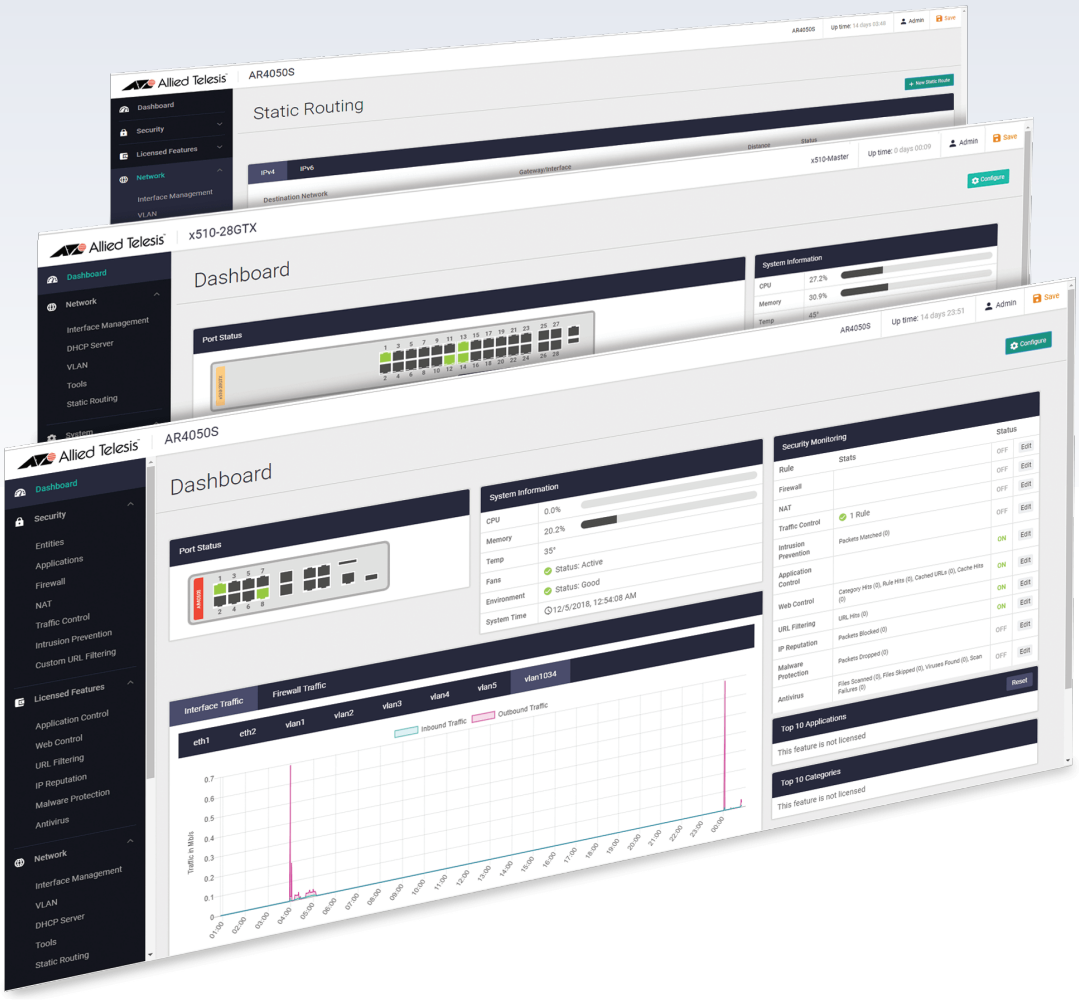
Release Note for Web-based Device GUI Version 2.19.x



» 2.19.0

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 2.19.0

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
x240 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V[2]
AR2010V[2]
AR1050V
TQ6702 GEN2-R

1. Not available in all regions
2. Does not support all of the latest features

Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.19.0. You can run 2.19.0 with AlliedWare Plus firmware versions 5.5.4-x.x, 5.5.3-x.x, or 5.5.2-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 11.

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

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

Models	Family
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
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 x330-52GTX	x330
x320-10GH x320-11GPT	x320
x240-10GTXm x240-10GHXm	x240
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
IE220-6GHX IE220-10GHX	IE220
IE210L-10GP IE210L-18GP	IE210L
SE240-10GTXm[1] SE240-10GHXm[1]	SE240
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

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

Models	Family
GS970EMX/10 GS970EMX/20 GS970EMX/28 GS970EMX/52	GS970EMX
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M
10GbE UTM Firewall	
AR4000S Cloud	
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls
AR2050V[2] AR2010V[2] AR1050V	AR-series VPN routers
TQ6702 GEN2-R	Wireless AP Router

1. Not available in all regions
2. Does not support all of the latest features

New Features and Enhancements

This section summarizes the new features in the Device GUI software version 2.19.0.

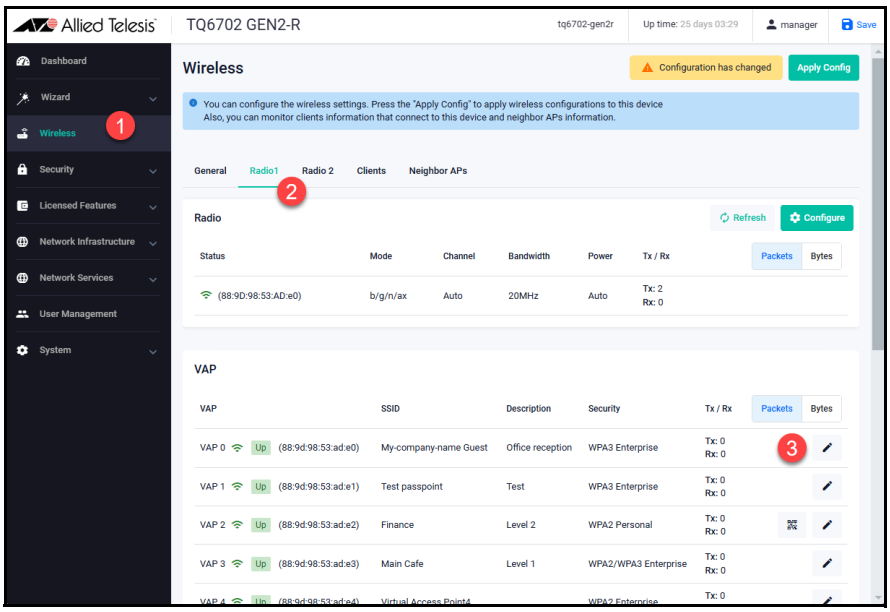
Support for CCMP cipher with WPA3 encryption on TQ6702 GEN2-R

From version 2.19.0 onwards, the CCMP cipher is supported for WPA Enterprise version WPA3 on TQ6702 GEN2-R wireless AP routers. The default cipher for WPA3 is still GCMP.

This enhancement means you can now select either CCMP or GCMP as the cipher.

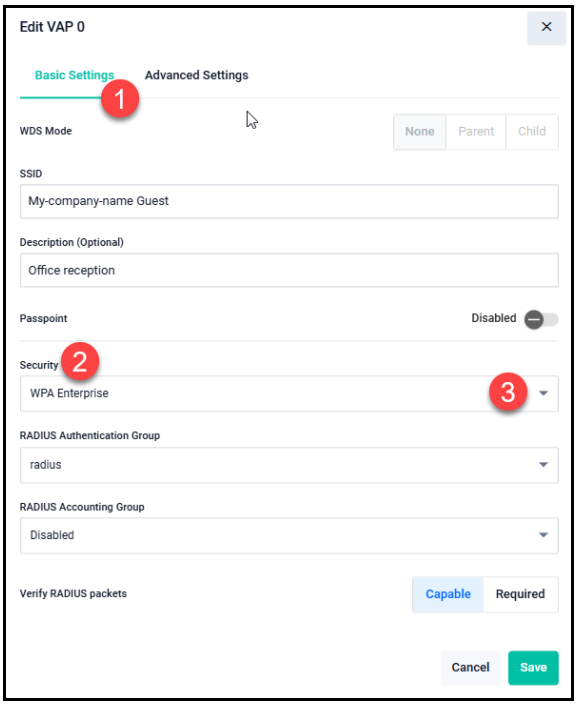
To configure CCMP as the cipher, select:

1. **Wireless**
2. **Radio**
3. **Edit VAP**

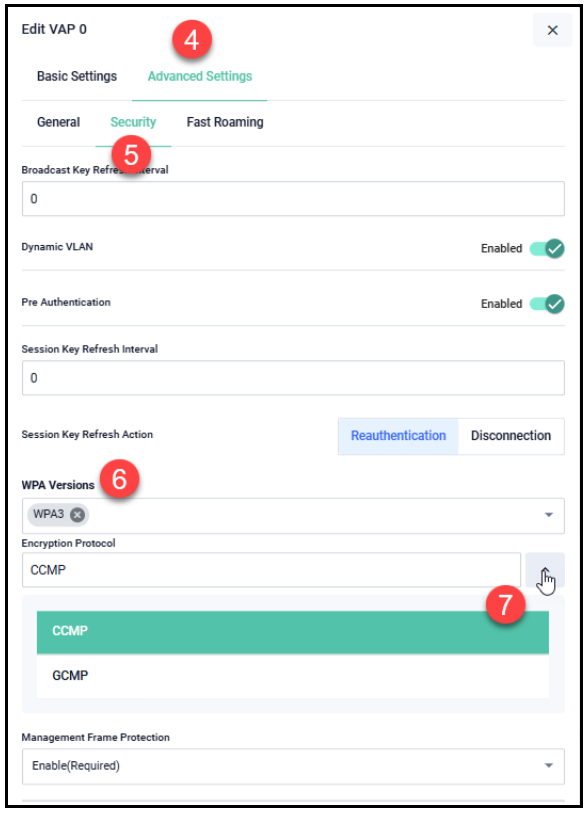


In **Edit VAP**, select:

1. **Basic Settings**
2. **Security**
3. **WPA Enterprise**



4. **Advanced Settings**
5. **Security**
6. **WPA Versions** - WPA3
7. **Encryption Protocol** - CCMP



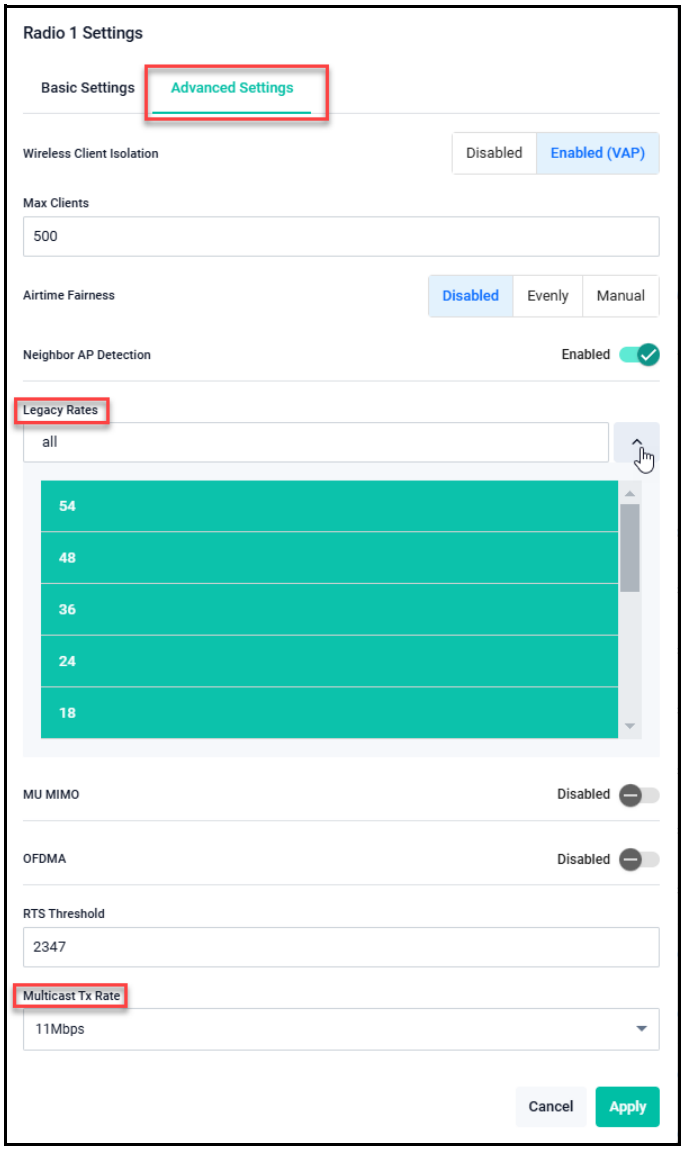
Removal of requirement to specify a basic rate on TQ6702 GEN2-R

From version 2.19.0 onwards, you are no longer required to specify a **basic** rate for Radio 1, when you specify the legacy rates to use. Basic rates are the most backward compatible rates in a Wi-Fi network - rates that will work with the oldest Wi-Fi standards. For 2.4Ghz, the basic rates are: 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps. For 5Ghz, the basic rates are: 6Mbps, 12Mbps, and 24Mbps.

Previously, you had to at least select 1 basic rate.

The purpose of this change is to allow you to stop 802.11b clients from connecting, as that standard uses a data rate between 1-11 Mbps.

If none of the basic rates is specified, the device will use the lowest selected **legacy** rate as the basic rate. Note that the beacon frame and management frame must use this lowest rate. This enhancement means that the multicast transfer rate you can specify has also changed.



Support for Dynamic VLAN with MAC-Auth on TQ6702 GEN2-R

From version 2.19.0, the TQ6702 GEN2-R supports Dynamic VLAN with MAC authentication on wireless networks, including WPA Personal. This enables dynamic VLAN assignment based on authentication, achieved through coordination between the TQ6702 GEN2-R (authenticator) and the RADIUS server.

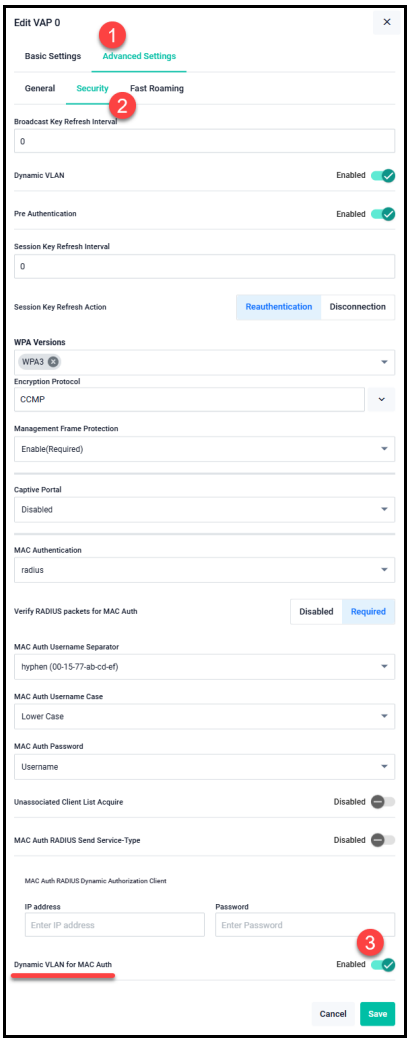
When the RADIUS server sends a RADIUS Access-Accept message to the authenticator, it can include attributes specifying the VLAN to which the authenticated device should be assigned.

Previously, with MAC authentication, VLAN assignment was based on the VAP the client connected to. In contrast, Dynamic VLAN allows each client to be assigned a specific VLAN individually.

To configure this, go to: **Wireless** > **Radio** > **Edit VAP**

Then select:

1. **Advanced Settings**
2. **Security**
3. **Enable Dynamic VLAN for MAC Auth**



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 and TQ6702 GEN2-R: 192.168.1.1

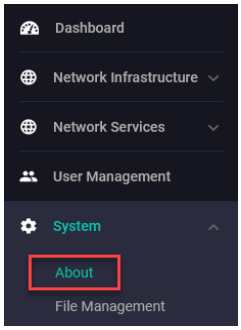
2. Open a web browser and browse to the IP address from step 1.

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 2.19.0, update it as described in "Update the GUI on switches" on page 12 or "Update the GUI on AR-Series devices" on page 13.



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 the Allied Telesis Support Portal.

   The filename for v2.19.0 of the GUI is:

   - awplus-gui_554_37.gui
   - awplus-gui_553_37.gui, or
   - awplus-gui_552_37.gui

   Make sure that the version string in the filename (e.g. 554) 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:

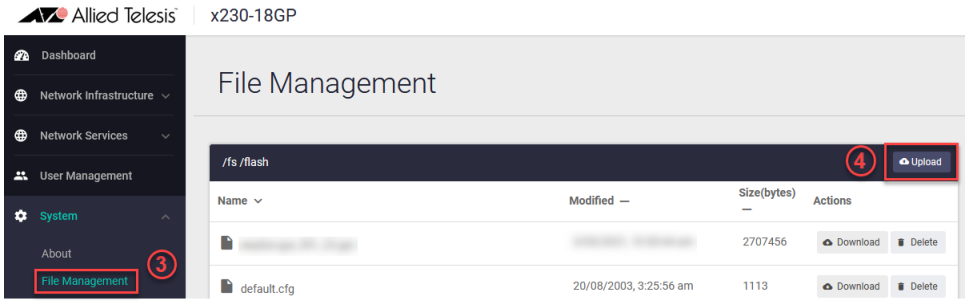
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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

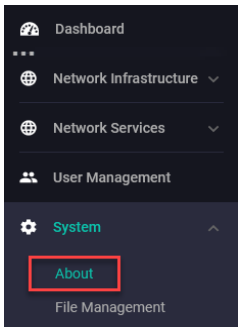
Prerequisite: On AR-Series devices, if the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

Perform the following steps 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 v2.19.0 or later.



Verifying the GUI File

On devices that support crypto secure mode, to ensure that the GUI file has not been corrupted or interfered with during download, you can verify the GUI file. To do this, enter Global Configuration mode and use the command:

```
awplus(config)#crypto verify gui <hash-value>
```

Where <*hash-value*> is the known correct hash of the file.

This command compares the SHA256 hash of the release file with the correct hash for the file.

The correct hash is listed in the table of Hash values below or in the release's sha256sum file, which is available from the Allied Telesis Download Center.

Caution

If the verification fails, the following error message will be generated:
"% Verification Failed"
In the case of verification failure, please delete the release file and contact Allied Telesis support.

If you want the device to re-verify the file when it boots up, add the **crypto verify** command to the boot configuration file.

Table: Hash values

Firmware Version	GUI File	Hash
5.5.4-x.x	awplus-gui_554_37.gui	9ec143214c63fbfb3b8a5ec9fb65c0317b21cea4fdcabe53a749e4275987a8d6
5.5.3-x.x	awplus-gui_553_37.gui	9ec143214c63fbfb3b8a5ec9fb65c0317b21cea4fdcabe53a749e4275987a8d6
5.5.2-x.x	awplus-gui_552_37.gui	9ec143214c63fbfb3b8a5ec9fb65c0317b21cea4fdcabe53a749e4275987a8d6