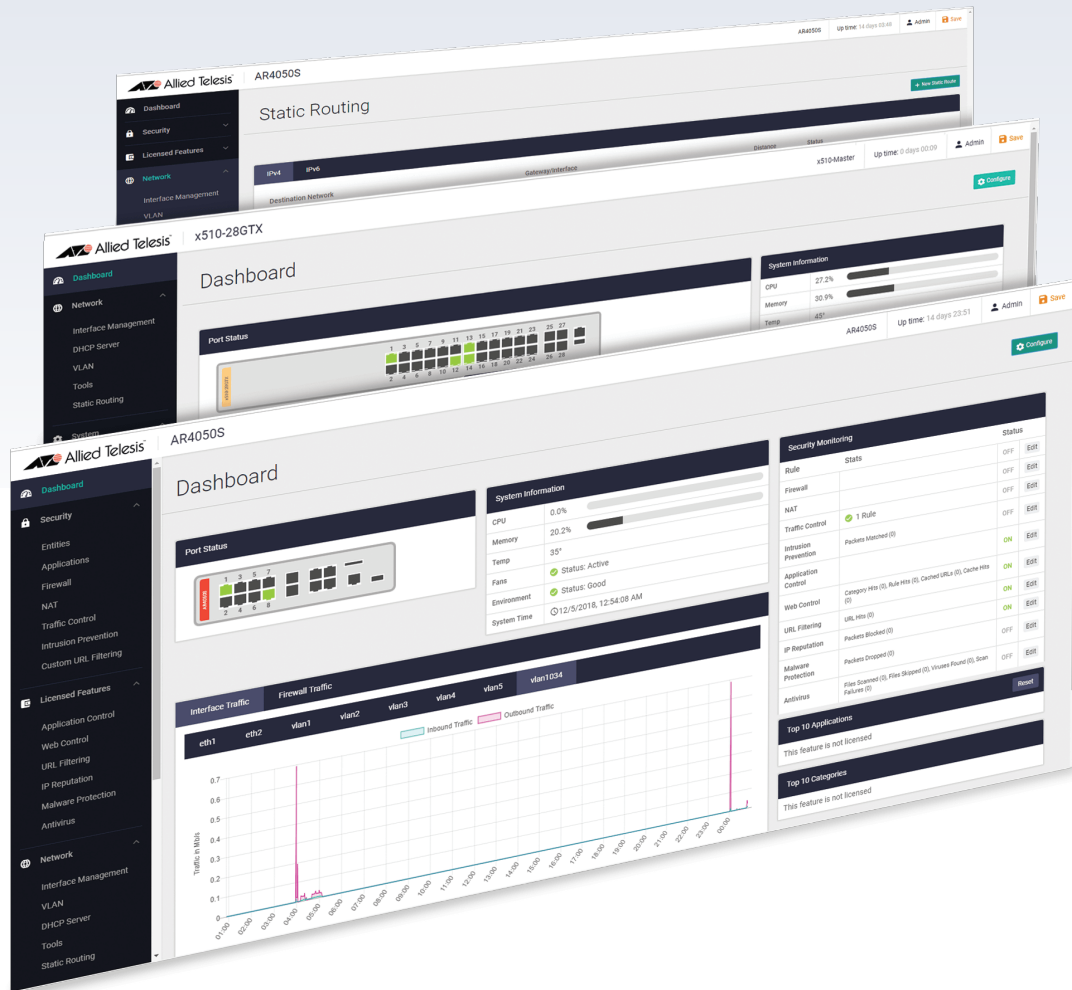


# Release Note for Web-based Device GUI Version 2.6.x



» 2.6.0 » 2.6.1

**AlliedWare Plus**  
OPERATING SYSTEM

---

## Acknowledgments

©2020 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

## Getting the most from this Release Note

To get the best from this release note, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from [www.adobe.com/](http://www.adobe.com/)

# Contents

<b>What's New in Version 2.6.1 .....</b>	<b>4</b>
<b>Introduction .....</b>	<b>4</b>
<b>New Features and Enhancements .....</b>	<b>7</b>
Captive Portal.....	7
Email trigger support .....	8
Enhancements to Device Discovery using SNMP .....	10
How to see information about discovered devices.....	10
How to see SNMP Monitoring trap data.....	12
Change the client polling interval for the current session .....	14
Issues Resolved in Version 2.6.1.....	15
<b>What's New in Version 2.6.0 .....</b>	<b>16</b>
<b>Introduction .....</b>	<b>16</b>
<b>New Features and Enhancements .....</b>	<b>19</b>
PoE enhancements .....	19
View contact and server location information.....	22
Configure up to 32 secondary IP addresses on an interface.....	23
View and configure multicast router interfaces for IGMP snooping.....	25
Sort by columns on the FDB and ARP tables .....	27
<b>Installing and Accessing the Web-based GUI on Switches.....</b>	<b>28</b>
<b>Installing and Accessing the Web-based GUI on AR-Series Devices .....</b>	<b>31</b>

# What's New in Version 2.6.1

Product families supported by this version:

SwitchBlade x908 GEN2	IE510-28GSX-80
SwitchBlade x8100 Series	IE340 Series
x950 Series	IE300 Series
x930 Series	IE210L Series
x550 Series	IE200 Series
x530 Series	XS900MX Series
x530L Series	GS980M Series
x510 Series	GS980EM Series
x510L Series	GS970M Series
IX5-28GPX	GS900MX/MPX Series
x310 Series	FS980M Series
x320 Series	AR4050S
x230 Series	AR3050S
x230L Series	AR2050V
x220 Series	AR2010V
	AR1050V

## Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.6.1. You can run 2.6.1 with any AlliedWare Plus firmware version on your device. However some of the new features are only available with 5.5.0-1.1 or later.

For information on accessing and updating the Device GUI, see [“Installing and Accessing the Web-based GUI on Switches”](#) on page 28 or [“Installing and Accessing the Web-based GUI on AR-Series Devices”](#) on page 31.

The following table lists model names that support this version:

Table 1: Models

Models	Family
SBx908 GEN2	SBx908 GEN2
SBx81CFC960	SBx8100
x950-28XSQ x950-28XTQm x950-52XSQ	x950
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930
x550-18SXQ x550-18XTQ x550-18XSPQm	x550

Table 1: Models (cont.)

Models	Family
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L
IX5-28GPX	IX5
x310-26FT x310-50FT x310-26FP x310-50FP	x310
x320-10GH x320-11GPT	x320
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L
x220-28GS x220-52GT x220-52GP	x220
IE510-28GSX	IE510-28GSX
IE340-20GP IE340L-18GP	IE340
IE300-12GT IE300-12GP	IE300
IE210L-10GP IE210L-18GP	IE210L
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200
XS916MXT XS916MXS	XS900MX
GS980M/52 GS980M/52PS	GS980M
GS980EM/10H GS980EM/11PT	GS980EM

Table 1: Models (cont.)

Models	Family
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28DP FS980M/28PS FS980M/52 FS980M/52PS	FS980M
AR4050S AR3050S	AR-series UTM firewalls
AR2050V AR2010V AR1050V	AR-series VPN routers

## New Features and Enhancements

This section summarizes the new features in the Device GUI software version 2.6.1, for devices running AlliedWare Plus.

From version 2.6.1 onwards, the following new features and enhancements are available:

### Captive Portal

Captive Portal is a mechanism to let wireless clients authenticate themselves before they are granted Wi-Fi access or external web access.

The most standard use for a Captive Portal is to provide a gateway to allow an outside guest access to a Wi-Fi network. This is typical for any office or business that wants to keep visiting guests on a separate network from their internal business network. This is a security feature that ensures the main business network is safe. It prevents guests who may knowingly or unknowingly download a malicious program or virus from spreading to the main business network, while also allowing a business to potentially restrict access.

### This is how it works

Wireless APs monitor traffic from wireless clients and when they detect the first HTTP/HTTPS packets from each client, they redirect HTTP/HTTPS traffic from that client to a page called Captive Portal.

There are three types of Captive Portal:

- **External RADIUS Authentication** - this method authenticates wireless clients. Use this if you want guests to log into the guest network using a username and password that you provide them with. You will need to store the username and password on a RADIUS server and use AlliedWare Plus to specify the RADIUS server.
- **Click-through** - this method only asks users to agree to the terms of use (click-through agreement) before allowing them to connect to the wireless network. The click-through page does not require authentication with a username/password pair, but can be configured to show an arbitrary "Terms of Use" that users have to accept before use, or to redirect to an external page. Use this if you don't need guests to log in.
- **External Page Redirect** - this method redirects the authentication page to a user configured URL such as a third-party Captive Portal vendor page. Use this if you want guests to login via the third-party vendor.

To see how to configure Captive Portal in the Device GUI, see the Autonomous Wave Control section of [User Guide: Vista Manager mini](#).

## Email trigger support

Menu location: *Network Services > SMTP Server*

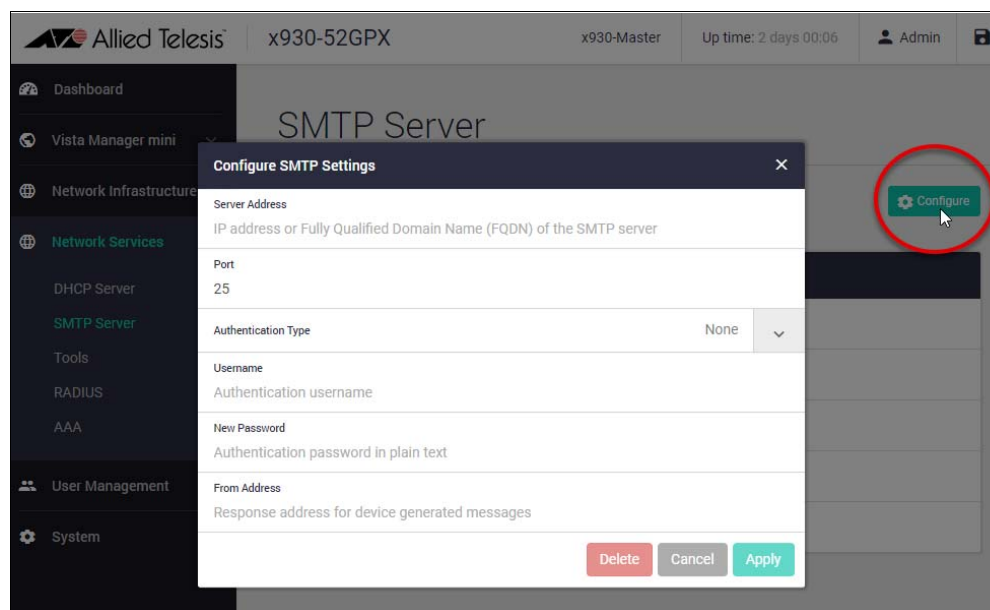
With this software version, you can use the GUI to configure the SMTP server.

Previously, this feature was only configurable using the commands:

- `mail smtpserver <string>`
- `mail from <string>`
- `mail smtpserver authentication <string> username <string> password <string>`
- `mail smtpserver port <port>`
- `show mail`

To configure the SMTP settings:

- In the **Network Services > SMTP Server** window, click **Configure**.
- Type in the **server address** and **port number**.
- Click **Apply**.

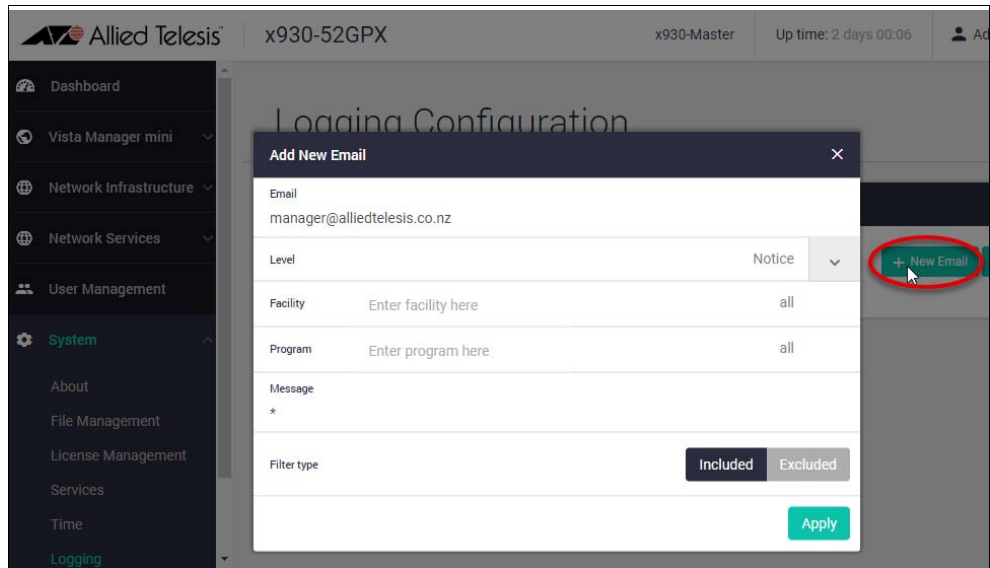


To configure an email filter:

1. In the **System > Logging** window, click **Configure Logging**.
2. Select the **Remote** tab.
3. Click **+New Email**.
4. The Add New Email window opens.
5. Type in a destination email address. This is a mandatory field.



6. Click **Apply**.



## Enhancements to Device Discovery using SNMP

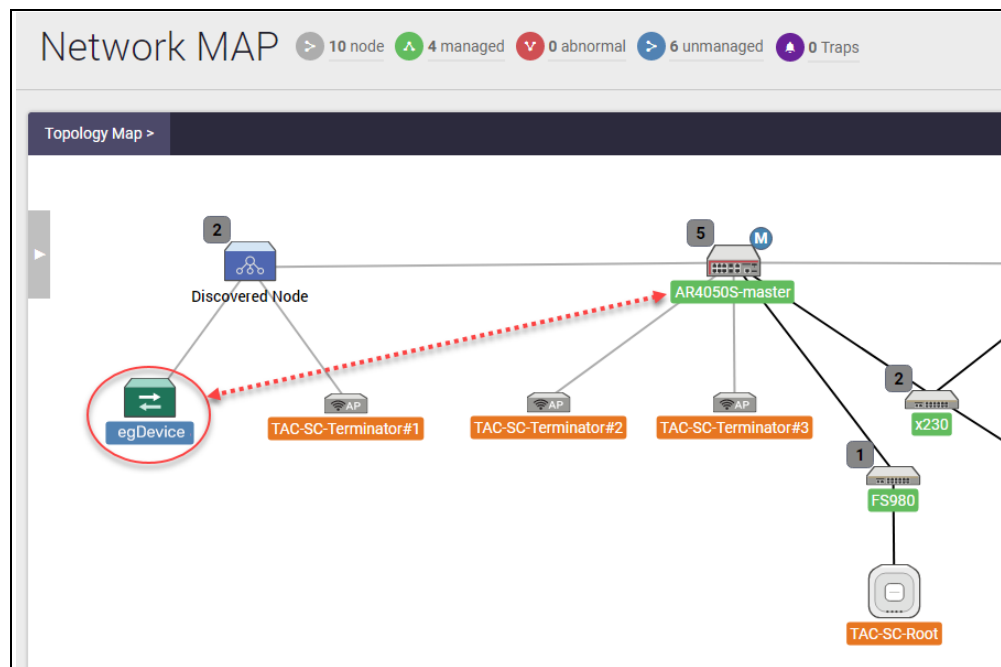
From version 2.6.1 onwards, you can move a node to a different location in the Network MAP with drag and drop. You can also more easily see the number of traps for each device.

### How to see information about discovered devices

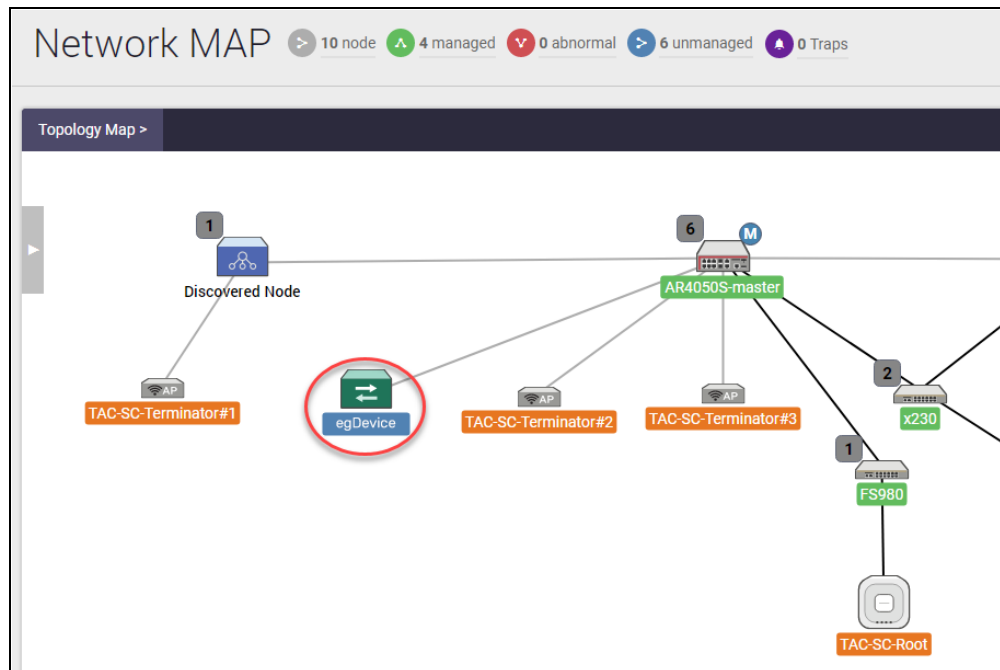
#### Drag and drop feature

If you want to move a node to a different location in the Network MAP, you can use the drag and drop feature. For example, to move the discovered node Host 'egDevice' from its current location to the AR4050S-master node click on the node to move and drag it to its new location.

1. Click on the node and drag it to the new location, for example:



The result below shows that the node is now repositioned from where you clicked on it and then dragged it to its new position:



2. To save the Network MAP node positions and locations click **save**:

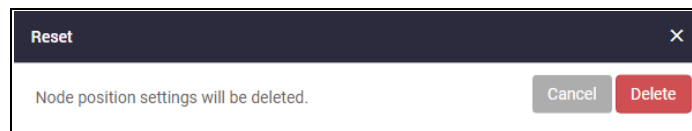


3. Click on the **save** button if you want to save the new position settings:



Or if you want to reset your Network Map nodes back to the original positions to the way they were before you changed it, choose the reset option.

4. Click on the **reset** button if you want to put the node positions settings back to how they were before you moved them:

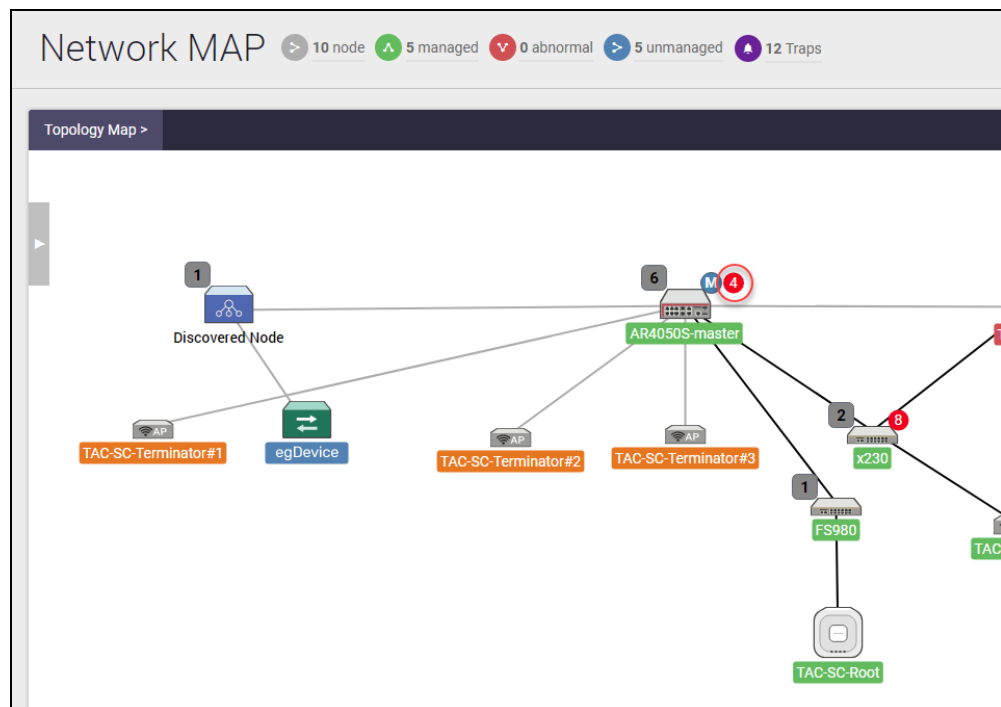


Now you can see your Network Map as it was before you changed it.

## How to see SNMP Monitoring trap data

### Trap badge

Trap indication also shows on the Network MAP on the node as a **trap badge** with the number of traps that have occurred. In the example below there are 4 traps on the AR4050S-master node and 8 traps on the x230 node. They show illuminated in red.



You can click on either the traps icon in the menu bar or the traps badge that appears on a node. In this example the events list is showing traps for the AR4050-master node. The **SNMP Recent Events List** shows the SNMP traps list:

Network MAP > 10 node 5 managed 0 abnormal 5 unmanaged 12 Traps

Topology Map >

SNMP Recent Events List

Date	MIB name	ID	Trap Type	IP Address	Interface	Description
2020-09-24 12:23	linkUp Trap	4	-		port1.0.1	An interface is linked up.
2020-09-24 12:15	linkUp Trap	3	-		port1.0.8	An interface is linked up.
2020-09-24 12:15	linkUp Trap	2	-		port1.0.2	An interface is linked up.
2020-09-24 12:15	coldStart Trap	1	-			Reinitializing itself and that its configuration may have been altered.

12 traps

1. Click on **all** to display all nodes, then select the node that you want to display the events list for. For example, the x230 node is selected below:

SNMP Recent Events List

All

All

AR4050S-master

x230

TAC-TQm#1

TAC-TQ#1

FS980

TAC-SC-Root

TAC-SC-Terminator#1

TAC-SC-Terminator#2

TAC-SC-Terminator#3

2020-09-10 08:05	linkDown Trap	54	-		port1.0.4	An interface is
2020-09-10 08:05	linkDown Trap	54	-		port1.0.3	An interface is
2020-09-10 08:05	linkUp Trap	53	-		port1.0.4	An interface is

14 traps

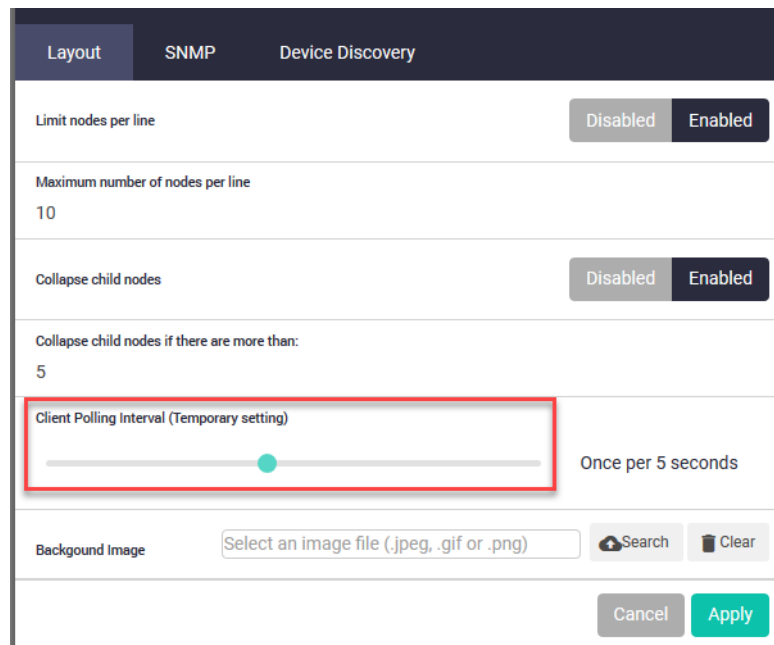
## Change the client polling interval for the current session

From version 2.6.1 onwards, it is possible to change how often Vista Manager mini polls clients. The change applies only to the current session.

We expect this new feature will be useful if you need to see a change particularly quickly, such as when demonstrating or assessing Vista Manager mini. For ordinary operation, we recommend leaving the polling interval at the default setting of 5 seconds.

To change the polling interval:

1. In the **Vista Manager mini** menu, select **Network MAP**.
2. Click on the **Configure** button. The Topology View Setting window opens.
3. On the **Layout** tab, move the slider in **Client Polling Interval (Temporary Setting)** to the desired setting.



## Issues Resolved in Version 2.6.1

This Device GUI version resolves the issues in the following table:

CR	Description
CR-69117	Previously, you could not use the GUI to create a web control rule that had a custom category. This issue has been resolved.
CR-69452	Previously, it was not possible to create custom web-control categories that had uppercase characters in their names. This issue has been resolved. Note that the GUI now converts uppercase characters to lowercase characters in category names. This means that if you create a category called 'example' and then a second category called 'Example', the second category's settings will replace and/or be appended to the first category's settings.
CR-69817	Previously, the PoE menu item was not displayed in Internet Explorer 11. This issue has been resolved.
CR-70024	Previously, the system up time was reset after 31 days. This issue has been resolved.
CR-70137	Previously, it was not possible to select a firmware file by clicking the date or size area on the firmware list. This issue has been resolved.

# What's New in Version 2.6.0

Product families supported by this version:

SwitchBlade x908 GEN2	IE510-28GSX-80
SwitchBlade x8100 Series	IE340 Series
x950 Series	IE300 Series
x930 Series	IE210L Series
x550 Series	IE200 Series
x530 Series	XS900MX Series
x530L Series	GS980M Series
x510 Series	GS980EM Series
x510L Series	GS970M Series
IX5-28GPX	GS900MX/MPX Series
x310 Series	FS980M Series
x320 Series	AR4050S
x230 Series	AR3050S
x230L Series	AR2050V
x220 Series	AR2010V
	AR1050V

## Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI software version 2.6.0. To use Device GUI version 2.6.0 you must be running AlliedWare Plus 5.4.9-0.1 or later firmware on your device. However some of the new features are only available with 5.4.9-1.x firmware.

You can obtain the Device GUI software file from the [Software Download area of the Allied Telesis website](#). Log in using your assigned email address and password.

For information on accessing and updating the Device GUI, see [“Installing and Accessing the Web-based GUI on Switches” on page 28](#)

The following table lists model names that support this version:

Table 1: Models

Models	Family
SBx908 GEN2	SBx908 GEN2
SBx81CFC960	SBx8100
x950-28XSQ x950-28XTQm	x950
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930
x550-18SXQ x550-18XTQ x550-18XSPQm	x550



Table 1: Models (cont.)

Models	Family
x530-28GTXm x530-28GPXm x530L-52GPX x530-52GTXm x530-52GPXm	x530 and x530L
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L
IX5-28GPX	IX5
x310-26FT x310-50FT x310-26FP x310-50FP	x310
x320-10GH x320-11GPT	x320
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L
x220-28GS x220-52GT x220-52GP	x220
IE510-28GSX	IE510-28GSX
IE340-20GP IE340L-18GP	IE340
IE300-12GT IE300-12GP	IE300
IE210L-10GP IE210L-18GP	IE210L
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200
XS916MXT XS916MXS	XS900MX
GS980M/52 GS980M/52PS	GS980M
GS980EM/10H GS980EM/11PT	GS980EM

Table 1: Models (cont.)

Models	Family
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M
AR4050S AR3050S	AR-series UTM firewalls
AR2050V AR2010V AR1050V	AR-series VPN routers

## New Features and Enhancements

This section summarizes the new features in the Device GUI software version 2.6.0, for devices running AlliedWare Plus.

From version 2.6.0 onwards, the following new features and enhancements are available:

### PoE enhancements

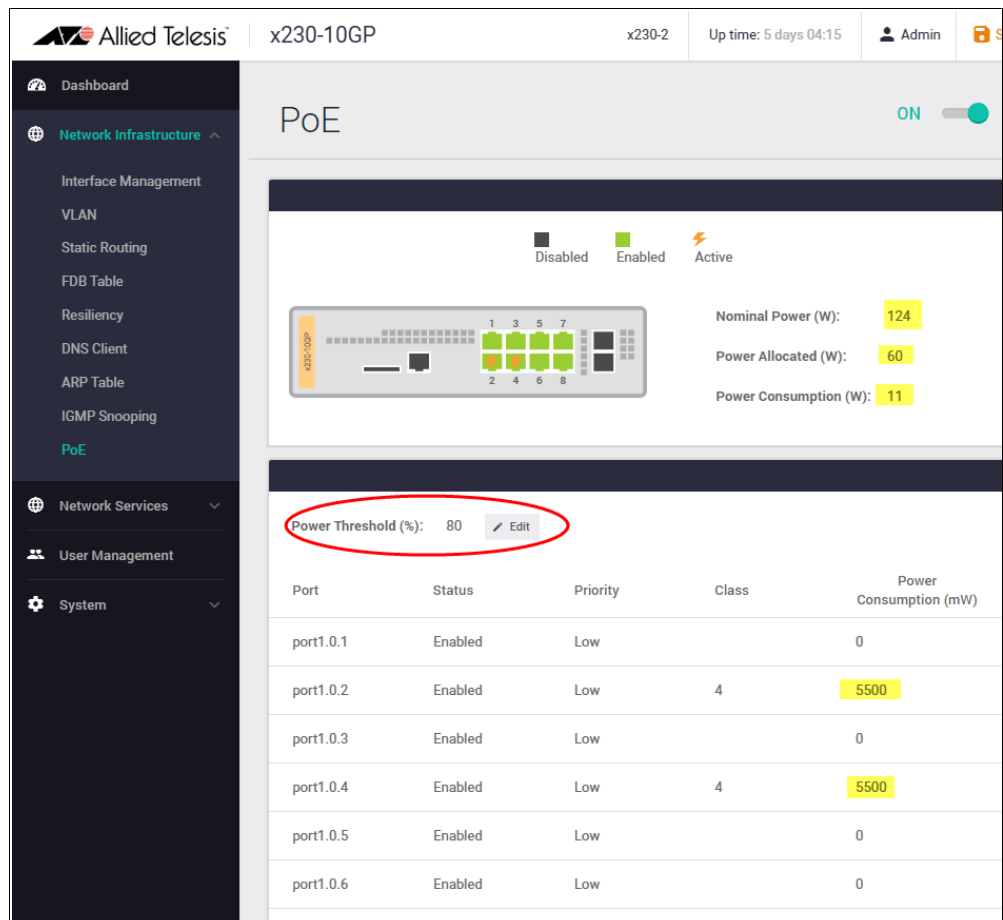
From version 2.6.0 onwards, you can use the GUI to:

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

### View detailed port information

*Menu location: Network Infrastructure > PoE*

With this software version, 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%.



The screenshot displays the PoE configuration page for device x230-10GP. The PoE status is currently ON. The power summary shows:

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

The Power Threshold (%) is set to 80, which is circled in red in the image. Below this, a table lists the port configurations:

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

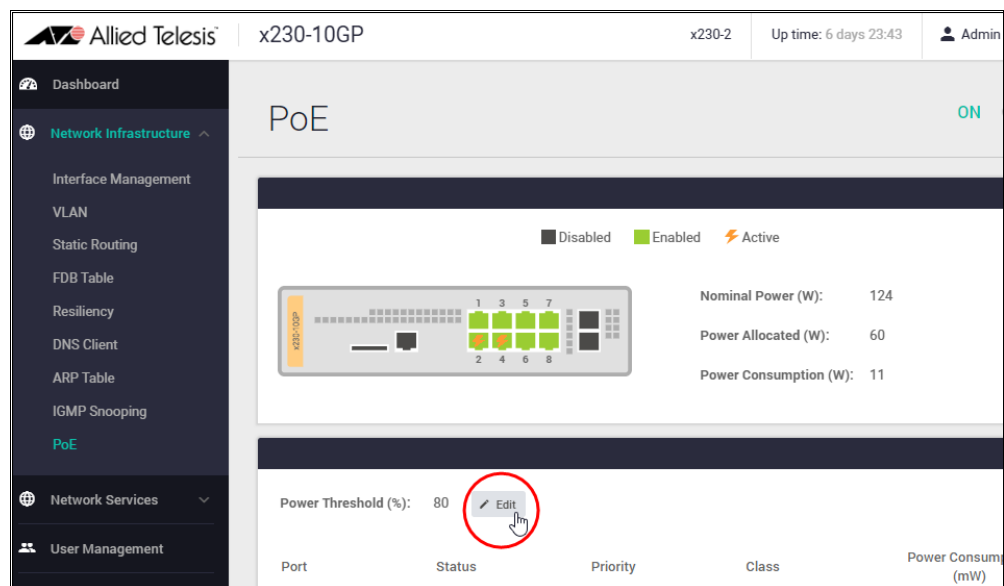
## Configure the PoE power threshold for a device

Menu location: Network Infrastructure > PoE

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:

- In the **Network Infrastructure > PoE** window
- Click on the Power Threshold (%) **Edit** button.



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



For more information on setting the PoE power threshold, see the [PoE Feature Overview and Configuration Guide](#).

## Configure the power priority per interface

Menu location: Network Infrastructure > PoE

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.

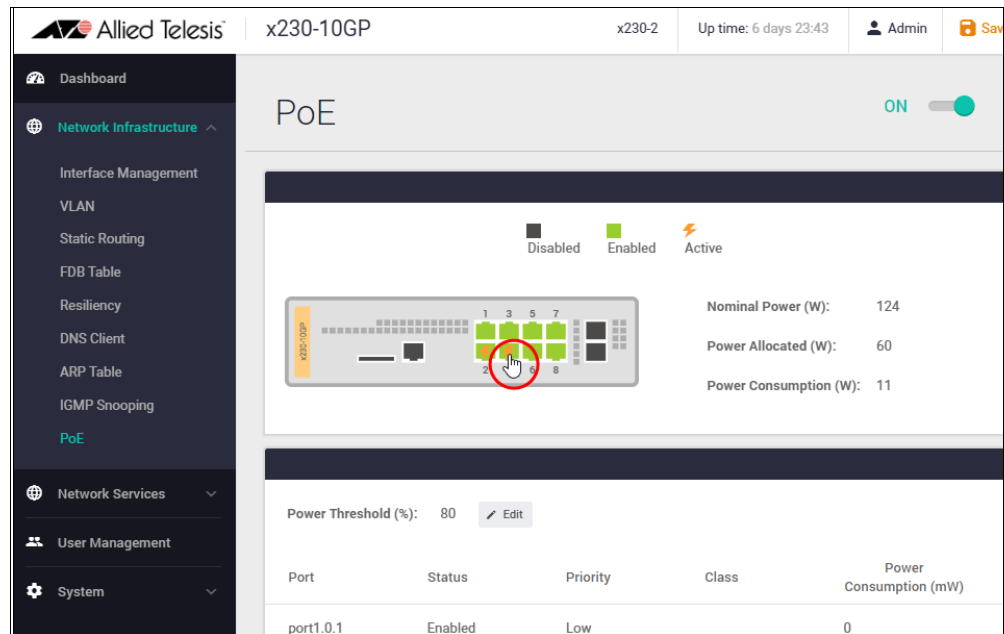
Port prioritization is the way the switch determines which ports are to receive power in the event that the needs of the PDs exceed the available power resources of the switch.

If power needs to be removed from some of the PoE ports, where if for example, one of the power supplies is disconnected; power will be removed from these ports in the order Low, High, and Critical.

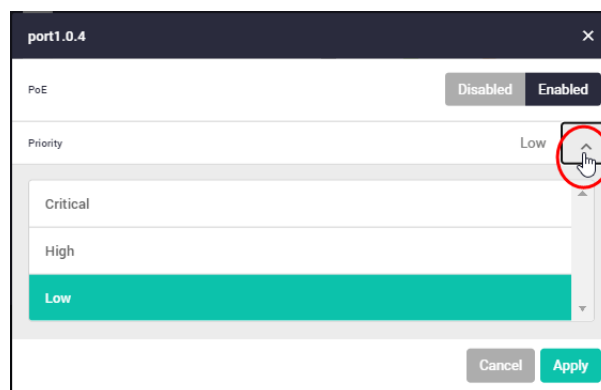
If there is not enough power to support all the ports set for a given priority level, power is provided to the ports based on the switch port number.

To change a port's power priority setting:

- In the **Network Infrastructure > PoE** window
- 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**.

## View contact and server location information

*Menu location: System > About*

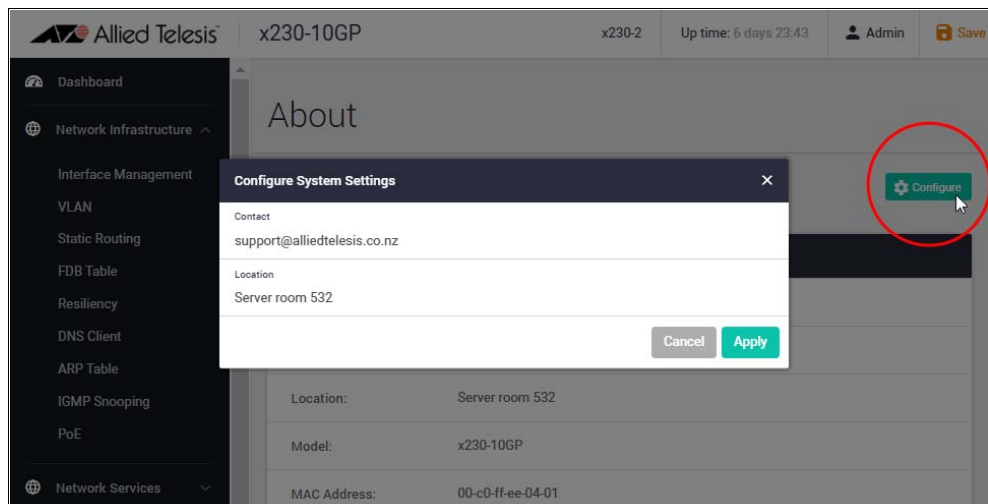
Previously, the server contact and server location information was configured using the commands:

- `snmp-server contact <string>`
- `snmp-server location <string>`

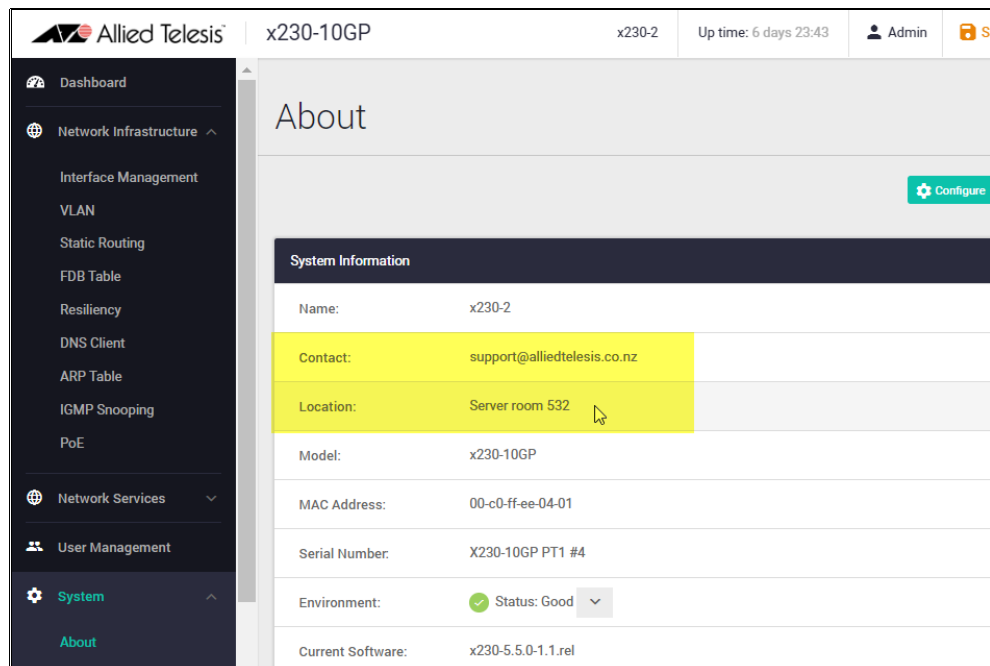
With this software update you can use the GUI to quickly configure and display these details on the **About** page.

To configure the contact and server location for a device:

- In the **System > About** window, click **Configure**
- Type in the **Contact** and **Location** details.
- Click **Apply**.



- The **System > About** page displays the contact and location details



## Configure up to 32 secondary IP addresses on an interface

*Menu location: Network Infrastructure > Interface Management*

From version 2.6.0 onwards, you can use the GUI to configure up to 32 secondary IP addresses on an interface. Previously, you could only configure one interface using the command:

```
ip address <ip-addr/prefix-length> [secondary] [label <label>]
```

Secondary IP addresses are most commonly used to:

- **Expand an existing subnet:**

There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.

- **Update older networks built using Level 2 bridges**

The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.

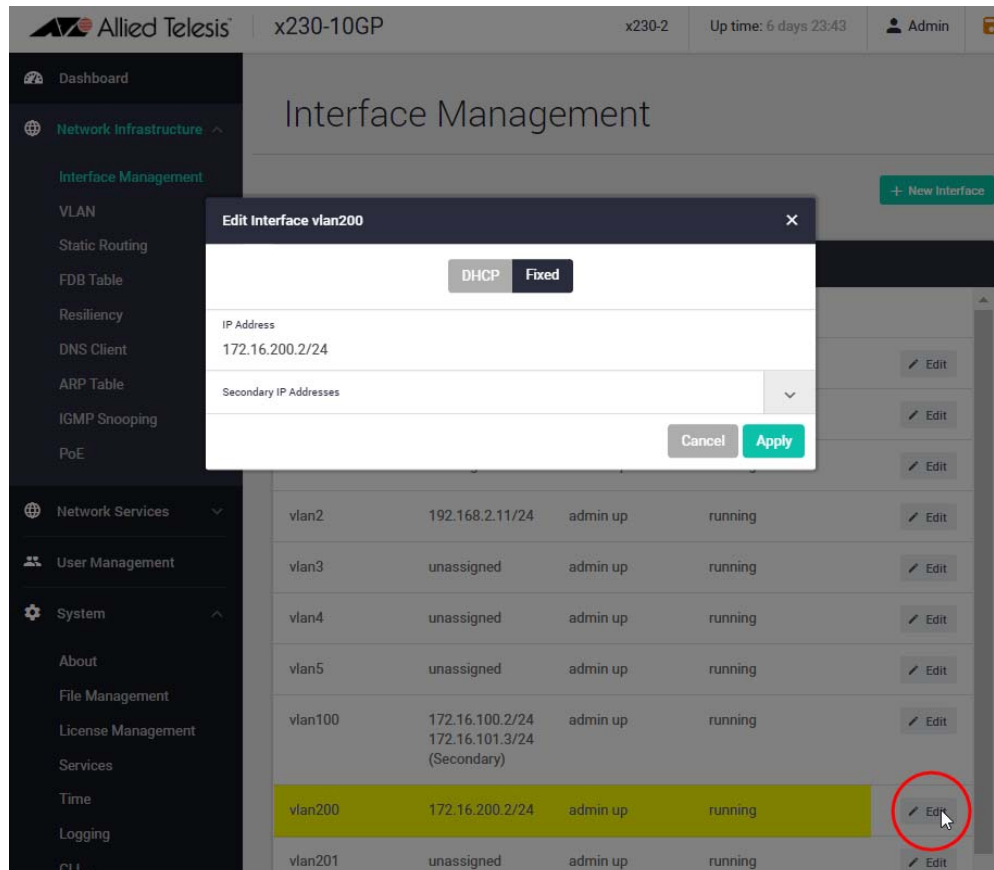
- **Combine separated subnets in a single network**

Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is extended, or layered on top of the second network using secondary addresses.

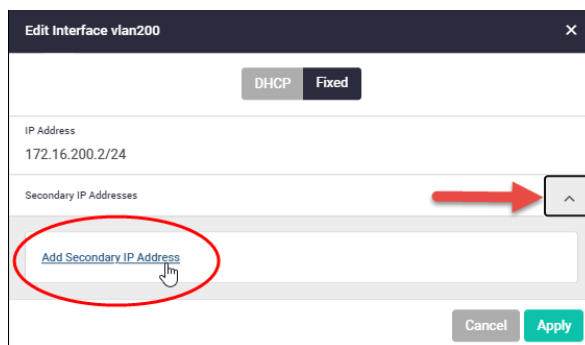
**Note:** A secondary interface can only be applied to an existing interface.

To configure a secondary IP address on an existing interface:

- In the **Network Infrastructure > Interface Management** window.
- Select an existing interface.
- Click **Edit**.



The **Edit Interface** window opens.

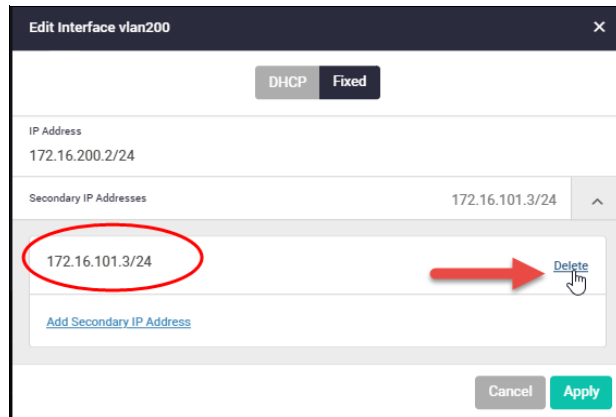


In the **Edit Interface** window:

- Click on the drop down box arrow.
- Click on the **Add Secondary IP Address** link.
- Type in the secondary IP address.
- Click **Apply**.



You can delete secondary IP addresses individually from an interface using the **Edit Interface** window.



## View and configure multicast router interfaces for IGMP snooping

*Menu location: Network Infrastructure > IGMP Snooping*

You can use the GUI to 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.

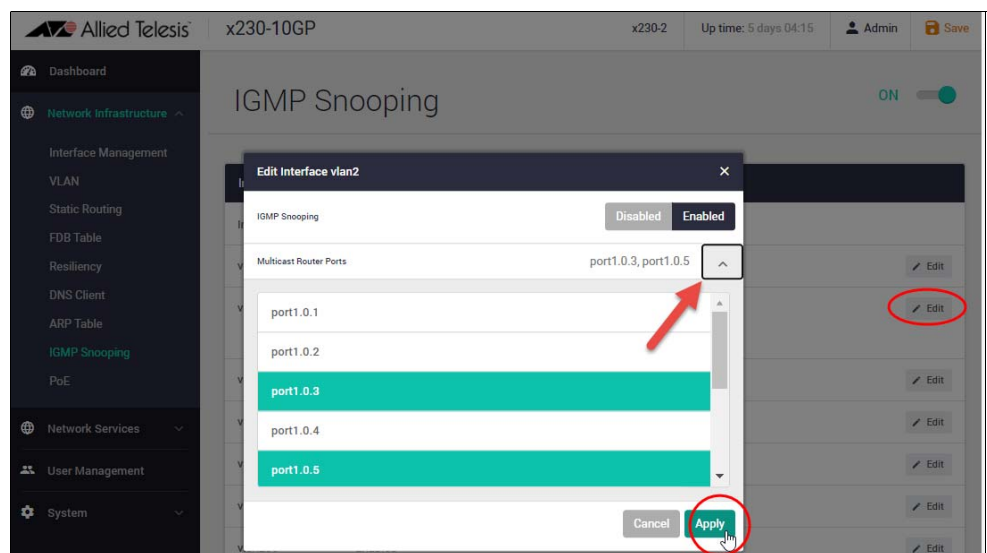
Previously, the function was only enabled by using the command:

```
ip igmp snooping mrouter interface <port>
```

The port 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).

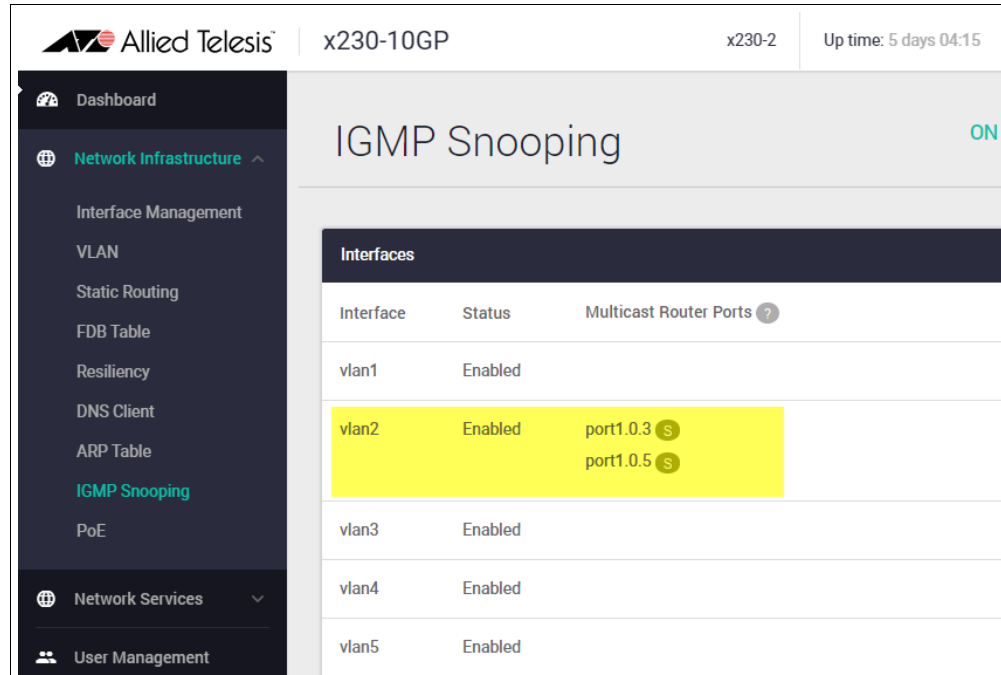
To configure an interface as an IGMP snooping multicast interface:

- In the **Network Infrastructure > IGMP Snooping** window
- Select an interface
- Click **Edit**
- The Edit Interface window opens.





In the **Edit Interface** window:

- Click on the drop down box arrow.
- Select the port(s) you wish to include.
- Click **Apply**.
- The IGMP Snooping window displays configured interfaces, their status, and which ports are assigned as multicast ports to an interface.



The screenshot shows the Allied Telesis GUI for device x230-10GP. The main heading is 'IGMP Snooping' with a status of 'ON'. A table titled 'Interfaces' lists the following data:

Interface	Status	Multicast Router Ports ?
vlan1	Enabled	
vlan2	Enabled	port1.0.3  port1.0.5 
vlan3	Enabled	
vlan4	Enabled	
vlan5	Enabled	

## Sort by columns on the FDB and ARP tables

Menu locations: *Network Infrastructure > FDB Table* and *Network Infrastructure > ARP Table*

You can sort the FDB and ARP tables by their individual columns.

From the **Network Infrastructure > FDB Table** (or ARP Table), 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.

The screenshot shows the 'FDB Table' interface for device 'x230-10GP'. The table contains the following data:

VLAN	Port/type	MAC Address	Mode	Learned Type
1	CPU	00c0.ffee.0401	Forward	Static
1	port1.0.3	eecd.6dd0.c136	Forward	Dynamic
2	port1.0.7	0000.f427.d630	Forward	Dynamic
2	CPU	00c0.ffee.0401	Forward	Static
2	port1.0.7	ce7f.dc5d.b53e	Forward	Dynamic

The screenshot shows the 'ARP Table' interface for device 'x230-10GP'. The table contains the following data:

IP Address	MAC Address	Interface	Port	Type
172.16.100.104	001a.ebcb.5e60	vlan100	port1.0.2	Dynamic
172.31.3.247	eecd.6dd0.c136	vlan4092	port1.0.3	Dynamic
172.16.100.1	eecd.6dd0.c136	vlan100	port1.0.3	Dynamic
172.16.100.105	001a.ebcb.21c0	vlan100	port1.0.4	Dynamic

1 - 4 of 4

# Installing and Accessing the Web-based GUI on Switches

This section describes how to access the GUI to manage and monitor your AlliedWare Plus switch.

The GUI is a convenient tool for monitoring your device's status and performing basic management tasks. Its dashboard provides at-a-glance monitoring of traffic and other key metrics.

On SBx908 GEN2 switches, x950 Series, x930 Series, and x530 Series, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

The steps for installing and accessing the GUI depend on whether the latest GUI has been pre-installed on your device in the factory.

## Check if the GUI is installed

To tell if the GUI is installed on your device, simply browse to it, as described below.

### Browse to the GUI

Perform the following steps to browse to the GUI.

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

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

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

2. Open a web browser and browse to the IP address from step 1.
3. If you do not see a login page, you need to install the GUI, as described in ["Install the GUI if it is not installed" on page 29](#). If you see a login page, log in. The default username is *manager* and the default password is *friend*.

### Check the GUI version

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

If you have an earlier version, update it as described in ["Update the GUI if it is not the latest version" on page 30](#)

## Install the GUI if it is not installed

Perform the following steps through the command-line interface if your AlliedWare Plus switch does not currently have a GUI installed.

1. Obtain the GUI file from our Software Download center. The file to use is `awplus-gui_550_20.gui`.

The file is not device-specific; the same file works on all devices.

2. Copy the file into Flash memory on your switch. You can copy the file into Flash using any of the following methods:

- « TFTP server
- « USB Flash drive
- « SD card

For example, to copy the GUI file from your USB Flash drive, use the following commands:

```
awplus>enable
awplus#copy usb awplus-gui_550_20.gui flash
```

To view all files in Flash and check that the newly installed file is there, use the following command:

```
awplus#dir
```

3. Delete any previous Java switch GUI files.

If you have been using the previous Java switch GUI, we recommend you delete the old GUI file to avoid any conflict. To do this, delete any Java files (.jar) from the switches Flash memory. For example:

```
awplus#del x510-gui_547_02.jar
```

4. If you haven't already, add an IP address to a VLAN on the switch. For example:

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

5. Make sure the HTTP service is running:

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

6. Log into the GUI:

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

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

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

## Update the GUI if it is not the latest version

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

1. Obtain the GUI file from our Software Download center. The file to use is `awplus-gui_550_20.gui`.

The file is not device-specific; the same file works on all devices.

2. Copy the file into Flash memory on your switch. You can copy the file into Flash using any of the following methods:

- « TFTP server
- « USB Flash drive
- « SD card

For example, to copy the GUI file from your USB Flash drive, use the following commands:

```
awplus>enable  
awplus#copy usb awplus-gui_550_20.gui flash
```

To view all files in Flash and check that the newly installed file is there, use the following command:

```
awplus#dir
```

3. Stop and restart the HTTP service:

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

4. Log into the GUI:

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

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

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

# Installing and Accessing the Web-based GUI on AR-Series Devices

This section describes how to access the GUI to manage and monitor your AlliedWare Plus device.

The GUI is a convenient tool for monitoring your device's status and performing basic management tasks. Its dashboard provides at-a-glance monitoring of traffic and other key metrics.

On AR4050S and AR3050S firewalls, you can use the GUI to create an advanced application-aware firewall with features such as Application control and Web control. Alternatively, you can configure real-time threat protection with URL filtering, Intrusion Prevention and Malware protection.

The steps for installing and accessing the GUI depend on whether the latest GUI has been pre-installed on your device in the factory.

## Check if the GUI is installed

To tell if the GUI is installed on your device, simply browse to it, as described below.

### Browse to the GUI

Perform the following steps to browse to the GUI.

**Prerequisite:** If the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the “Configuring a Firewall Rule for Required External Services” section in the [Firewall and Network Address Translation \(NAT\) Feature Overview and Configuration Guide](#).

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

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

Alternatively, you can use the default address on unconfigured devices, which is 192.168.1.1.

2. Open a web browser and browse to the IP address from step 1.
3. If you do not see a login page, you need to install the GUI, as described in “[Install the GUI if it is not installed](#)” on page 32. If you see a login page, log in. The default username is *manager* and the default password is *friend*.

### Check the GUI version

To see which version you have, open the About page in the GUI and check the field called **GUI version**. The version to use is 2.5.0. If you have an earlier version, update it as described in “[Install the GUI if it is not installed](#)” on page 32.

## Install the GUI if it is not installed

Perform the following steps through the command-line interface if your AR-series device does not currently have a GUI installed.

1. If the device's firewall is enabled, create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the [Firewall and Network Address Translation \(NAT\) Feature Overview and Configuration Guide](#).
2. If you haven't already, create one or more IP interfaces and assign them IP addresses, including configuring WAN connectivity. For information about configuring PPP, see the [PPP Feature Overview and Configuration Guide](#). For information about configuring IP, see the [IP Feature Overview and Configuration Guide](#).

3. Use the following command to download and install the GUI:

```
awplus# update webgui now
```

4. Make sure the HTTP service is running:

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

5. Log into the GUI:

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

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

## Update the GUI if it is not the latest version

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

1. Use the following command to download and install the GUI:

```
awplus# update webgui now
```

2. Stop and restart the HTTP service:

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

3. Log into the GUI:

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

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