

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



» 2.14.0

Allied Ware Plus operating system

Acknowledgments

©2023 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

Introduction	4
New Features and Enhancements	7
Generate technical support data for AR4000S-Cloud	7
Enhanced IPS category tables	8
Device GUI support for 5G router firmware upgrades	9
Webroot renamed as OpenText	10
SNMP configuration improved access	11
Network map displays AMF Plus cross-links based on actual topology	12
Accessing and Updating the Web-based GUI	13



What's New in Version 2.14.0

Product families supported by this version:

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

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



Models	Family
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530D-10GHXm x530L-18GHXm x530L-18GHXm x530L-28GTX x530L-28GTX x530L-25GTX 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.)



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.

	Allied Telesis	AR-Cloud				awplus	Up time: 0 days 18:07	💄 manager	🗟 Save
@ *	Dashboard Wizard v	File Management) Reboot
a ©	Security v	/ts /lash		Size(hutes)	Jpload Generate Tech Support	Set Boo	nt Release File		
⊕ ⊕	Network Infrastructure V	Name ~	Modified — 4/3/2023, 9:00:48 AM	- 786	Actions Operations Delete	Current	: AR4000S-Cloud-0.0.0	0-202302 1.iso	Browse
**	User Management	log	4/4/2023, 3:02:00 AM	68240	Davidant E Dalata	Set Boo	ot Config File : flash:/default.cfg	6	Browse
*	About	tech-support.txt.gz	4/4/2023, 3:03:53 AM	87783	Download Delete	Backup	: Not Set		Browse
	File Management License Management Services Time					Flash U	sage	512.0K	/ 3.9G
	Logging CLI 🖸								

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).

-	Allied Tele	zsis	AR4050S		S3-Master Up time: 0 days 00:53	2 manager	Save
a	Dashboard		Advanced IDS System Cate	2007/			
*	Wizard		Category	Action	Description	Rule Co	unt
8	Vista Manager mini		3coresec	Log Block Ignore	IP block list signatures automatically generated from the 3CORESec team's H	29	_
ô	Security			Log Diotek ignore			
C			activex	Log Block Ignore	Signatures for protection against attacks on Microsoft ActiveX controls and e	241	
<			attack_response	Log Block Ignore	Signatures to identify responses indicative of intrusion. Examples include but .	. 582	2
	Web Control URL Filtering		botcc	Log Block Ignore	(Bot Command and Control) Signatures that are autogenerated from several s.	. 24	
			chat	Log Block Ignore	Signatures that identify traffic related to numerous chat clients such as Intern	73	
	Malware Protection Advanced IPS		ciarmy	Log Block Ignore	Signatures generated using Collective Intelligence's IP rules for blocking. For	99	
	Antivirus			Long Block James	Mains annully simply and any local in some no to entire and short lived area	0500	
-	Natwork Infractructure	•	current_events_major	Log Block Ignore	major severity signatures developed in response to active and short-lived cam.	. 9590	

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:
                                    35657/39383
 Usage:
  Alert:
                                    35657
                                    õ
  Denv:
                                    3726
 Disable:
   Category (* = invalid) Action Rules Description
                                                                                                                     _____
                                                                      Signatures for protection against
attacks on Microsoft ActiveX controls
and exploits targeting vulnerabilities
   activex
                                            disable 242
                                                                          in ActiveX controls
                                                                      Signatures to identify responses
indicative of intrusion. Examples
include but not limited to LMHost file
   attack-response
                                            alert 583
                                                                         download, presence of web banners and
the detection of Metasploit
Meterpreter kill command. These are
                                                                          designed to catch the results of a
                                                                          successful attack
                                                          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
disactors
   current-events-major
                                            alert
                                                                          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:

Firmware S	lots			
Slot ID	Status	Build ID	State	+ Add Firmware/Carrier
1	Good	03.04.03.00_?	Usable	Delete
2	Good	03.09.06.00_?	Active 🧭	

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**:

Firmware S	Slots			
Slot ID	Status	Build ID	State	+ Add Firmware/Carrier
1	Good	03.04.03.00_?	Active 🤡	
2	Empty			Telete
3	Empty			Telete

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





Allied Telesis	AR4050S-5G				AR4050S	Up time: 0 days 04:04	🛓 manager 🛛 🔒 Save
Dashboard Wizard	File Management						Reboot
Vista Manager mini V	/fø/flash		(inc/butes)	🛆 Upload	Set Boot Release File	í.	
Licensed Features	Name ~	Modified — 2/23/2023, 6:32:55 PM	=	Actions	Current: flash:/A Backup: flash:/A	R4050S-main-20230331-1.rel	Browse
Network Services	 03.09.03.00 5gver2 	2/23/2023, 6:23:11 PM 2/20/2023, 9:11:55 AM			Set Boot Config File	r me nocioana)	L Browse
User Management System	5gver2_test	3/3/2023, 1:56:30 PM			Current: flash:/d	efault.cfg	Browse
About File Management License Management	Sgver3	2/20/2023, 9:12:20 AM 11/1/2022, 9:42:54 AM	1426	🚯 Download 🔋 Delete	Flash Usage		Drowse
Services	AR40503-5.5.2-1.1.rel	2/16/2023, 3:36:33 PM	53293943	🚯 Download 🧃 Delete	21%		768.7M / 3.5G
Logging	AR4050S-5.5.2-2.1.rel	2/16/2023, 3:36:14 PM	53412151	🚯 Download 🔋 Delete			

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.

	🚺 Allied Telesis	S	x230-18GP				
a	Dashboard						
⊕	Network Infrastructure $$		File Management				
⊕	Network Services 🗸 🗸						
*	User Management		/fs /flash		oles (hutes)	(4)	Upload
٠			Name V	Modified —	–	Actions	
	About 3				2707456	Download	Delete
	File Management		efault.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

 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.

