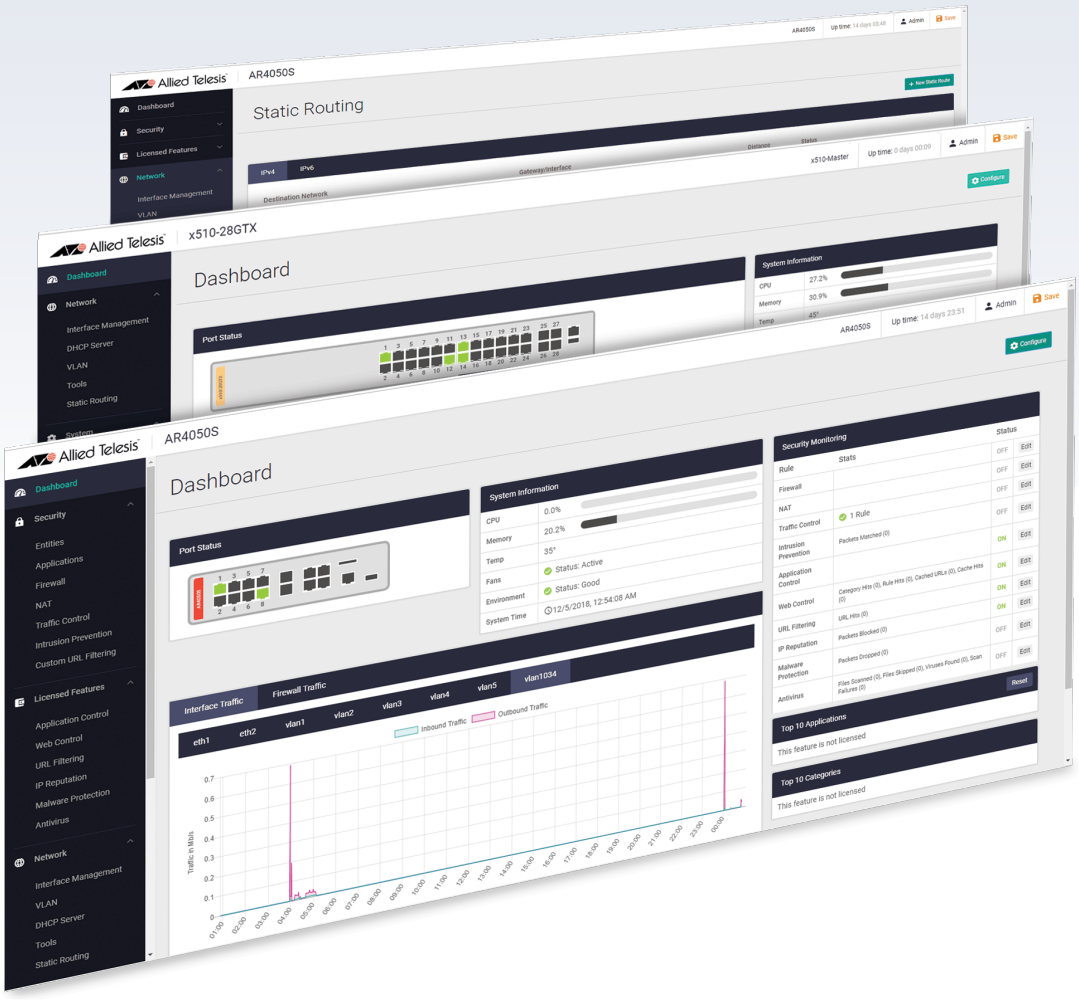
Release Note for Web-based Device GUI Version 2.14.x



» 2.14.0

AlliedWare Plus OPERATING SYSTEM

Acknowledgments

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/**

Contents

What's New in Version 2.14.0

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330-10GTX
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
10 GbE Virtual UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.14.0. You can run 2.14.0 with AlliedWare Plus firmware versions 5.5.1-x.x, 5.5.2-x.x, or 5.5.3-x.x on your device, although the latest GUI features may only be supported with the latest firmware version.

For information on accessing and updating the Device GUI, see "Accessing and Updating the Web-based GUI" on page 13.

The following table lists model names that support this version:

Table 1: Models and software file names

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

Table 1: Models and software file names (cont.)

Models	Family
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L
x330-10GTX x330-20GTX x330-28GTX	x330
x320-10GH x320-11GPT	x320
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
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340
IE210L-10GP IE210L-18GP	IE210L
XS916MXT XS916MXS	XS900MX
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX
GS980EM/10H GS980EM/11PT	GS980EM
GS980M/52 GS980M/52PS	GS980M
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX

Table 1: Models and software file names (cont.)

Models	Family
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
10 GbE Virtual UTM Firewall	vFW
AR4050S AR4050S-5G 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 2.14.0.

Generate technical support data for AR4000S-Cloud

Available on: AR4000S-Cloud advanced virtual UTM firewall running AlliedWare Plus 5.5.3-0.1 onwards

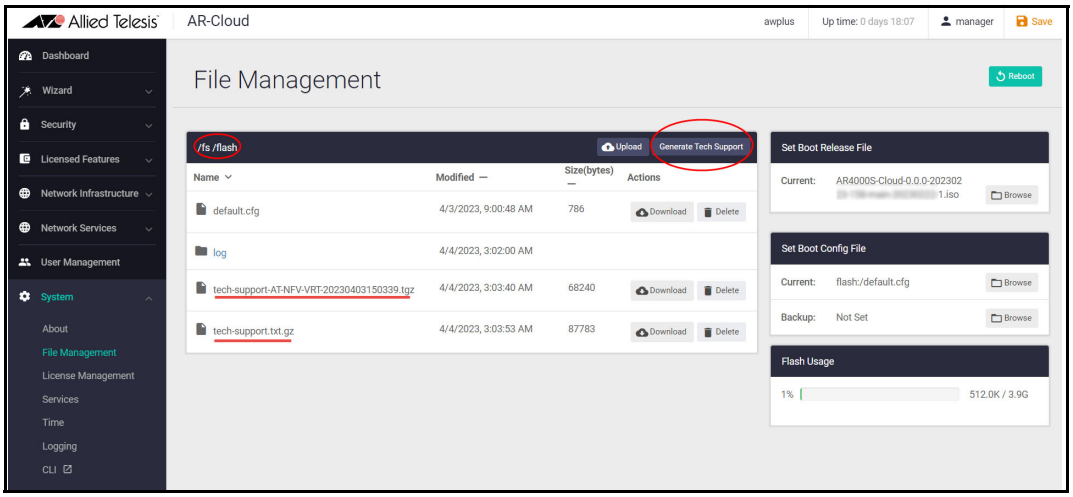
The Device GUI now allows you to generate tech-support output for the AR4000S-Cloud.

Tech-support output can assist with troubleshooting. If you contact Allied Telesis for support, you can include these tech-support files.

To generate tech support output:

1. Make sure the application is running.
2. From the AR-Cloud dashboard menu, navigate to **System** > **File Management**
3. Click the **Generate Tech Support** button. The application generates the tech support output and stores it in the appliance **/fs/flash** directory.
4. Wait while the application generates the tech-support output. This can take up to a few minutes. The larger the tech support data, the longer this takes.
5. Navigate to **System** > **File Management** and the **/fs/flash** directory to view or download the output. You may need to refresh the page to see the new files.

There are two tech support files generated, one for the container platform and the other for the virtual application. Both files should be sent to Allied Telesis support to assist with troubleshooting.

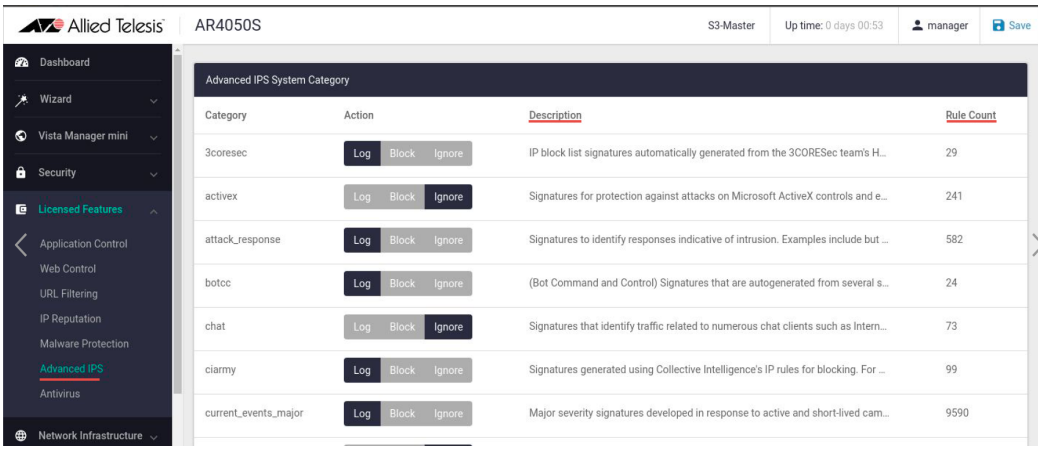


Enhanced IPS category tables

Available on: AR4050S, AR4050S-5G, and 10GbE UTM Firewall

From version 2.14.0 onwards, the IPS category tables includes two addional columns:

- **Description** - explains what the category of rules is used for.
- **Rule Count** - a count to help you understand the performance impact (i.e. more rules = slower performance).



The Description and Rule Count columns are visible in the following tables:

- Security > Intrusion Prevention System Category
- Licensed Features > Advanced IPS System Category

Previously, the CLI show command output displayed these fields. Now the Device GUI provides this information as well.

```
awplus#show ips categories detail
Rule Statistics:
 Usage:              35657/39383
 Alert:              35657
 Deny:               0
 Disable:            3726

  Category (* = invalid) Action  Rules Description
------------------------------------------------------------------------------
  ...
  activex               disable 242   Signatures for protection against
                                        attacks on Microsoft ActiveX controls
                                        and exploits targeting vulnerabilities
                                        in ActiveX controls
  attack-response       alert   583   Signatures to identify responses
                                        indicative of intrusion. Examples
                                        include but not limited to LMHost file
                                        download, presence of web banners and
                                        the detection of Metasploit
                                        Meterpreter kill command. These are
                                        designed to catch the results of a
                                        successful attack
  ...
  current-events-major  alert   9621  Major severity signatures developed in
                                        response to active and short-lived
                                        campaigns and high-profile items that
                                        are expected to be temporary. One
                                        example is fraud campaigns related to
                                        disasters
  ...
```

Device GUI support for 5G router firmware upgrades

Available on: AR4050S-5G

From Device GUI version 2.14.0 onwards, you can upgrade firmware and carrier files using the Device GUI.

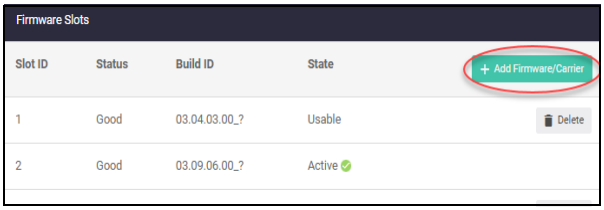
From the Device GUI main menu:

1. Go to **Network Infrastructure > Wireless WAN**.

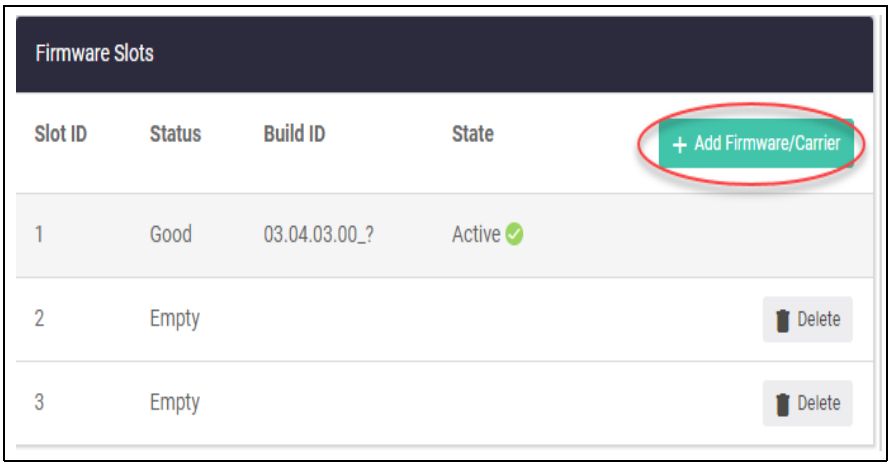
2. Click on the **Carriers** tab.

The **Firmware Slots** dialog displays the slot ID, status, and build ID as well as the state of the slot. For example, if the firmware slot is good or empty and is usable or active:

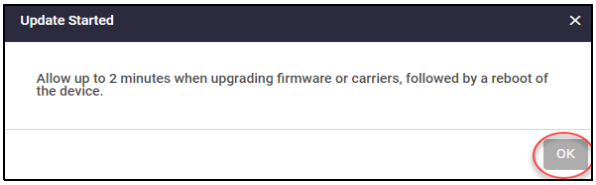
3. To add firmware and carriers click on the **+ Add Firmware/Carrier** button:



4. From the **Add Firmware/Carrier** dialog, select the required firmware file and the matching carrier name file from their correct locations and click **Apply**:

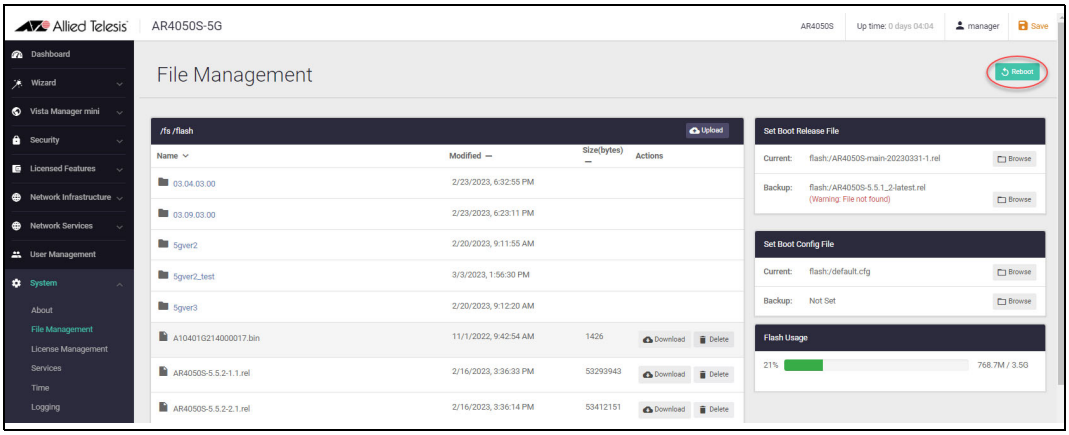


5. The following **Update Started** dialog appears, click the **OK** button to proceed:



NOTE: To ensure the files have been copied successfully, wait 2 minutes then reboot your device.

6. To reboot your device, from the **main menu**, select **System** > **File Management**:



7. Click the **Reboot** button and wait for the device to come back up.

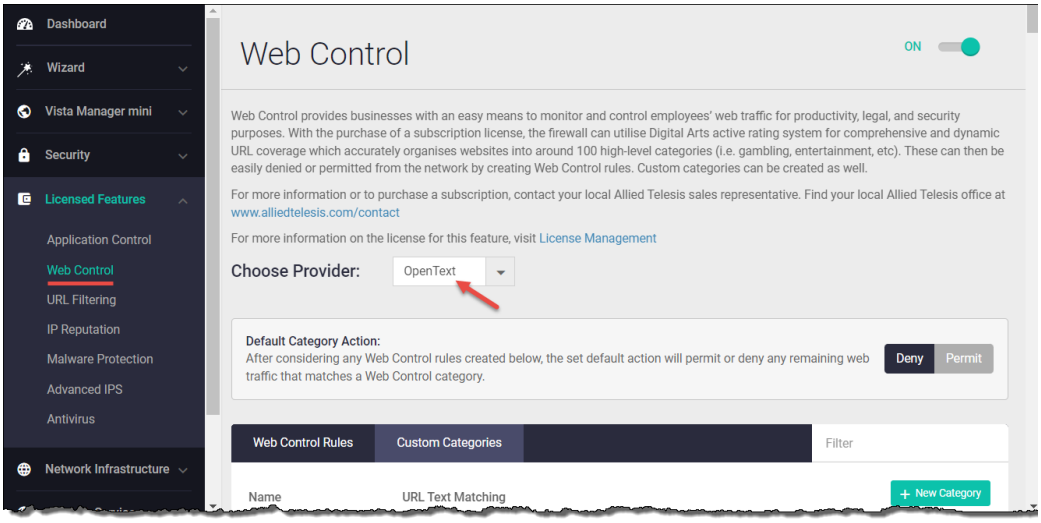
For detailed documentation on 5G mobile broadband UTM Firewall configuration, see 5G Mobile UTM Firewall Feature Overview and Configuration Guide.

Webroot renamed as OpenText

Available on: AR4050S, AR4050S-5G, and vFW

From version 5.5.3-0.1 onwards, the AlliedWare Plus provider for the Web Categorization and Web Control features has been renamed.

Formerly Webroot, the provider is now known as OpenText. While the name has changed, the functionality remains the same as before.



For more information about advanced network security features on the AlliedWare Plus UTM firewalls, see the Advanced Network Protection Feature Overview and Configuration Guide.

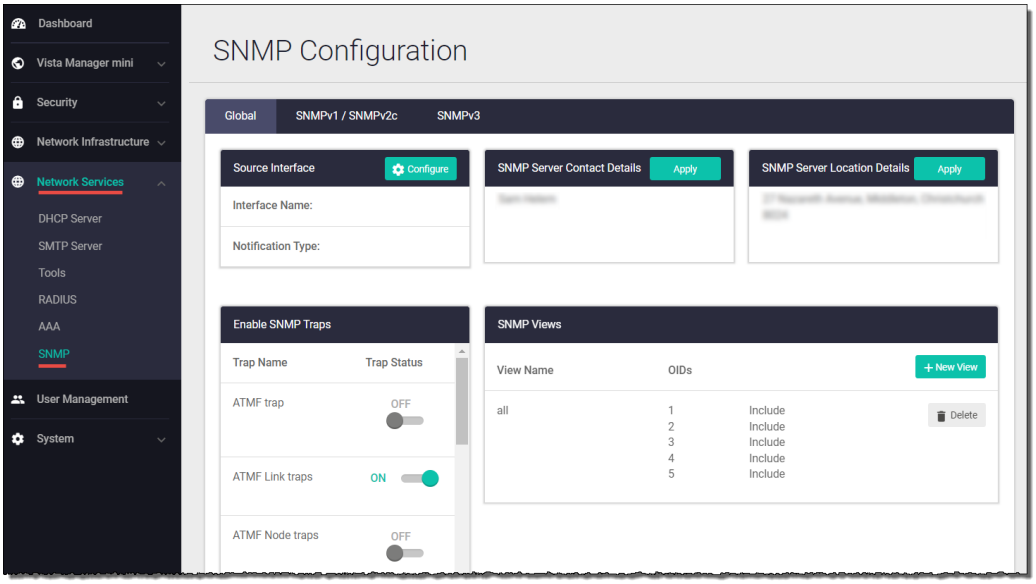
SNMP configuration improved access

Available on devices running AlliedWare Plus version 5.5.1-1 onwards.

A Simple Network Management Protocol (SNMP) is the protocol used for communication between management stations and managed devices.

From Device GUI version 2.14.0 onwards, you can use the GUI to configure SNMP options, including the ability to create and delete views, groups, users, and supported traps. Previously, you needed to use the CLI to configure SNMP.

The **SNMP** menu is located under the **Network Services** menu:



Notes

- You cannot edit views, groups, users, communities, and trap hosts. To make changes, you must first delete the view/group/user/community/trap host and then add it again.
- SNMP is enabled by default. You cannot enable or disable it from the Device GUI.

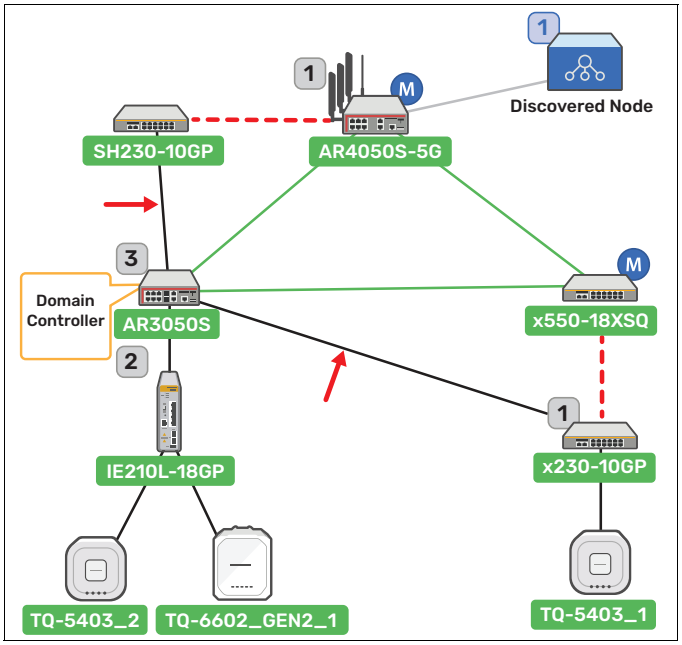
For more information about SNMP and AlliedWare Plus devices, see the SNMP Overview and Configuration Guide.

Network map displays AMF Plus cross-links based on actual topology

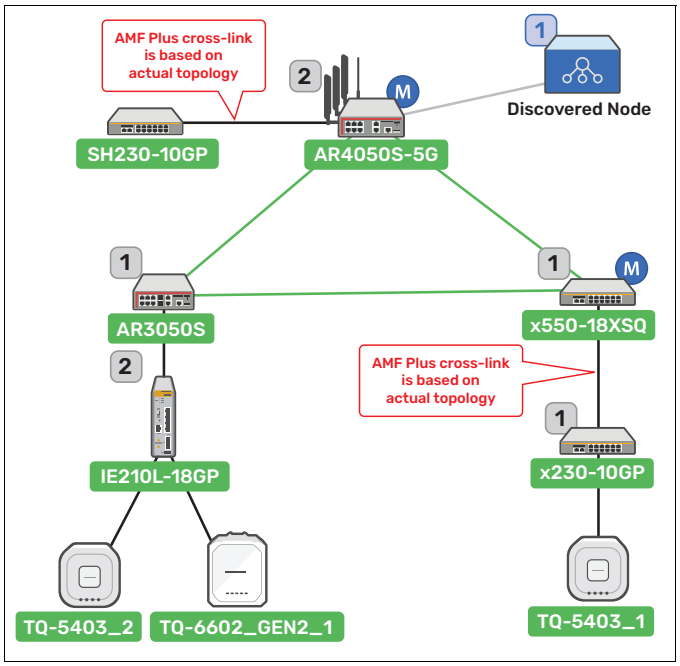
Available on devices running AlliedWare Plus version 5.5.1-1 onwards.

From Device GUI version 2.14.0 onwards, the network map correctly draws AMF Plus cross-links between the AMF Plus nodes the cross-link is configured on. Previously all cross-links in a domain were drawn between the node and the Domain Controller.

Previously For example, in this older network map, the Domain Controller is the AR3050S. The two AMF Plus cross-links (indicated by arrows) were drawn based on the Domain Controller.



Now From Device GUI 2.14 onwards, the AMF Plus cross-links are displayed based on the actual topology.



Accessing and Updating the Web-based GUI

This section describes how to access the GUI, check the version, and update it.

Important Note: Very old browsers may not be able to access the Device GUI. From AlliedWare Plus version 5.5.2-2.1 onwards, to improve the security of the communication for the Device GUI, ciphersuites which use RSA or CBC based algorithms have been disabled, as they are no longer considered secure. Note that the removal of ciphersuites using those algorithms may prevent some old versions of browsers from communicating with the device using HTTPS.

Browse to the GUI

Perform the following steps to browse to the GUI.

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

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

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

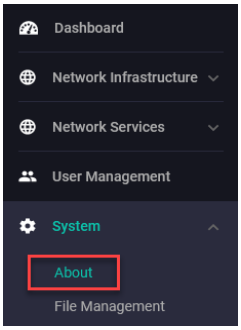
   - on switches: 169.254.42.42
   - on AR-Series: 192.168.1.1

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

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

Check the GUI version

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



If you have an earlier version than 2.14.0, update it as described in "Update the GUI on switches" on page 14 or "Update the GUI on AR-Series devices" on page 15.

Update the GUI on switches

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

1. Obtain the GUI file from our Software Download center. The filename for v2.14.0 of the GUI is:

   - awplus-gui_553_29.gui
   - awplus-gui_552_29.gui, or
   - awplus-gui_551_29.gui

   Make sure that the version string in the filename (e.g. 553) matches the version of AlliedWare Plus running on the switch. The file is not device-specific; the same file works on all devices.

2. Log into the GUI:

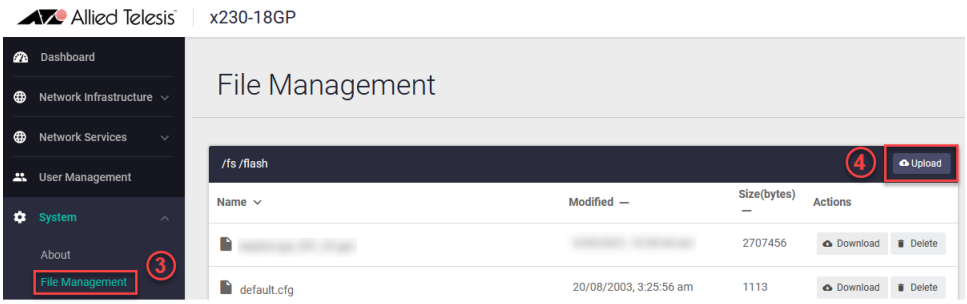
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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

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

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

4. Click **Upload**.



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

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

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

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

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

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

Update the GUI on AR-Series devices

Prerequisite: On AR-Series devices, 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.

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 a Serial console connection or SSH to access the CLI, then use the following commands to download the new GUI:

```
awplus> enable
awplus# update webgui now
```

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

1. Use a Serial console connection or SSH to access the CLI, then use the following commands to download the new GUI:

```
awplus> enable
awplus# update webgui now
```

2. Browse to the GUI and check that you have the latest version now, on the **System** > **About** page. You should have v2.14.0 or later.