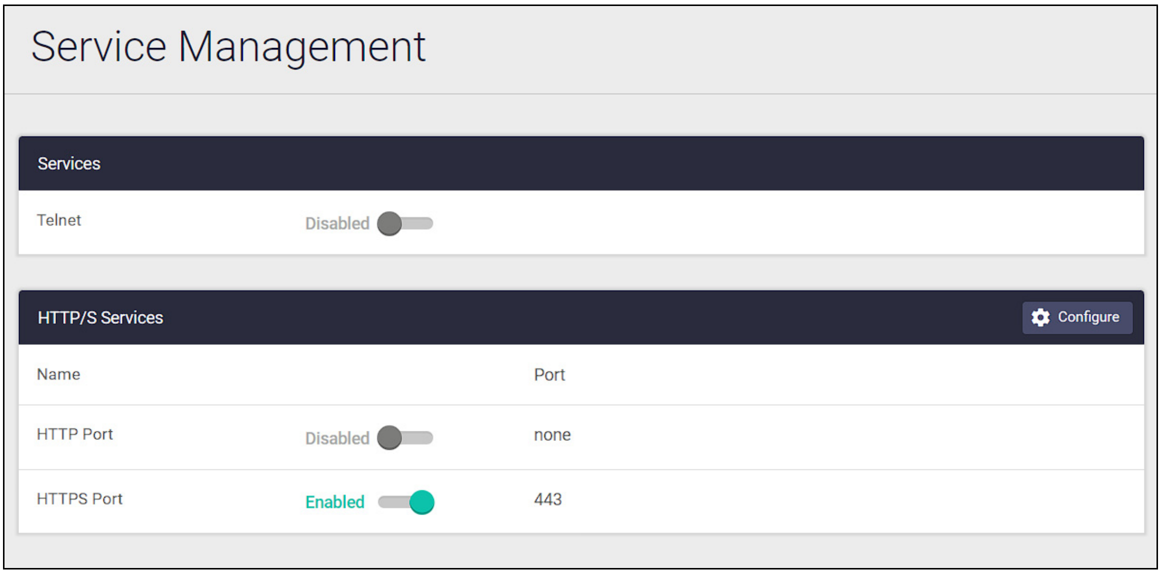
Licenses added successfully

Services

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

SSH settings are shown on the Services page for versions earlier than 2.16.0. These settings moved in version 2.16.0, and are now on the SSH page. To see SSH settings for versions 2.16.0 and above, see "SSH" on page 40.

From version 2.16.0 onwards, you can see and configure HTTP and HTTPS services from the **Service Management** page.



Service Management

Services

Telnet	Disabled

HTTP/S Services

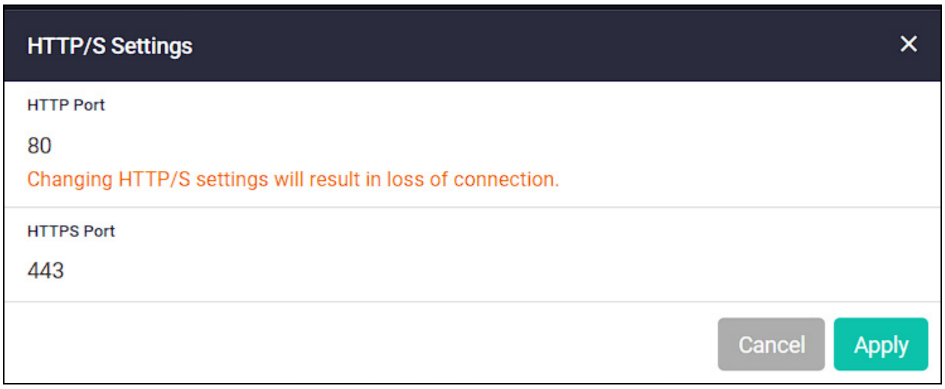
Name		Port
HTTP Port	Disabled	none
HTTPS Port	Enabled	443

The Service Management page provides the ability to enable or disable Telnet, and change or disable HTTP ports.

- Click the toggle next to Telnet to enable or disable Telnet.
- 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.

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



HTTP/S Settings

HTTP Port

80

Changing HTTP/S settings will result in loss of connection.

HTTPS Port

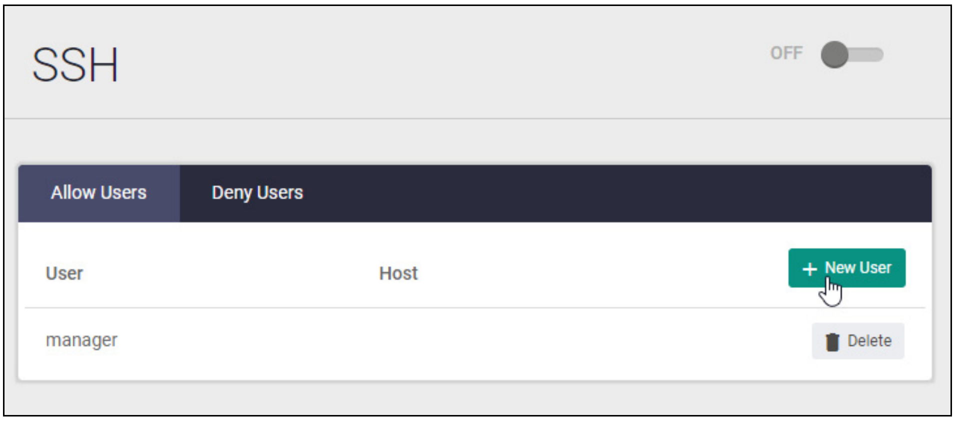
443

- 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

From version 2.16.0 onwards, you can access the SSH section from the **System** menu.

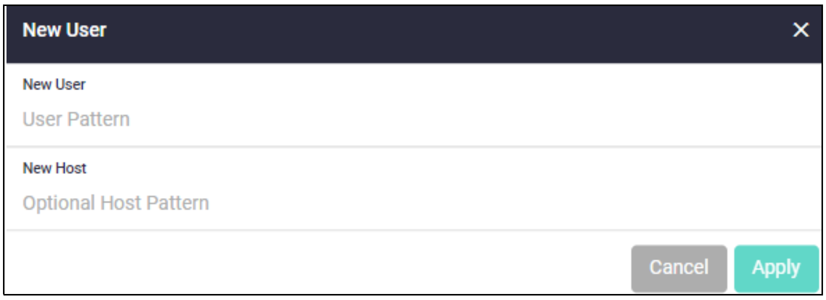


You can:

- Click the toggle next to SSH to enable or disable SSH.
- Allow specific users by clicking **+ New User** in the Allow Users tab.
- Deny specific users by clicking **+ New User** from the Deny Users tab.

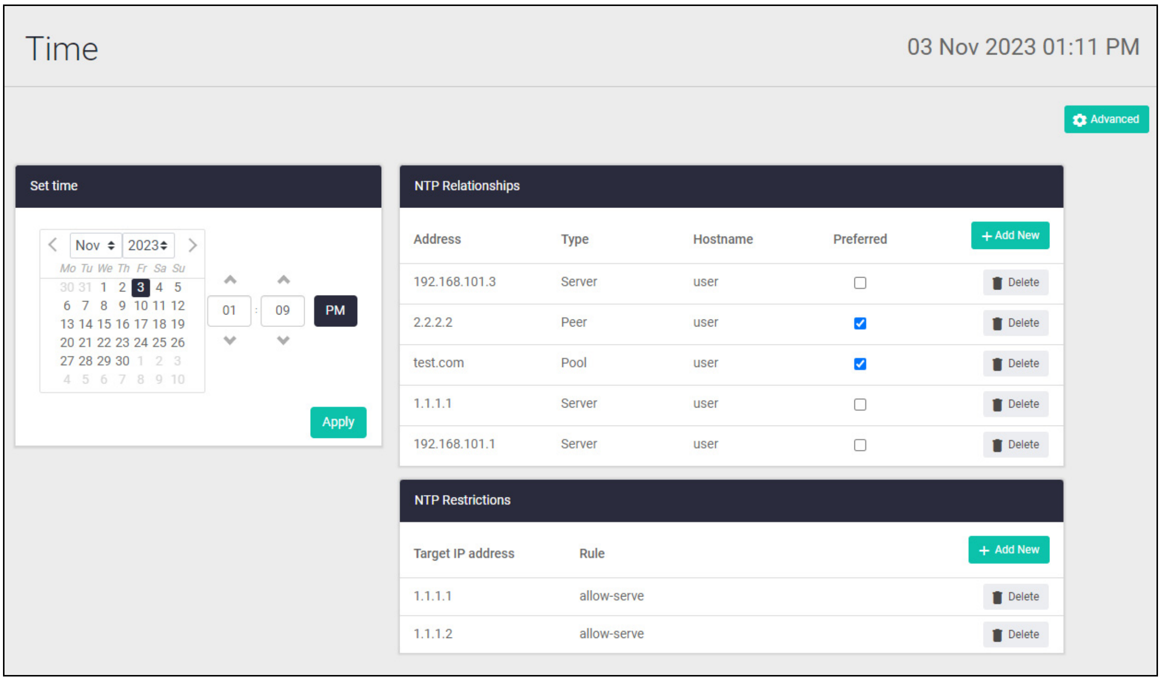
When you click **+ New User**, you can enter a user and host pattern from the New User window. The hostname pattern can be an IP address or a domain.

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.



Time

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



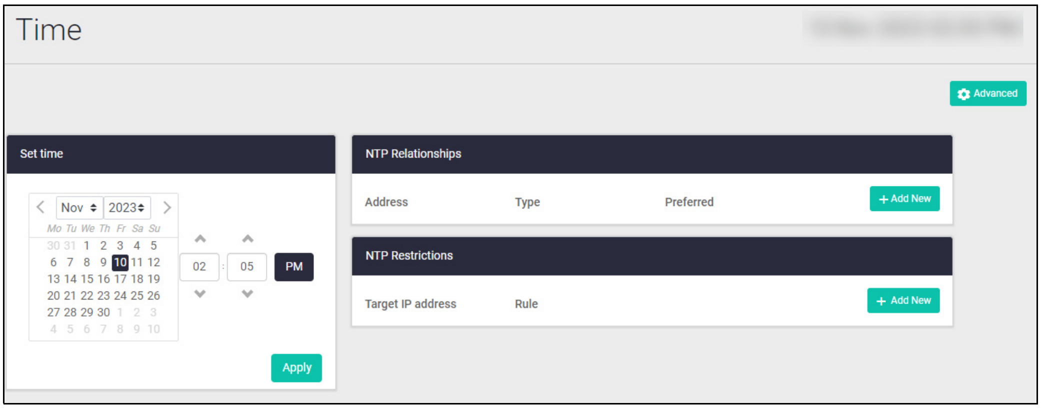
Mo	Tu	We	Th	Fr	Sa	Su
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Address	Type	Hostname	Preferred	+ Add New
192.168.101.3	Server	user	☐	Delete
2.2.2.2	Peer	user	☑	Delete
test.com	Pool	user	☑	Delete
1.1.1.1	Server	user	☐	Delete
192.168.101.1	Server	user	☐	Delete

Target IP address	Rule	+ Add New
1.1.1.1	allow-serve	Delete
1.1.1.2	allow-serve	Delete

From version 2.16.0 onwards, you can configure NTP settings on the Time page. These additions include:

- NTP relationships,
- and NTP restrictions.



Mo	Tu	We	Th	Fr	Sa	Su
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Address	Type	Preferred	+ Add New

Target IP address	Rule	+ Add New

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

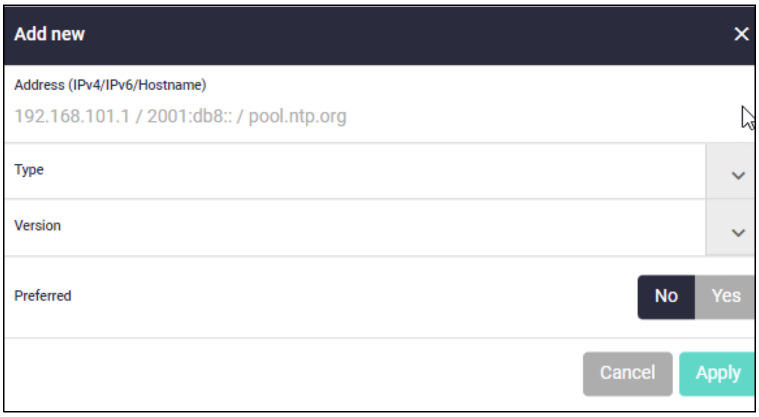
- It is recommended that you use more than one NTP server for redundancy.

You can then 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


Add new

Address (IPv4/IPv6/Hostname)

192.168.101.1 / 2001:db8:: / pool.ntp.org

Type

Version

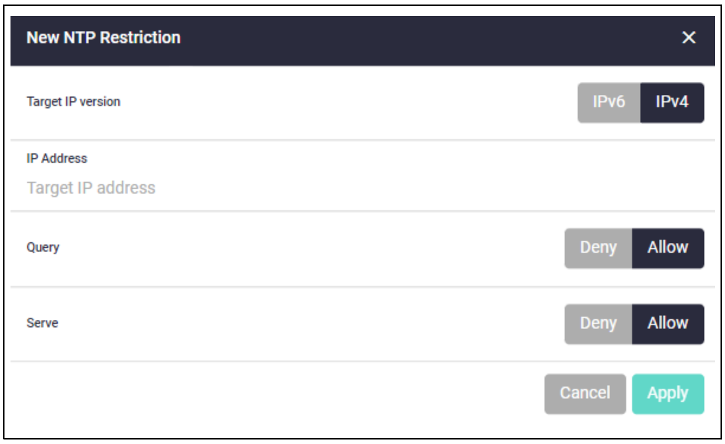
Preferred

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.


New NTP Restriction

Target IP version: IPv6 [✓ IPv4]

IP Address

Target IP address

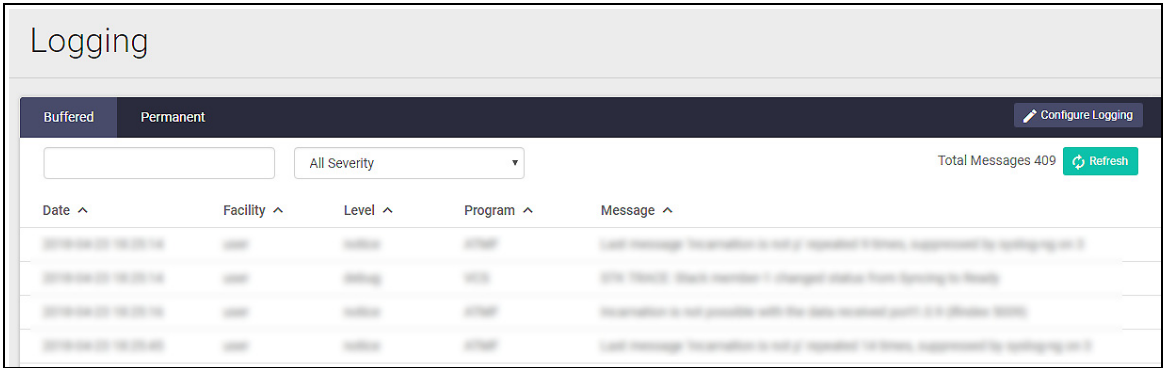
Query: Deny [✓ Allow]

Serve: Deny [✓ Allow]

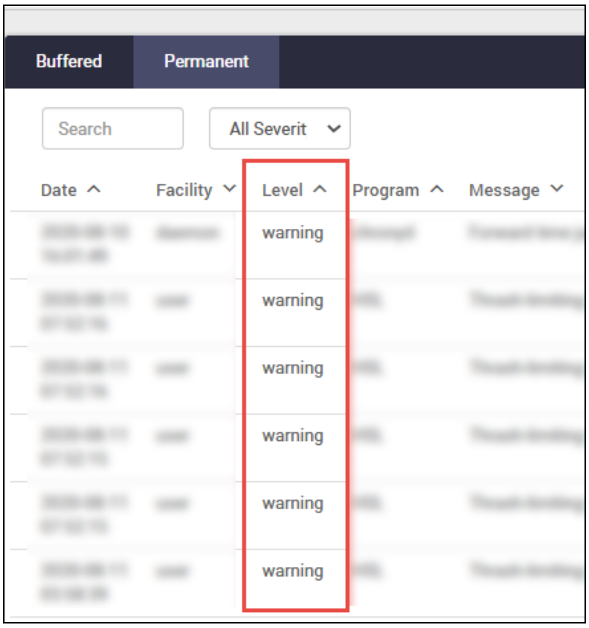
Logging

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

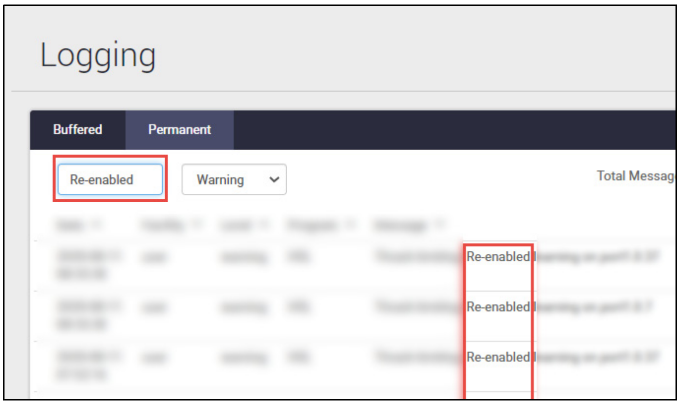
You can filter the logs in 3 ways to focus your view and support easy analysis:



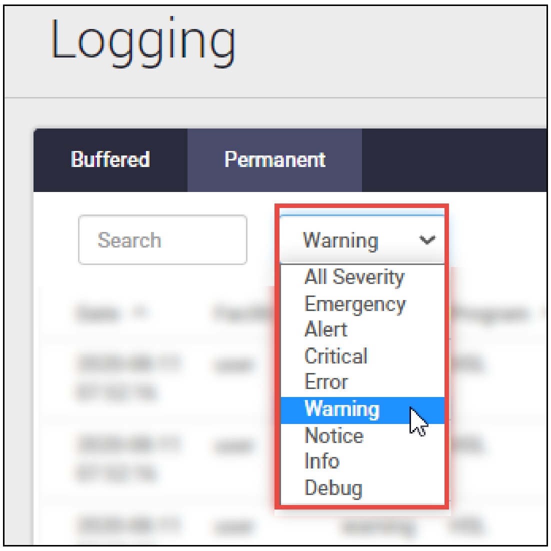
- Click the name of a category to sort by that type:



- Search for any text string found in the logs with the search function:



- Select the level of logs to display from the drop-down next to the search:

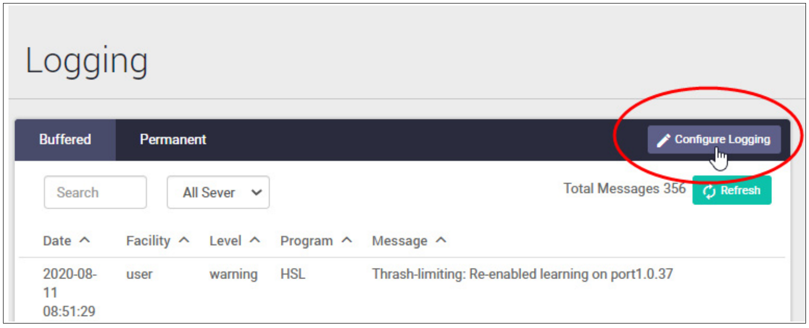


Logging Filters

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.

Note: In older GUI versions, click the **Configure Logging** button to access the Logging Configuration page. The Filters information is on this page.

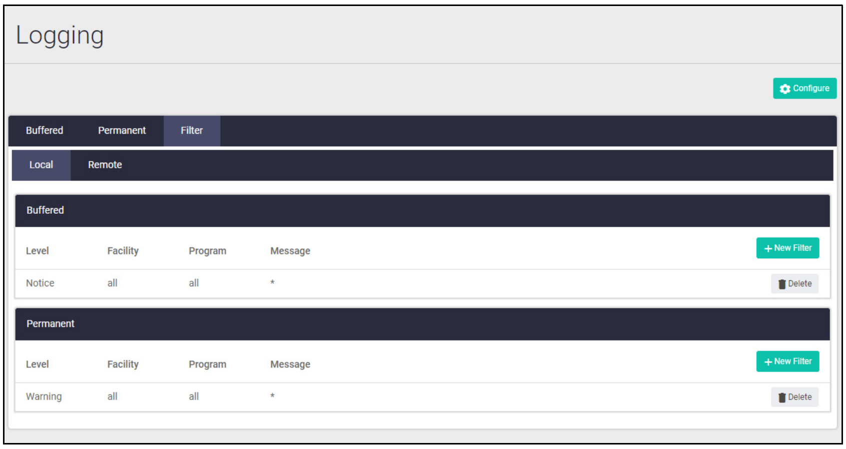


Date	Facility	Level	Program	Message
2020-08-11 08:51:29	user	warning	HSL	Thrash-limiting: Re-enabled learning on port1.0.37

From version 2.16.0 onwards, various changes have been made to the Logging page:

- The **Filters** tab has moved, and you can now configure filters on the main Logging page. From the Local tab, you can create Buffered or Permanent filters.
- The **Configure** button on the Logging page now allows you to set a Date/Time format.
- The **Clear Log** button has moved to the Buffered or Permanent log tabs.

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



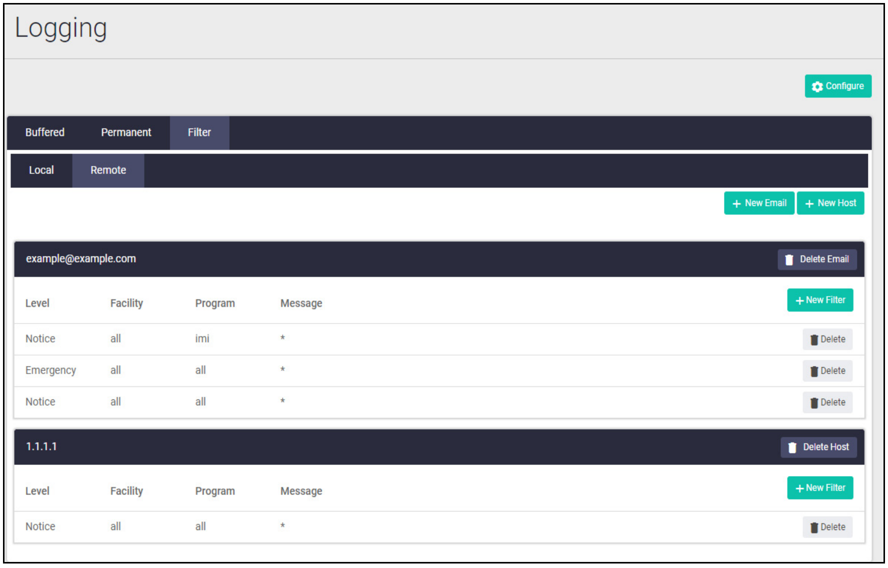
Buffered

Level	Facility	Program	Message
Notice	all	all	*

Permanent

Level	Facility	Program	Message
Warning	all	all	*

From the **Remote** tab, you can create filters for email addresses or hosts.



example@example.com

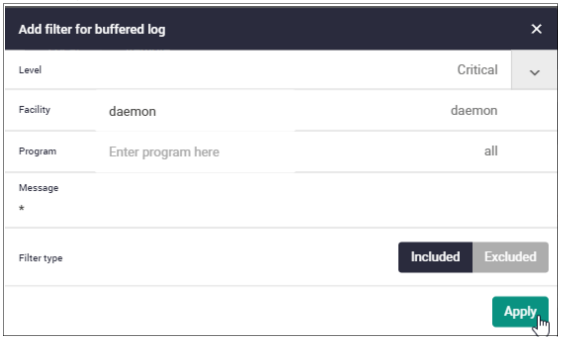
Level	Facility	Program	Message
Notice	all	imi	*
Emergency	all	all	*
Notice	all	all	*

1.1.1.1

Level	Facility	Program	Message
Notice	all	all	*

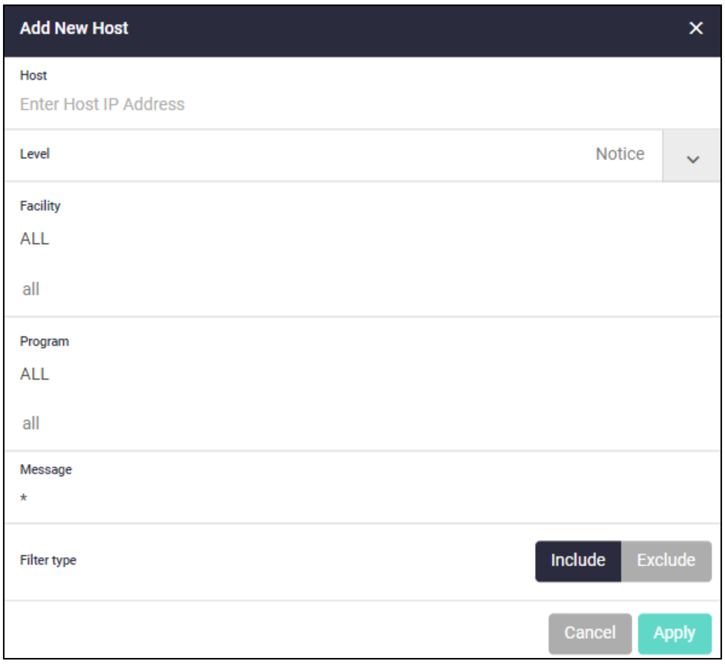
- To add a new email or host, click the **+ New Email** or **+ New Host** button.
- To create filters for specific emails or hosts, click the **+ New Filter** button.

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.



Level		Critical
Facility	daemon	daemon
Program	Enter program here	all
Message *		
Filter type		Included / Excluded

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



Add New Host

Host
Enter Host IP Address

Level: Notice

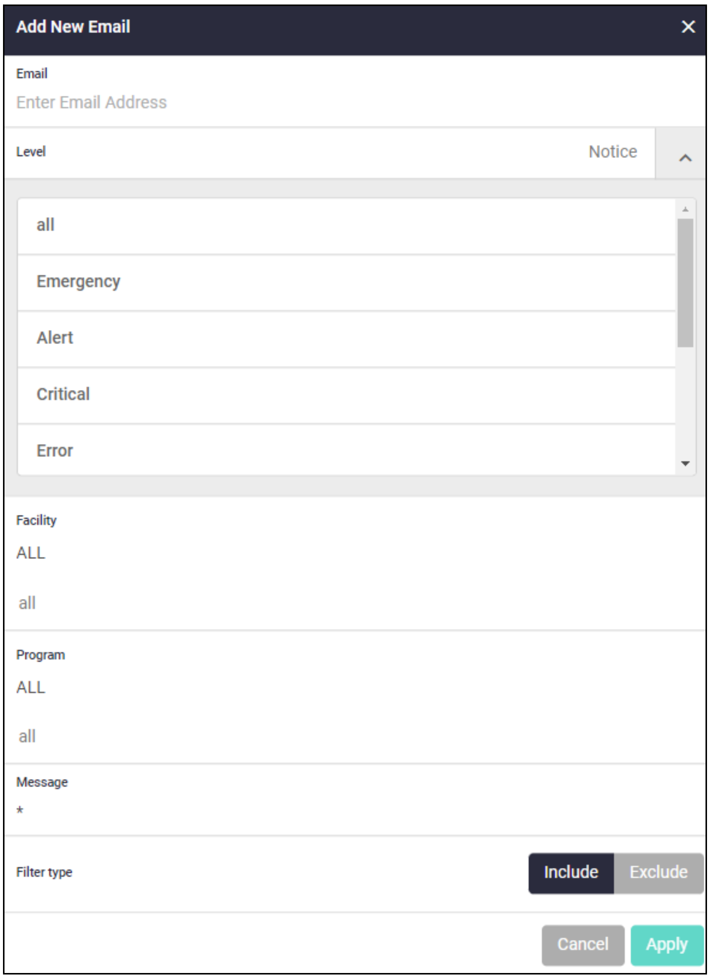
Facility
ALL
all

Program
ALL
all

Message
*

Filter type: Include | Exclude

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**.



Add New Email

Email
Enter Email Address

Level: Notice

- all
- Emergency
- Alert
- Critical
- Error

Facility
ALL
all

Program
ALL
all

Message
*

Filter type: Include | Exclude

Trigger

From version 2.16.0 onwards, you can create triggers through the Device GUI.

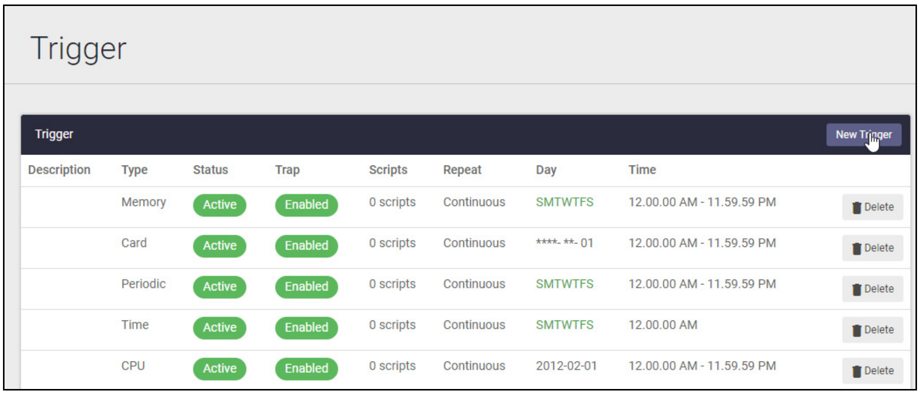
- A **trigger** is an ordered sequence of scripts that is executed when a certain event occurs.
- A **script** is a sequence of commands stored as a plain text file on a file subsystem accessible to the device, such as Flash memory.

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

When you create a trigger, you can fill out different fields depending on the type of trigger you select.

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.

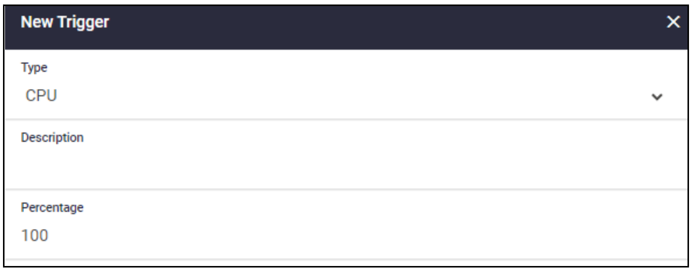


Trigger

Trigger

Description	Type	Status	Trap	Scripts	Repeat	Day	Time	
	Memory	Active	Enabled	0 scripts	Continuous	SMTWTFS	12.00.00 AM - 11.59.59 PM	Delete
	Card	Active	Enabled	0 scripts	Continuous	****- **- 01	12.00.00 AM - 11.59.59 PM	Delete
	Periodic	Active	Enabled	0 scripts	Continuous	SMTWTFS	12.00.00 AM - 11.59.59 PM	Delete
	Time	Active	Enabled	0 scripts	Continuous	SMTWTFS	12.00.00 AM	Delete
	CPU	Active	Enabled	0 scripts	Continuous	2012-02-01	12.00.00 AM - 11.59.59 PM	Delete

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



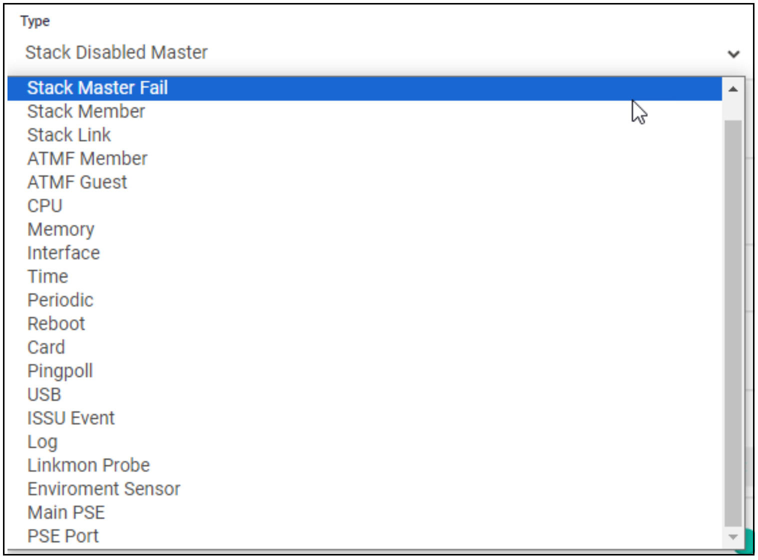
New Trigger

Type: CPU

Description:

Percentage: 100

You can select from a variety of triggers.:



Type

Stack Disabled Master

Type

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/Event

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.

Scripts

In this section, you can add a script to run when the trigger activates.

Repeat

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

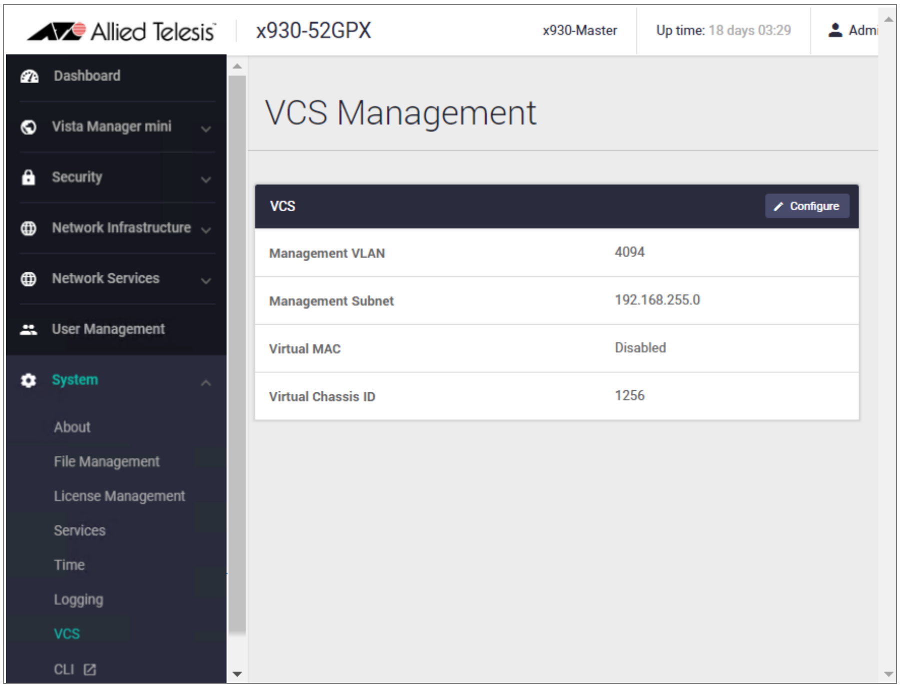
Toggles

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.

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.



VCS Management

VCS

Management VLAN	4094
Management Subnet	192.168.255.0
Virtual MAC	Disabled
Virtual Chassis ID	1256

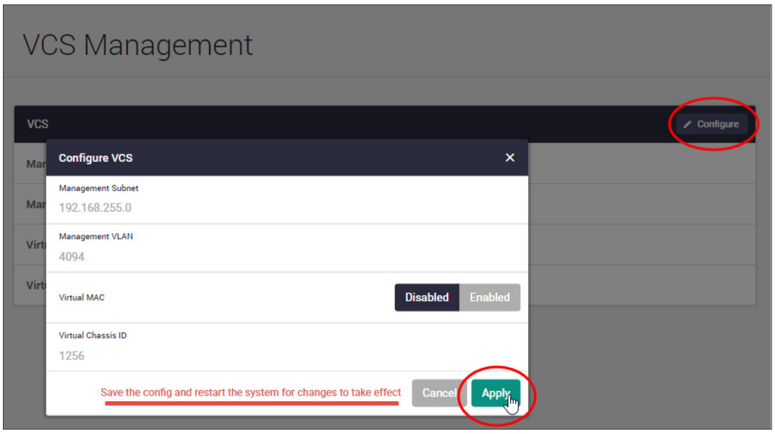
By default, the VLAN and subnet used are:

- 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.



Management Subnet
192.168.255.0

Management VLAN
4094

Virtual MAC ● Disabled ○ Enabled

Virtual Chassis ID
1256

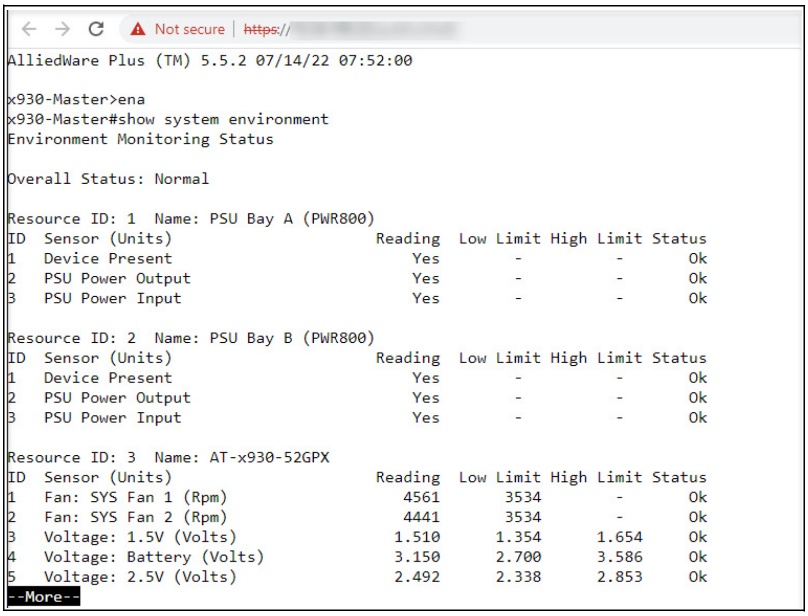
Save the config and restart the system for changes to take effect

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.

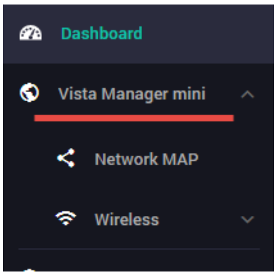


```
AlliedWare Plus (TM) 5.5.2 07/14/22 07:52:00

x930-Master>ena
x930-Master#show system environment
Environment Monitoring Status

Overall Status: Normal

Resource ID: 1  Name: PSU Bay A (PWR800)
ID  Sensor (Units)                      Reading  Low Limit High Limit Status
1   Device Present                          Yes        -          -       Ok
2   PSU Power Output                        Yes        -          -       Ok
3   PSU Power Input                         Yes        -          -       Ok

Resource ID: 2  Name: PSU Bay B (PWR800)
ID  Sensor (Units)                      Reading  Low Limit High Limit Status
1   Device Present                          Yes        -          -       Ok
2   PSU Power Output                        Yes        -          -       Ok
3   PSU Power Input                         Yes        -          -       Ok

Resource ID: 3  Name: AT-x930-52GPX
ID  Sensor (Units)                      Reading  Low Limit High Limit Status
1   Fan: SYS Fan 1 (Rpm)                   4561       3534        -       Ok
2   Fan: SYS Fan 2 (Rpm)                   4441       3534        -       Ok
3   Voltage: 1.5V (Volts)                 1.510      1.354      1.654     Ok
4   Voltage: Battery (Volts)              3.150      2.700      3.586     Ok
5   Voltage: 2.5V (Volts)                 2.492      2.338      2.853     Ok
--More--
```

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.

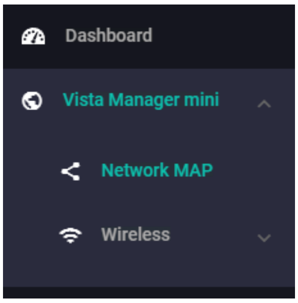


The device GUI also displays heat maps for managed APs on the network map.

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.

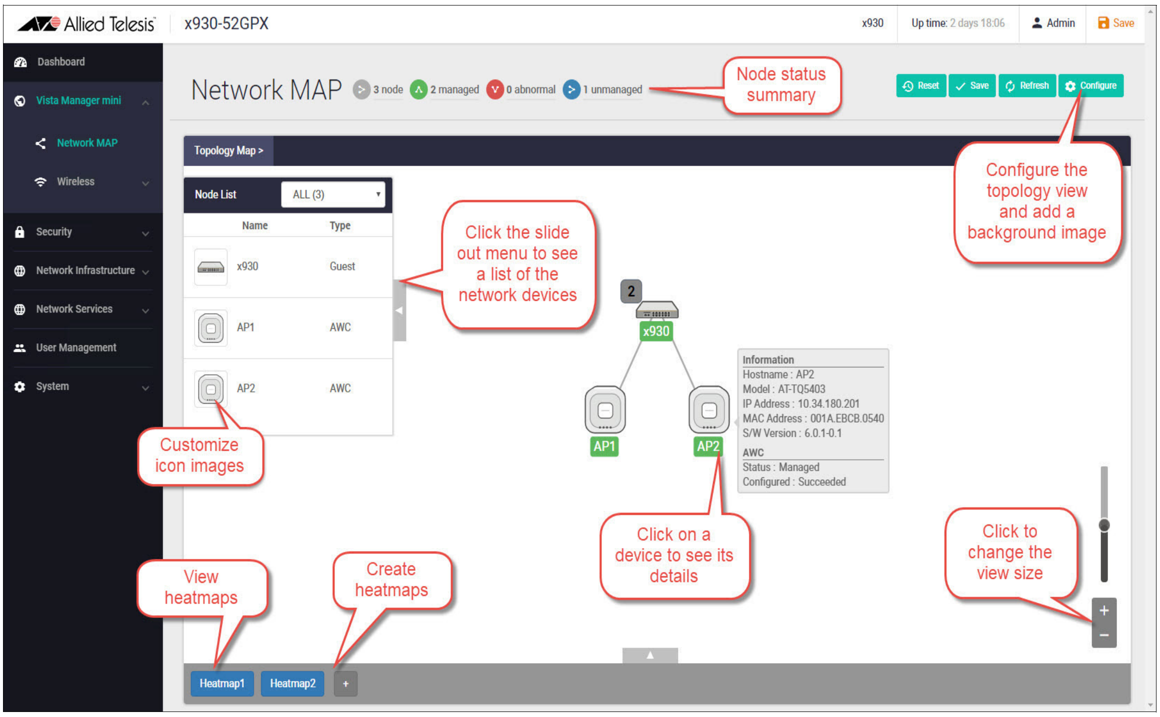
Note that the screenshots in this section show an x930 Series switch, but the functionality is the same for all models that include Vista Manager mini.

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



Name	Type
x930	Guest
AP1	AWC
AP2	AWC

Information
Hostname : AP2
Model : AT-TQ5403
IP Address : 10.34.180.201
MAC Address : 001A.EBCB.0540
S/W Version : 6.0.1-0.1

AWC
Status : Managed
Configured : Succeeded

Node status summary

Configure the topology view and add a background image

Click the slide out menu to see a list of the network devices

Customize icon images

Click on a device to see its details

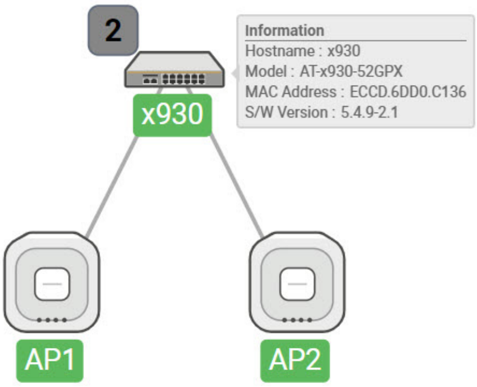
Click to change the view size

View heatmaps

Create heatmaps

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.



Information
Hostname : x930
Model : AT-x930-52GPX
MAC Address : ECCD.6DD0.C136
S/W Version : 5.4.9-2.1

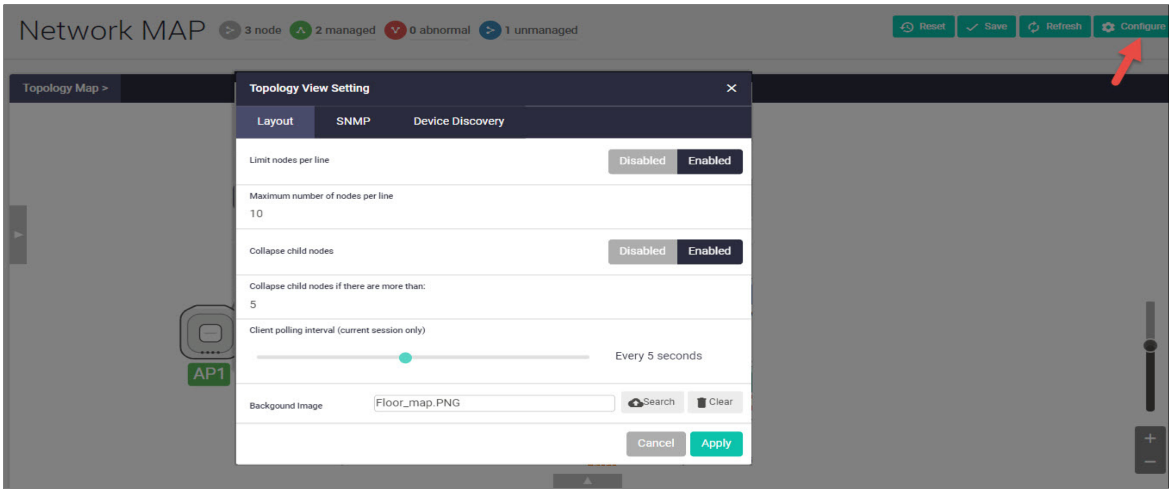
Configuring the topology view

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.



Topology View Setting

Limit nodes per line: Disabled **Enabled**

Maximum number of nodes per line: 10

Collapse child nodes: Disabled **Enabled**

Collapse child nodes if there are more than: 5

Client polling interval (current session only): Every 5 seconds

Backgound Image: Floor_map.PNG

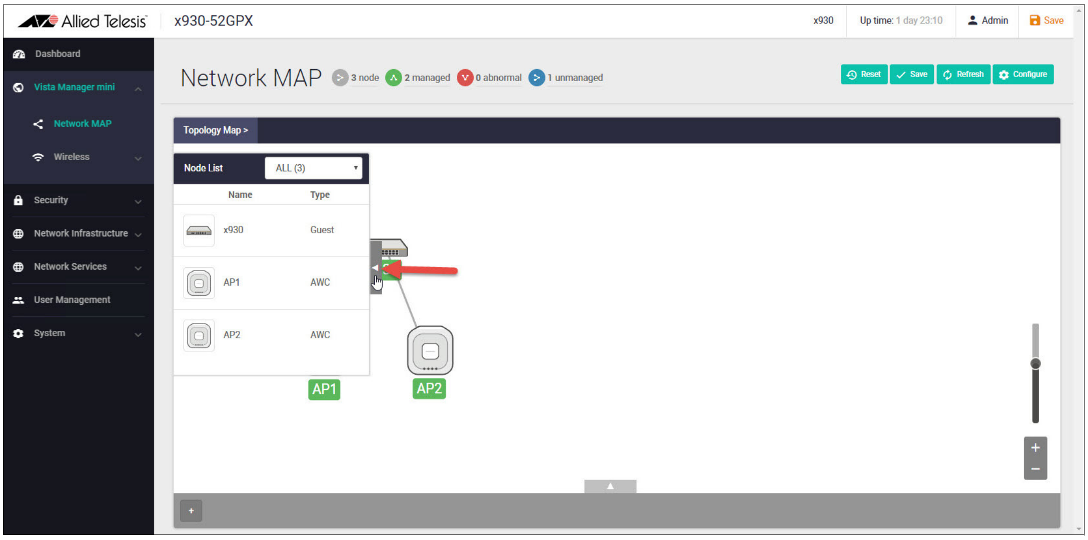
Customizing network node icon images

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)

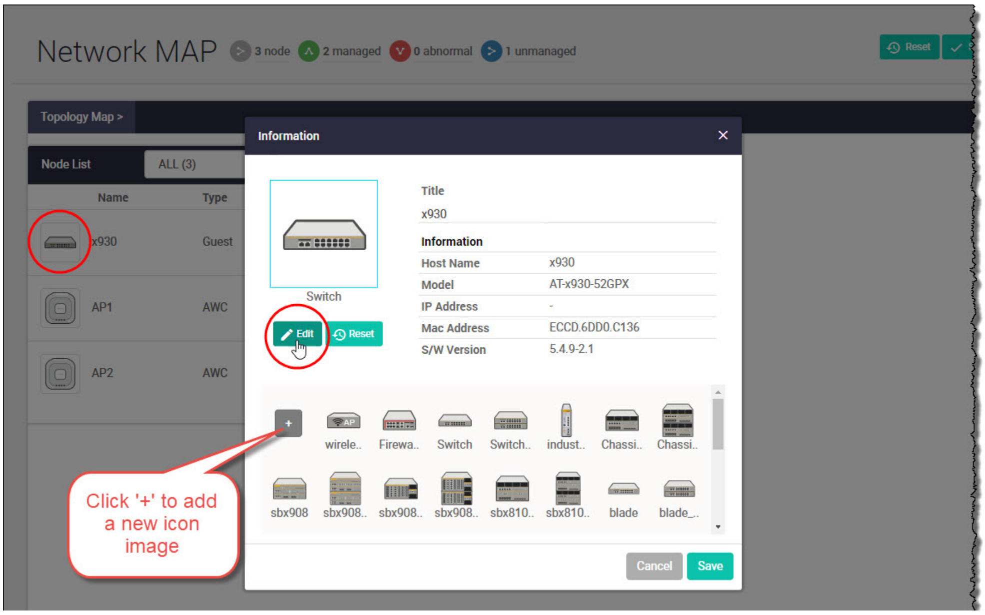


Name	Type
x930	Guest
AP1	AWC
AP2	AWC

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**.



Title
x930

Information

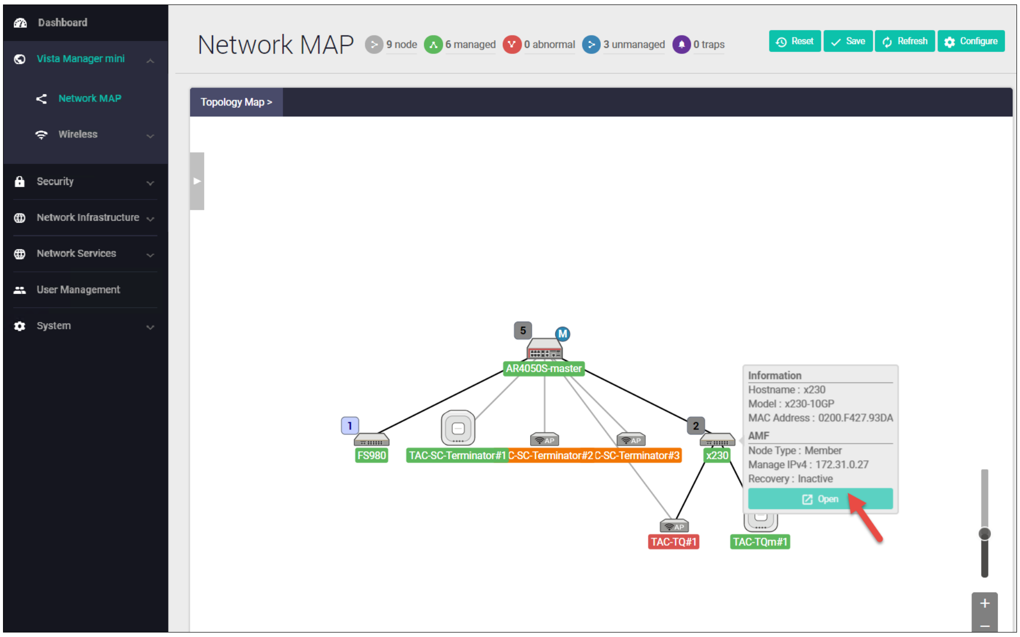
Host Name x930
Model AT-x930-52GPX
IP Address -
Mac Address ECCD.6DD0.C136
S/W Version 5.4.9-2.1

Click '+' to add a new icon image

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).

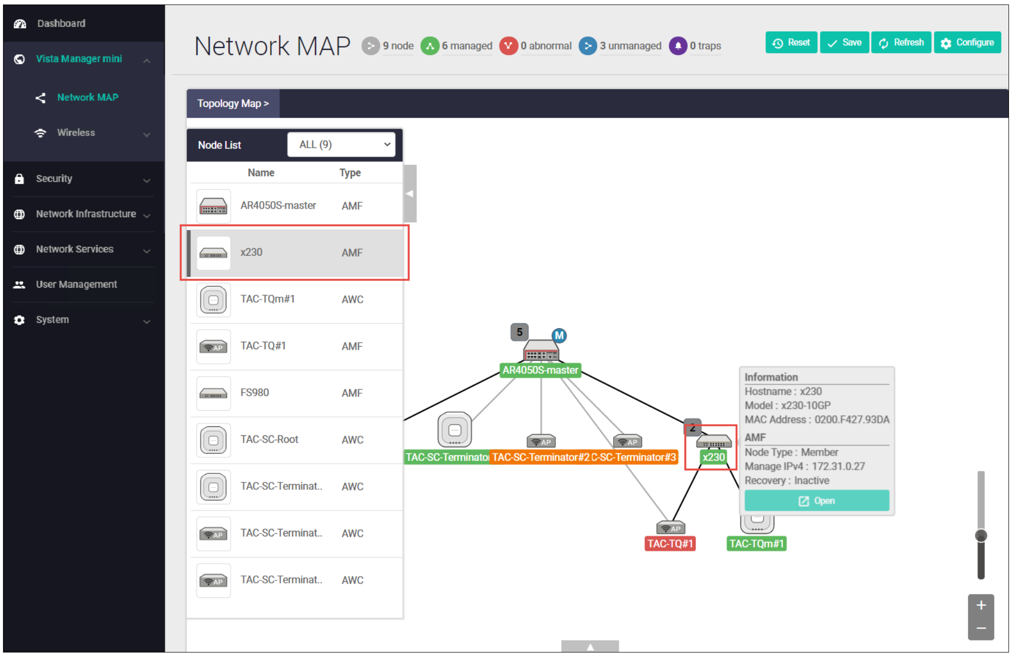
When you click a node icon on the Network Map, the node information is displayed. In the node information window, click on the **Open** button to access the device’s GUI.



Information
Hostname : x230
Model : x230-10GP
MAC Address : 0200.F427.93DA

AMF
Node Type : Member
Manage IPv4 : 172.31.0.27
Recovery : Inactive

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.

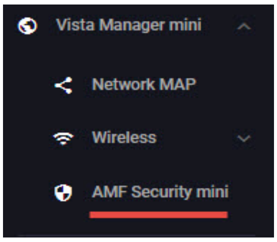


Name	Type
AR4050S-master	AMF
x230	AMF
TAC-TQm#1	AWC
TAC-TQ#1	AMF
FS980	AMF
TAC-SC-Root	AWC
TAC-SC-Terminat..	AWC
TAC-SC-Terminat..	AWC
TAC-SC-Terminat..	AWC

Information
Hostname : x230
Model : x230-10GP
MAC Address : 0200.F427.93DA
AMF
Node Type : Member
Manage IPv4 : 172.31.0.27
Recovery : Inactive

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