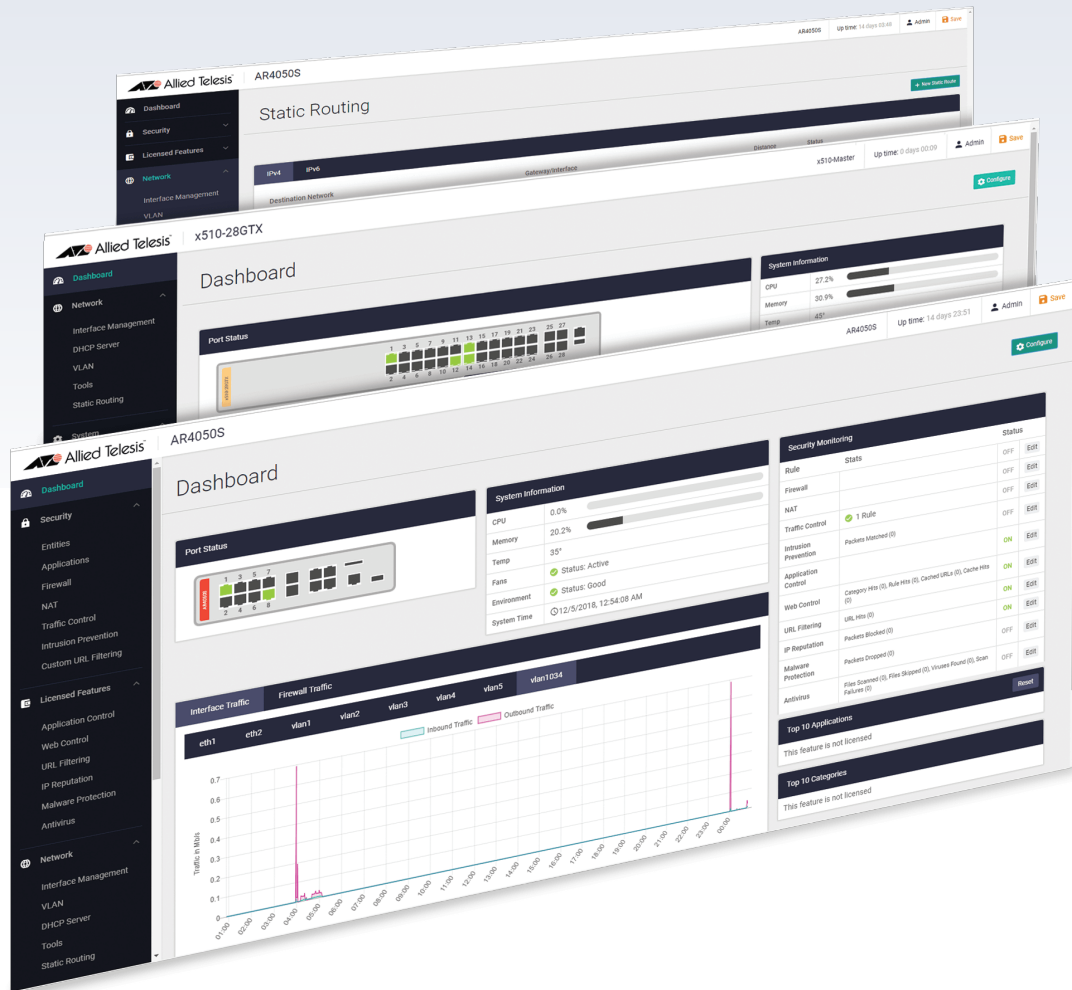


Release Note for Web-based Device GUI Version 2.10.x



» 2.10.0

AlliedWare Plus
OPERATING SYSTEM

Acknowledgments

©2021 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/

Contents

What's New in Version 2.10.0	1
Introduction	1
New Features and Enhancements	4
Read-only support on wireless for Vista mini	4
Usability improvements in Vista mini.....	5
Configuring TQ access points.....	8
Captive Portal re-authentication timer	9
Accessing and Updating the Web-based GUI.....	11

What's New in Version 2.10.0

Product families supported by this version:

SwitchBlade x908 GEN2	XS900MX Series
SwitchBlade x8100 Series	GS980MX Series
x950 Series	GS980M Series
x930 Series	GS980EM Series
x550 Series	GS970M Series
x530 Series	GS900MX/MPX Series
x530L Series	FS980M Series
x510 Series	AR4050S
x510L Series	AR3050S
IX5-28GPX	AR2050V
x310 Series	AR2010V
x320 Series	AR1050V
x230 Series	
x230L Series	
x220 Series	
IE510-28GSX-80	
IE340 Series	
IE340L Series	
IE300 Series	
IE210L Series	
IE200 Series	

Introduction

This release note describes the new features in the Allied Telesis Web-based Device GUI version 2.10.0. You can run 2.10.0 with any AlliedWare Plus firmware version on your device, although recent GUI features may only be supported with recent firmware versions.

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

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

Table 1: Models (cont.)

Models	Family
x550-18SXQ x550-18XTQ x550-18XSPQm	x550
x530DP-28GHXm x530DP-52GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX x530L-10GHXm	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
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340 and IE340L
IE300-12GT IE300-12GP	IE300
IE210L-10GP IE210L-18GP	IE210L

Table 1: Models (cont.)

Models	Family
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200
XS916MXT XS916MXS	XS900MX
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX
GS980M/52 GS980M/52PS	GS980M
GS980EM/10H GS980EM/11PT	GS980EM
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

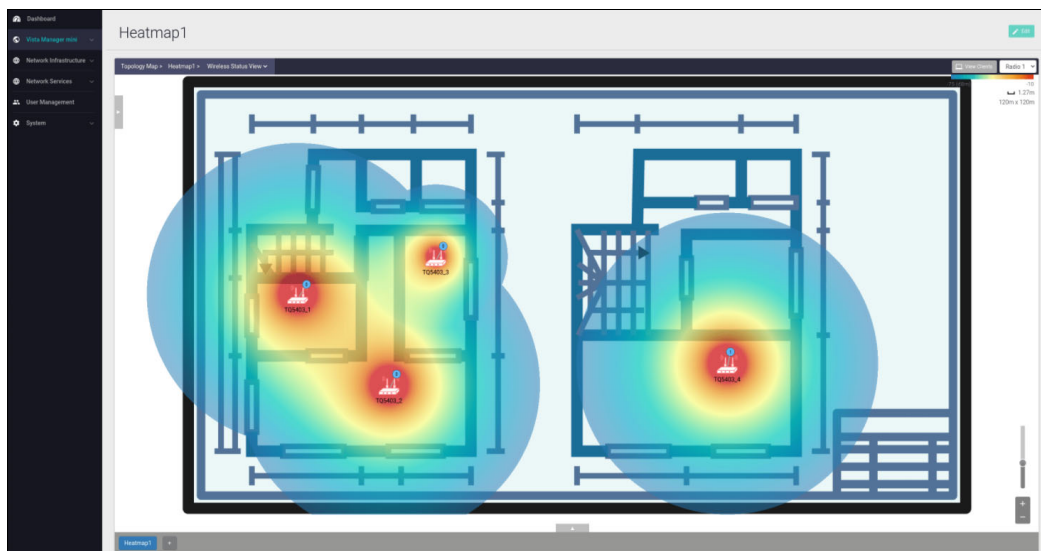
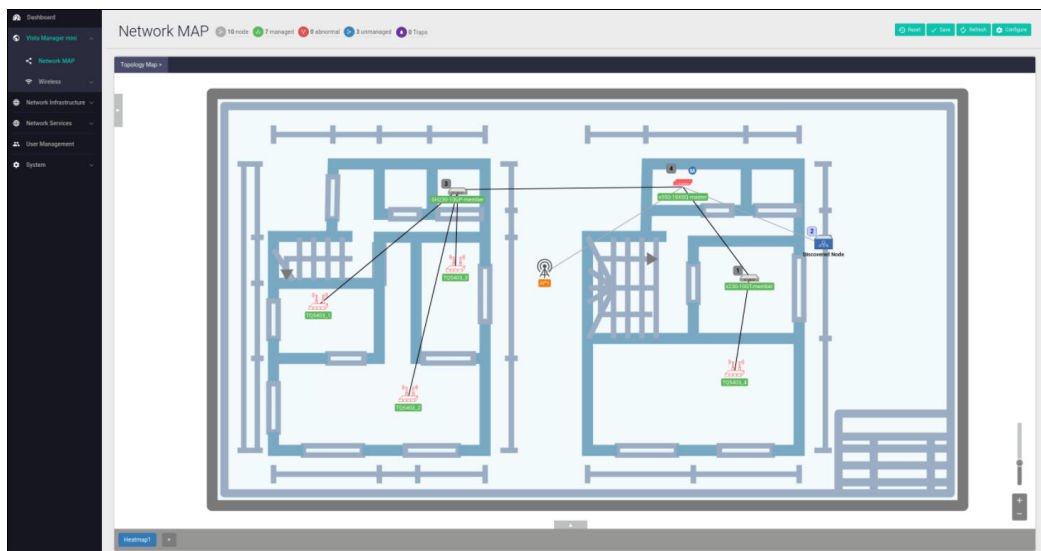
This section summarizes the new features in the Device GUI software version 2.10.0.

Read-only support on wireless for Vista mini

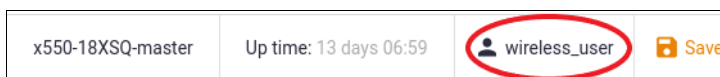
Applicable to devices running AlliedWare Plus 5.5.1-2 onwards.

From Device GUI version 2.10.0 onwards, logging in to the Device GUI with a privilege level of less than 15 gives you read-only access to device information and network maps.

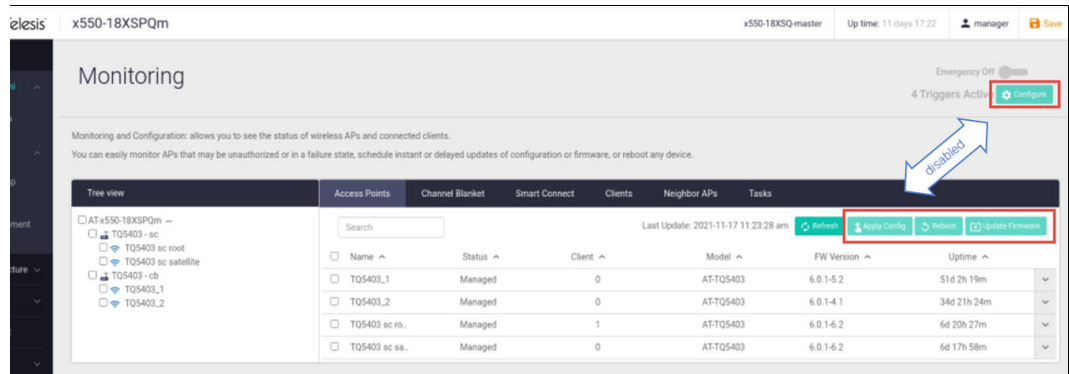
In read-only access, you can click refresh to update the device information and you can also view Network topology and Heat maps set by the Administrator:



In addition, the GUI login user-name is now displayed in the GUI's top bar:



When a read-only user is logged in, all buttons except the **Refresh** button are disabled:

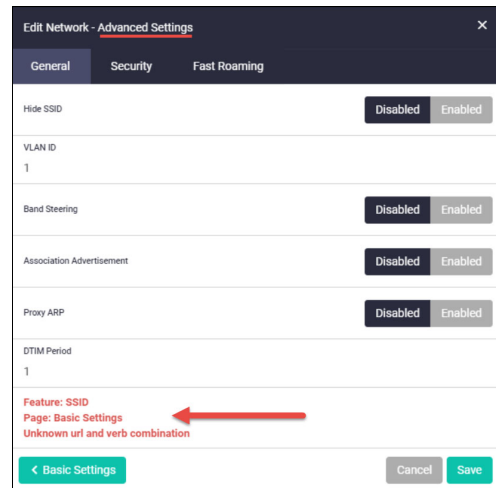
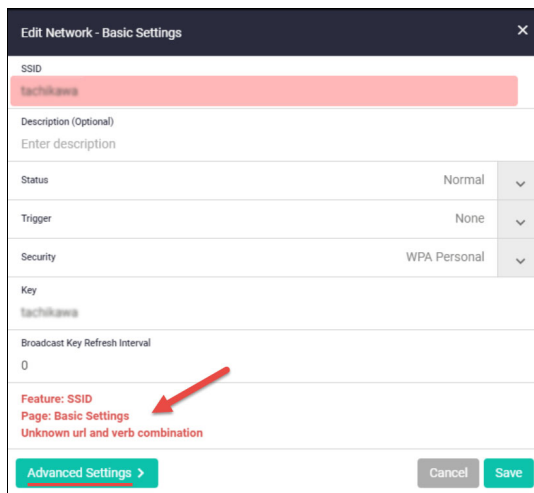


Usability improvements in Vista mini

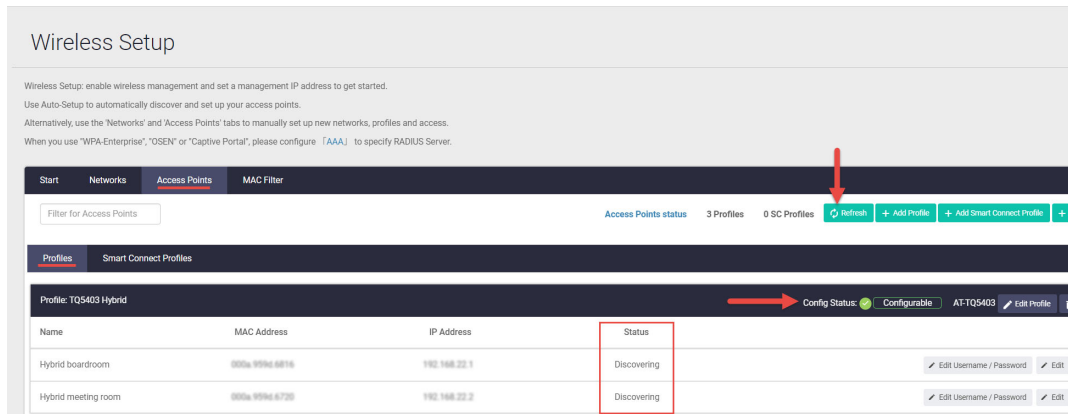
Applicable to devices running AlliedWare Plus 5.5.1-2 onwards.

Device GUI version 2.10.0 provides improvements in **Wireless Setup** error handling, configuration, validation, and monitoring. The improvements allow you to:

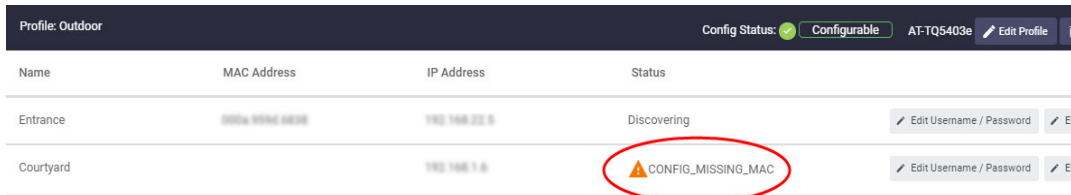
- easily identify error notifications. Error notifications are displayed using red text and remain visible even if you move to a new page - for example, moving between Basic and Advanced settings:



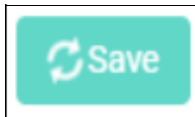
- check and refresh the **Status** of Network, AP Profile, and Access Point configurations:



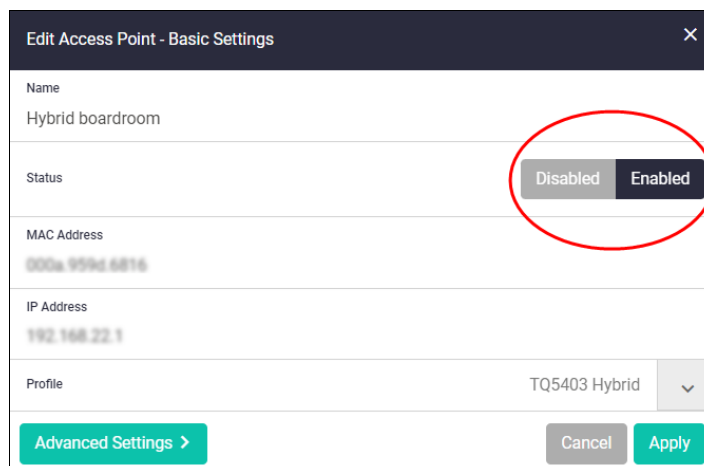
- easily identify a missing configuration - look in the **Status** column:



- confirm a configuration is being applied - when you click the **Save** button, a spinning wheel animation is displayed:



- enable or disable an Access Point configuration:



- monitor the **Status** of enabled Access Points and connected clients : **Wireless > Monitoring**

Name	Status	Client	Model
TQ-1402_1	Managed	0	AT-TQ1402
TQ-1402_2	Managed	0	AT-TQ1402
TQ-5403_1	Managed	0	AT-TQ5403
TQ-5403_2	Managed	0	AT-TQ5403
TQ-6602	CONFIG_MISSING_VAP0	0	AT-TQ6602
tachikawa_ap	CONFIG_MISSING_RADIUS	0	-

- confirm that a configuration is applied correctly to an Access Point. If an Access Point is not managed, the configuration will not be applied to the Access Point:

Apply Config

Are you sure you want to apply your configuration to the selected Access Point?

Verify whether the status of the Access Point is "Managed"

Configuration will not be applied if the Access Point is not managed.

Clients associated to the Access Point will be disconnected.

When Apply now

Submit

- To see if an Access Point is 'Managed', go to **Monitoring > Access Points**, and check the **Status** column:

Monitoring

Emergency Off ()
0 Trigger Active

Monitoring and Configuration: allows you to see the status of wireless APs and connected clients.
You can easily monitor APs that may be unauthorized or in a failure state, schedule instant or delayed updates of configuration or firmware, or reboot any device.

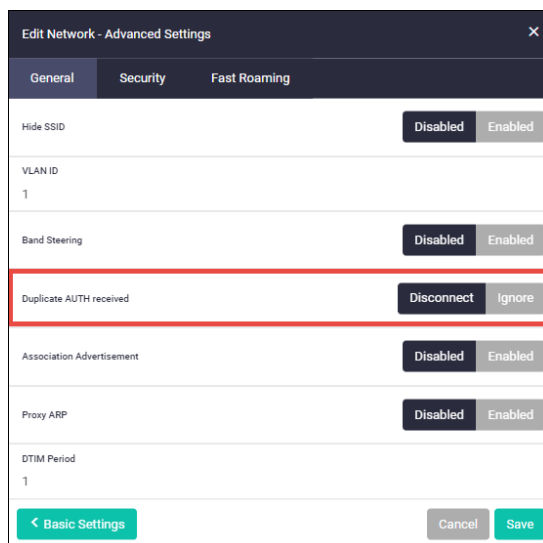
Name	Status	Client	Model	FW Version	Uptime
Hybrid board..	Discovering	0	-	-	0s
Hybrid meeti..	Discovering	0	-	-	0s
Hallway 1	Discovering	0	-	-	0s
Hallway 2	Discovering	0	-	-	0s
<input checked="" type="checkbox"/> Entrance	Discovering	0	-	-	0s

Configuring TQ access points

Applicable to devices running AlliedWare Plus 5.5.1-2 onwards.

From Device GUI version 2.10.0 onwards, for TQ access points: *TQ5403*, *TQm5403*, and *TQ5403e*, you can:

- Change the **Duplicate AUTH received** parameter in the **Network > General > Advanced Settings** tab from **Ignore** to **Disconnect**. The reason this feature is provided is that some devices may not connect again after being disconnected. To avoid this situation, you can use the **Ignore** option:

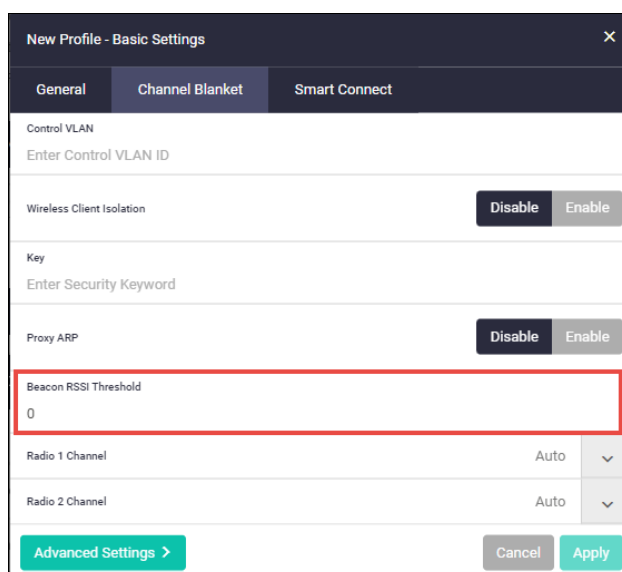


The screenshot shows the 'Edit Network - Advanced Settings' dialog box with the following settings:

- Hide SSID: Disabled
- VLAN ID: 1
- Band Steering: Disabled
- Duplicate AUTH received: Disconnect** (highlighted with a red box)
- Association Advertisement: Disabled
- Proxy ARP: Disabled
- DTIM Period: 1

Buttons at the bottom: < Basic Settings, Cancel, Save

- Set the **Beacon RSSI Threshold** value for a wireless **Channel Blanket** configuration.
 - « RSSI (Received Signal Strength Indicator) is a measurement of how well your device can hear a signal from an access point or router. It's a value that is useful for determining if you have enough signal to get a good wireless connection. The closer to 0 dBm, the better the signal is.



The screenshot shows the 'New Profile - Basic Settings' dialog box with the following settings:

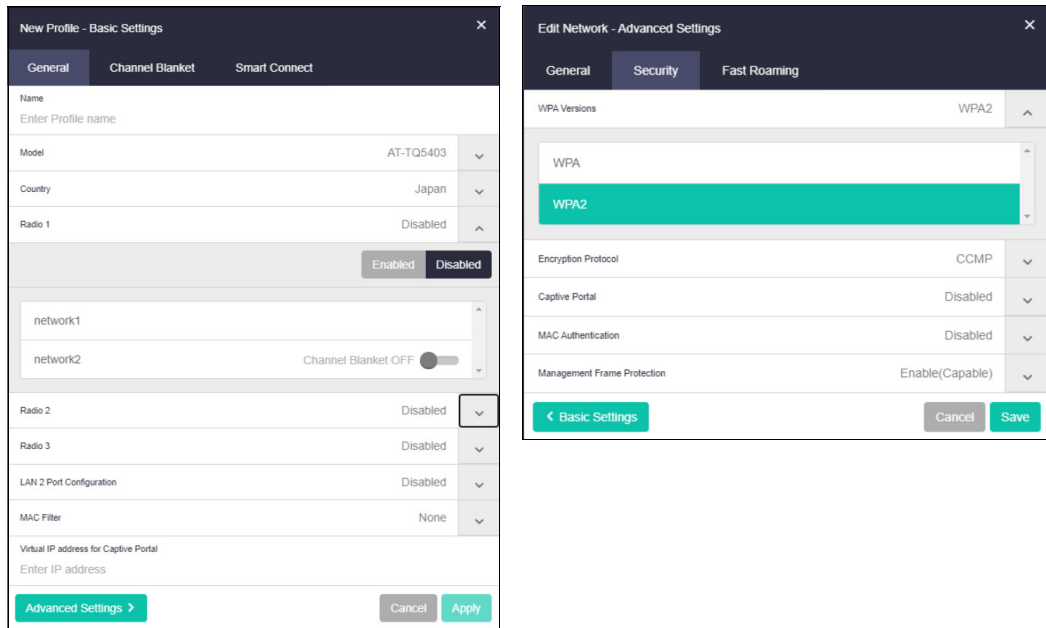
- Control VLAN: Enter Control VLAN ID
- Wireless Client Isolation: Disable
- Key: Enter Security Keyword
- Proxy ARP: Disable
- Beacon RSSI Threshold: 0** (highlighted with a red box)
- Radio 1 Channel: Auto
- Radio 2 Channel: Auto

Buttons at the bottom: Advanced Settings >, Cancel, Apply

- Previously, you could configure a combination of WPA3 and Channel Blanket even though it was not supported. This issue has been resolved.

Now, you cannot:

- set up a Channel Blanket VAP with WPA3 security type.
- change the security type to WPA3 on a Network that is set up with a Channel Blanket VAP.



Captive Portal re-authentication timer

Applicable to devices running AlliedWare Plus 5.5.1-2 onwards:

From Device GUI version 2.10.0 onwards, for TQ access points, you can limit the connection (session) and refresh time for clients on a Captive Portal session.

Go to: **Wireless > Networks > Advanced Settings > Security**

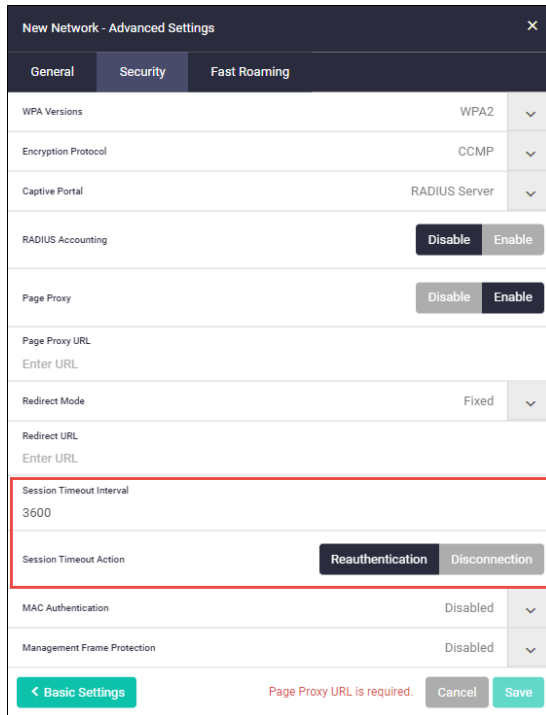
Configuring the Session Timeout Interval

When the session times-out, the client will either be presented with the authentication page or be disconnected.

The **Session Timeout Interval** value is in seconds <0-86400>. To disable the timeout function, set a value of '0' seconds.

The **Session Timeout Action** options are:

- Reauthentication - the client must re-authenticate before continuing to use the Captive Portal session.
- Disconnection - the client will be disconnected when the Captive Portal session expires. The client can decide whether or not to go through the process of re-authentication.



New Network - Advanced Settings

General | **Security** | Fast Roaming

WPA Versions: WPA2

Encryption Protocol: CCMP

Captive Portal: RADIUS Server

RADIUS Accounting:

Page Proxy:

Page Proxy URL: Enter URL

Redirect Mode: Fixed

Redirect URL: Enter URL

Session Timeout Interval: 3600

Session Timeout Action:

MAC Authentication: Disabled

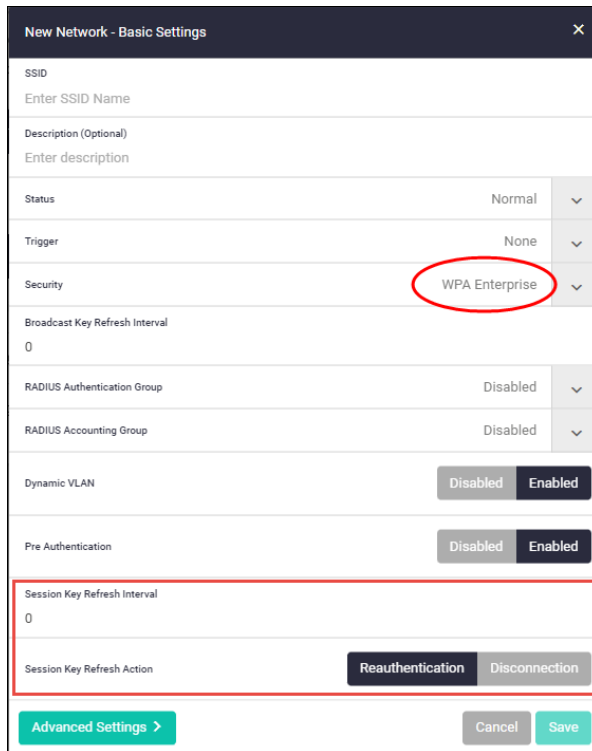
Management Frame Protection: Disabled

Page Proxy URL is required.

Configuring the Session Key Refresh Interval

The Session Key Refresh interval is only available in a WPA-enterprise security configuration.

- The **Session Key Refresh Interval** value is in seconds <0-86400>, the default value is '0' seconds.
- The **Session Key Refresh Action** options are: Reauthentication and Disconnection.



New Network - Basic Settings

SSID: Enter SSID Name

Description (Optional): Enter description

Status: Normal

Trigger: None

Security: WPA Enterprise

Broadcast Key Refresh Interval: 0

RADIUS Authentication Group: Disabled

RADIUS Accounting Group: Disabled

Dynamic VLAN:

Pre Authentication:

Session Key Refresh Interval: 0

Session Key Refresh Action:

Accessing and Updating the Web-based GUI

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

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:

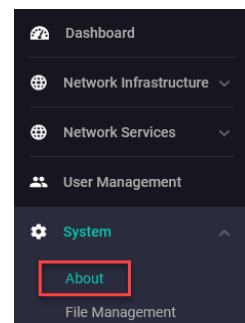
- « on switches: 169.254.42.42
- « on AR-Series: 192.168.1.1

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**. It should be 2.10.0 or later.

If you have an earlier version, 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 our Software Download center. The filename for v2.10.0 of the GUI is awplus-gui_551_25.gui.

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

2. Log into the GUI:

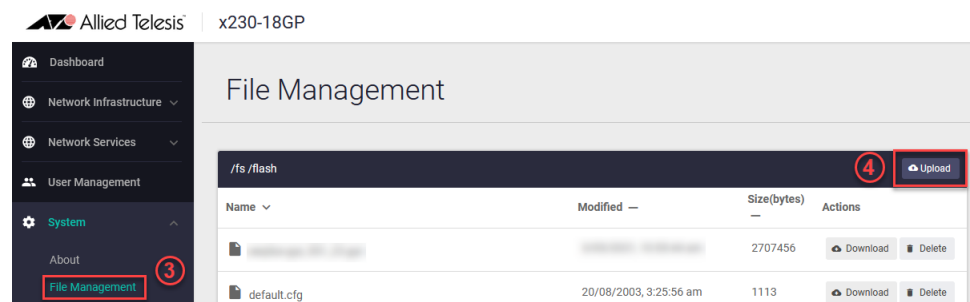
Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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 v2.10.0 or later.

