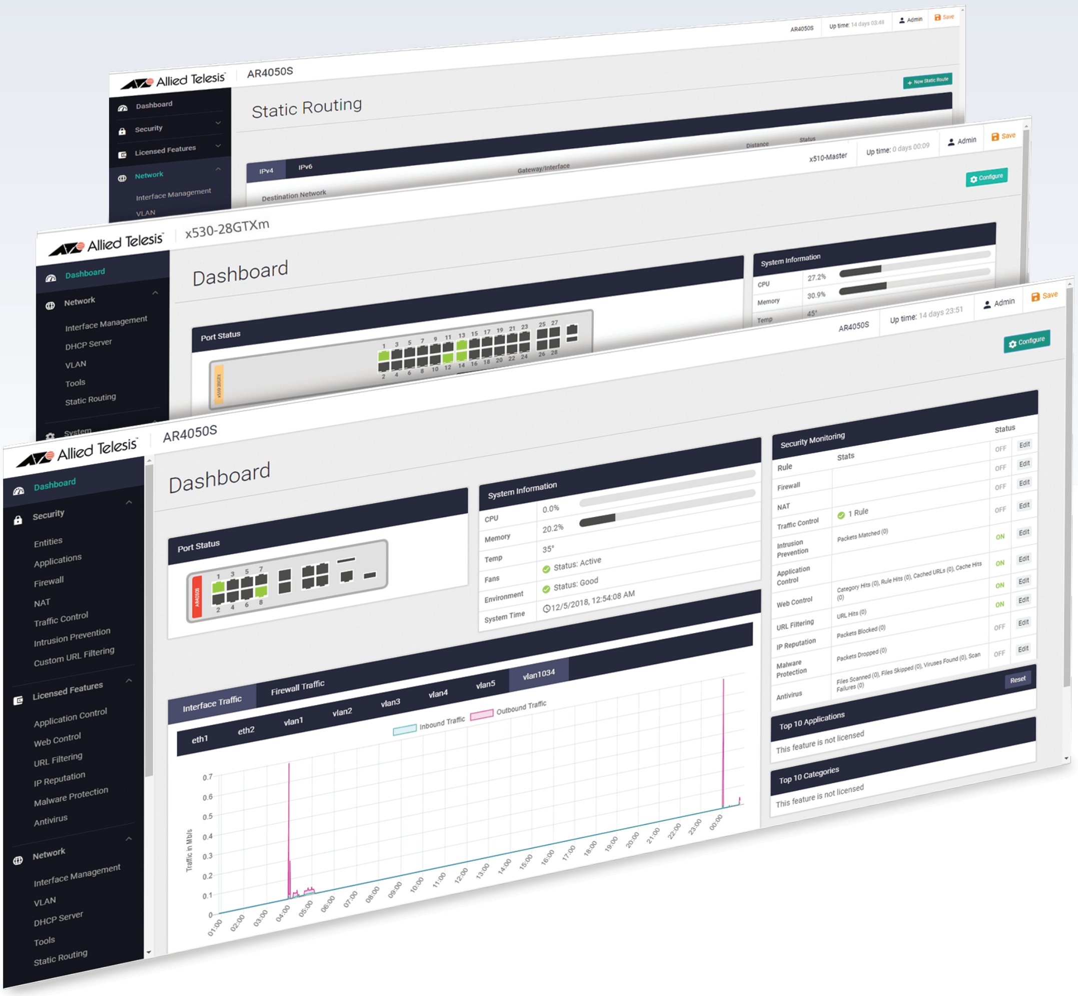
Allied Telesis™

Release Note for Web-based Device GUI Version 2.13.x



» 2.13.0

AlliedWare Plus
OPERATING SYSTEM

Acknowledgments

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 2.13.0

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 2.13.0. You can run 2.13.0 with AlliedWare Plus firmware versions 5.5.0-x.x, 5.5.1-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
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 2.13.0.

Alternative and additional security options

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

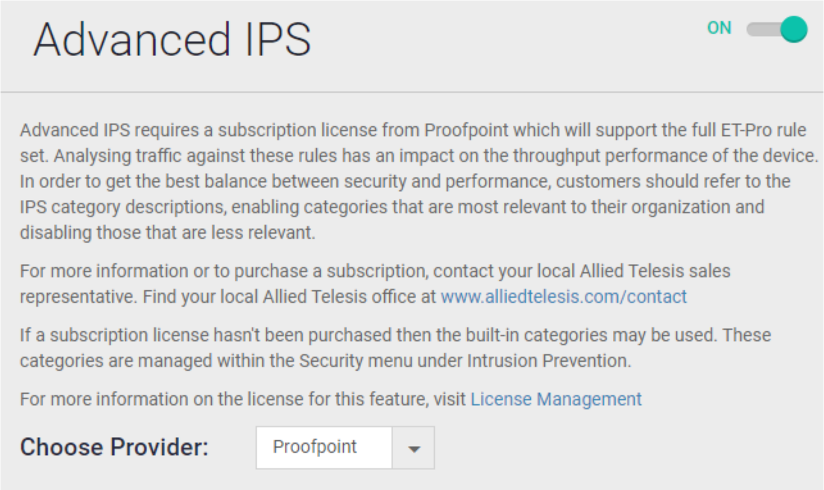
From version 5.5.2-2.1 onwards, AlliedWare Plus provides Advanced IPS (Intrusion Prevention System) functionality.

This is made possible by the addition of the third-party vendor Proofpoint's ET Pro Ruleset.

The Proofpoint ET Pro Ruleset detects and blocks advanced threats. Updated daily, it covers malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing. It also detects and blocks distributed denial-of-service attacks (DDoS), protocol and application anomalies, exploit kits and supervisory control and data acquisition (SCADA) attacks.

This feature requires a license, which is available in the bundle pack: AT-AR4-UTM-02-1/3/5YR. Contact your authorized Allied Telesis support center to obtain a license.

You can choose Proofpoint as your provider on the **Licensed Features** > **Advanced IPS** screen.



Advanced IPS

Advanced IPS requires a subscription license from Proofpoint which will support the full ET-Pro rule set. Analysing traffic against these rules has an impact on the throughput performance of the device. In order to get the best balance between security and performance, customers should refer to the IPS category descriptions, enabling categories that are most relevant to their organization and disabling those that are less relevant.

For more information or to purchase a subscription, contact your local Allied Telesis sales representative. Find your local Allied Telesis office at www.alliedtelesis.com/contact

If a subscription license hasn't been purchased then the built-in categories may be used. These categories are managed within the Security menu under Intrusion Prevention.

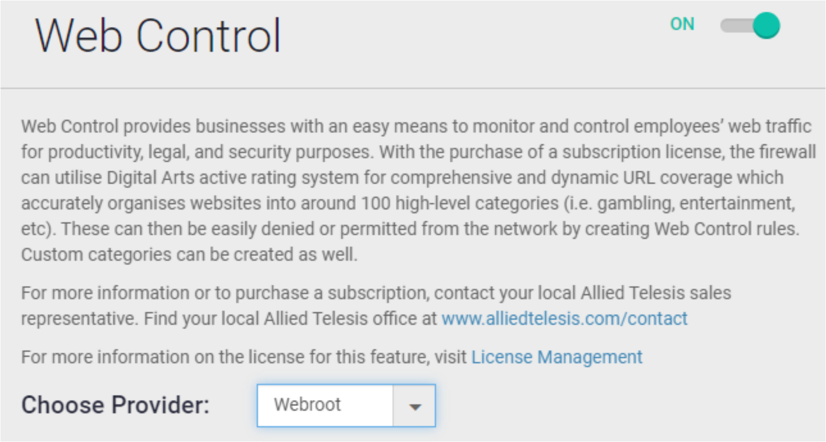
For more information on the license for this feature, visit License Management

Choose Provider: Proofpoint

Also available from version 5.5.2-2.1, support for provider Webroot has be added to Web Categorization and Web Control. Webroot delivers multi-vector protection for endpoints and networks and threat intelligence.

Additionally, an alternative solution for Kaspersky URL Filtering based on a combination of DPI Web Categorization (provider Webroot) and firewall rules has been added.

You can choose Webroot as your provider on the **Licensed Features** > **Web Control** screen.



Web Control

Web Control provides businesses with an easy means to monitor and control employees' web traffic for productivity, legal, and security purposes. With the purchase of a subscription license, the firewall can utilise Digital Arts active rating system for comprehensive and dynamic URL coverage which accurately organises websites into around 100 high-level categories (i.e. gambling, entertainment, etc). These can then be easily denied or permitted from the network by creating Web Control rules. Custom categories can be created as well.

For more information or to purchase a subscription, contact your local Allied Telesis sales representative. Find your local Allied Telesis office at www.alliedtelesis.com/contact

For more information on the license for this feature, visit License Management

Choose Provider: Webroot

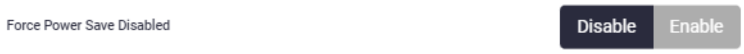
Support for existing features/capabilities via Digital Arts and Kaspersky remain.

Force Power Save Disabled setting for Channel Blanket

Applies to all AlliedWare Plus devices 5.5.2-2.1 onwards.

Some models of wireless client may unintentionally change to power saving mode, even though the connection between the AP and client is alive. To avoid this, you can enable the Force Power Save Disabled setting. This will prevent clients from changing to power saving mode.

You can enable or disable this setting on the **Vista Manager mini** > **Wireless Setup** > **Access Points tab** > **Add Profile or Edit** > **Channel Blanket tab**.



Force Power Save Disabled

This field is only displayed if one of the following models is selected for the AP profile:

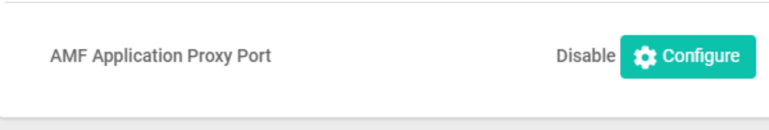
- AT-TQ6702 GEN2
- AT-TQ6602 GEN2
- AT-TQ6602
- AT-TQ5403
- AT-TQ5403e

AMF SEC configuration for Vista mini

Applies to all AlliedWare Plus devices 5.5.2-2.1 onwards.

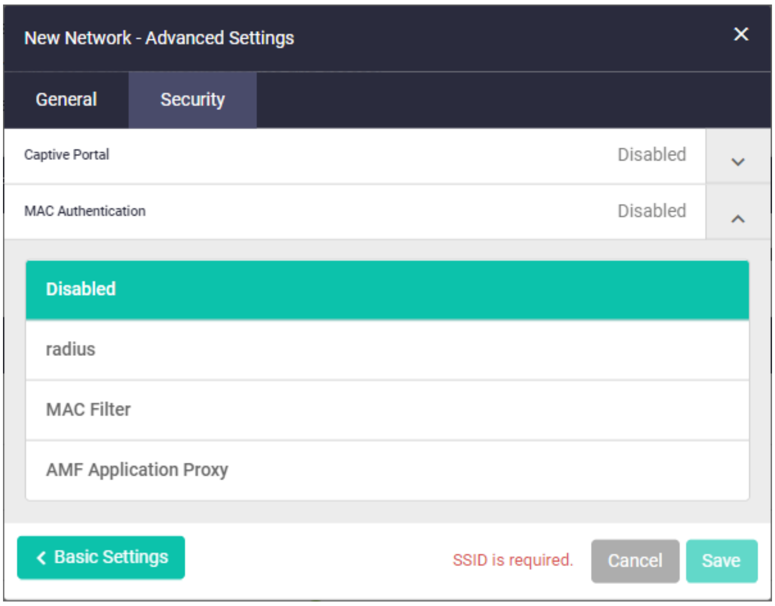
The Device GUI now lets you configure AMF application proxy settings for Vista Manager mini. This then allows you to use the AMF Application Proxy for MAC authentication.

You can enable and configure the AMF application proxy port. The setting is located on the **Vista Manager mini** > **Wireless Setup** > **Start tab**.



AMF Application Proxy Port Disable

The new authentication method is then available on the **Vista Manager mini** > **Wireless Setup** > **Networks tab** > **Add Network or Edit** > **Advanced Settings** > **Security tab**.



New Network - Advanced Settings

Captive Portal Disabled

MAC Authentication Disabled

SSID is required.

For information on how to configure and use these features, please refer to the AMF-Sec mini User Guide.

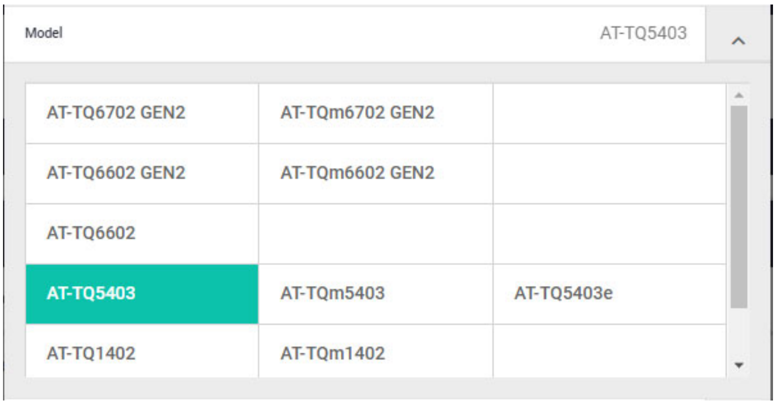
Channel Blanket support for Vista mini

Available on all devices that support Vista Manager mini for wireless control. The APs must be running firmware version 8.0.2-1.1 or later.

Two additional APs are now supported:

- AT-TQ6702 GEN2
- AT-TQ6602 GEN2

They can be configured with up to 7 channel blanket VAPs on both Radio1 and Radio2 (14 VAPs in total). All currently supported channel blanket features are also available on these APs.



Model AT-TQ5403

AT-TQ6702 GEN2	AT-TQm6702 GEN2	
AT-TQ6602 GEN2	AT-TQm6602 GEN2	
AT-TQ6602		
AT-TQ5403	AT-TQm5403	AT-TQ5403e
AT-TQ1402	AT-TQm1402	

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
```

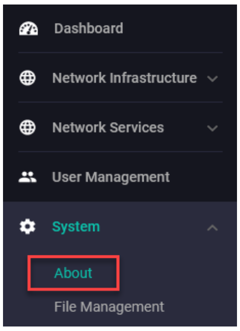
   Alternatively, on unconfigured devices you can use the default address, which is:

   - 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 2.13.0, 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 our Software Download center. The filename for v2.13.0 of the GUI is awplus-gui_552_28.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.

2. Log into the GUI:

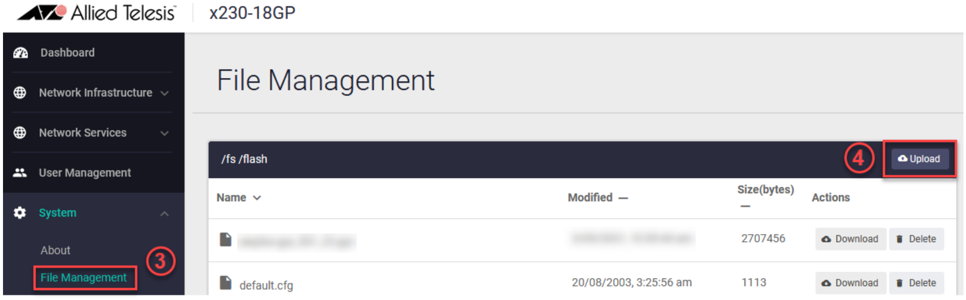
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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**.



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

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:

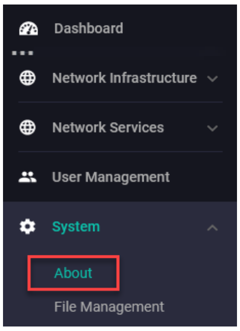
```
awplus> enable
awplus# update webgui now
```

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.


Dashboard
Network Infrastructure
Network Services
User Management
System
About
File Management