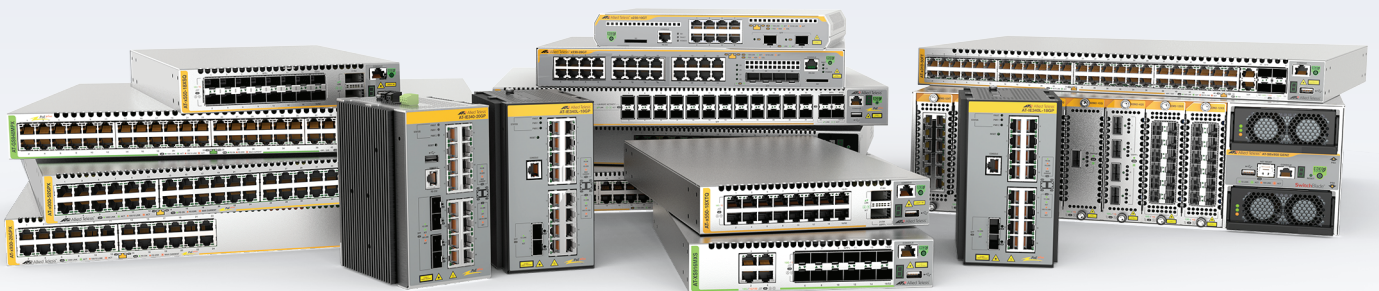


# Release Note for AlliedWare Plus Software Version 5.5.4-2.x



## AlliedWare Plus OPERATING SYSTEM

AMF Cloud  
SBx81CFC960  
SBx908 GEN2  
x950 Series  
x930 Series  
x550 Series  
x540L Series  
x530 Series  
x530L Series  
x330 Series

x320 Series  
x250 Series  
x240 Series  
x230 Series  
x220 Series  
IE360 Series  
IE340 Series  
IE220 Series  
IE210L Series

SE540L Series  
SE250 Series  
SE240 Series  
XS900MX Series  
GS980MX Series  
GS980EM Series  
GS980M Series  
GS970EMX Series  
GS970M Series

ARX200S-GTX  
AR4000S-Cloud  
10GbE UTM Firewall  
AR4050S-5G  
AR4050S  
AR3050S  
ARI050V  
TQ6702 GEN2-R

» 5.5.4-2.3 » 5.5.4-2.4 » 5.5.4-2.5

## Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.

Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California.

All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see [www.openssl.org/](http://www.openssl.org/)

Copyright (c) 1998-2019 The OpenSSL Project

Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson

All rights reserved.

This product includes software licensed under the GNU General Public License available from: [www.gnu.org/licenses/gpl2.html](http://www.gnu.org/licenses/gpl2.html)

Source code for all GPL licensed software in this product can be obtained from the Allied Telesis GPL Code Download Center at: [www.alliedtelesis.com/support/gpl-code](http://www.alliedtelesis.com/support/gpl-code)

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by emailing [gpl@alliedtelesis.co.nz](mailto:gpl@alliedtelesis.co.nz).

©2025 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. 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/](http://www.adobe.com/)

---

# Content

<b>What's New in Version 5.5.4-2.5 .....</b>	<b>1</b>
<b>Introduction.....</b>	<b>1</b>
<b>Enhancements .....</b>	<b>5</b>
<b>Issues Resolved in Version 5.5.4-2.5.....</b>	<b>7</b>
<b>What's New in Version 5.5.4-2.4 .....</b>	<b>21</b>
<b>Introduction.....</b>	<b>21</b>
<b>Issues Resolved in Version 5.5.4-2.4.....</b>	<b>25</b>
<b>What's New in Version 5.5.4-2.3 .....</b>	<b>33</b>
<b>Introduction.....</b>	<b>33</b>
<b>New Features and Enhancements .....</b>	<b>37</b>
<b>Important Considerations Before Upgrading.....</b>	<b>52</b>
<b>Obtaining User Documentation.....</b>	<b>59</b>
<b>Verifying the Release File .....</b>	<b>59</b>
<b>Licensing this Version on an SBx908 GEN2 Switch.....</b>	<b>61</b>
<b>Licensing this Version on an SBx8100 Series CFC960 Control Card .....</b>	<b>63</b>
<b>Installing this Software Version.....</b>	<b>65</b>
<b>Accessing and Updating the Web-based GUI .....</b>	<b>67</b>

# What's New in Version 5.5.4-2.5

Product families supported by this version:

AMF Cloud	SE540L Series <sup>1</sup>
SwitchBlade x8100: SBx81CFC960	SE250 Series <sup>1</sup>
SwitchBlade x908 Generation 2	SE240 Series <sup>1</sup>
x950 Series	XS900MX Series
x930 Series	GS980MX Series
x550 Series	GS980EM Series
x540L Series	GS980M Series
x530 Series	GS970EMX Series
x530L Series	GS970M Series
x330 Series	10GbE UTM Firewall
x320 Series	ARX200S-GTX
x250 Series <sup>1</sup>	AR4000S-Cloud
x240 Series	AR4050S
x230 Series	AR4050S-5G
x220 Series	AR3050S
IE360 Series	AR1050V
IE340 Series	TQ6702 GEN2-R
IE220 Series	
IE210L Series	

1. Not available in all regions

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-2.5.

Software file details for this version are listed in [Table 1](#) on the next page. You can obtain the software files from the [Allied Telesis Support Portal](#). Log in using your assigned email address and password.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 65](#).

For instructions on how to update the web-based GUI, see [“Accessing and Updating the Web-based GUI” on page 67](#). The GUI offers easy visual monitoring and configuration of your device.

## New licensing system: Feature String Licenses (FSL)

With this software update, a new licensing system has been introduced to replace existing subscription licenses. The new **Feature String Licenses (FSL)** work in the same way as existing licenses but provide enhanced security through encryption and digital signatures.

Existing license management commands, such as **license update file** and **show license external**, continue to operate identically for FSL licenses as they did for existing subscription licenses.

Starting from AlliedWare Plus version **5.5.4-2.5**, the system supports both existing subscription licenses and FSL licenses. Existing subscription licenses will continue to be supported, but all customers will need to migrate to the new FSL system before support ends.

Please contact your local sales office for more information.



**Caution:** Using a software version file for the wrong device may cause unpredictable results, including disruption to the network.

Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

The following table lists model names and software files for this version. Note that some models are not available in all regions.

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		09/2025	vaa-5.5.4-2.5.iso (VAA OS) vaa-5.5.4-2.5.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-2.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	09/2025	SBx81CFC960-5.5.4-2.5.rel
SBx908 GEN2	SBx908 GEN2	09/2025	SBx908NG-5.5.4-2.5.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	09/2025	x950-5.5.4-2.5.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	09/2025	x930-5.5.4-2.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	09/2025	x550-5.5.4-2.5.rel

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

Models	Family	Date	Software File
x540L-28XTm x540L-28XS	x540L	09/2025	x540-5.5.4-2.5.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	09/2025	x530-5.5.4-2.5.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	09/2025	x530-5.5.4-2.5.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	09/2025	x330-5.5.4-2.5.rel
x320-10GH x320-11GPT	x320	09/2025	x320-5.5.4-2.5.rel
x250-18XS x250-28XS x250-28XTm	x250	09/2025	x250-5.5.4-2.5.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	09/2025	x240-5.5.4-2.5.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	09/2025	x230-5.5.4-2.5.rel
x220-28GS x220-52GT x220-52GP	x220	09/2025	x220-5.5.4-2.5.rel
IE360-12GTX IE360-12GHX	IE360	09/2025	IE360-5.5.4-2.5.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	09/2025	IE340-5.5.4-2.5.rel
IE220-6GHX IE220-10GHX	IE220	09/2025	IE220-5.5.4-2.5.rel
IE210L-10GP IE210L-18GP	IE210L	09/2025	IE210-5.5.4-2.5.rel
SE540L-28XTm SE540L-28XS	SE540L	09/2025	SE540-5.5.4-2.5.rel
SE250-18XTm SE250-28XTm SE250-28XS	SE250	09/2025	SE250-5.5.4-2.5.rel
SE240-10GTXm SE240-10GHXm	SE240	09/2025	SE240-5.5.4-2.5.rel
XS916MXT XS916MXS	XS900MX	09/2025	XS900-5.5.4-2.5.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	09/2025	GS980MX-5.5.4-2.5.rel
GS980EM/10H GS980EM/11PT	GS980EM	09/2025	GS980EM-5.5.4-2.5.rel
GS980M/52 GS980M/52PS	GS980M	09/2025	GS980M-5.5.4-2.5.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	09/2025	GS970EMX-5.5.4-2.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	09/2025	GS970-5.5.4-2.5.rel
AR4000S-Cloud		09/2025	AR-4000S-Cloud-5.5.4-2.5.iso
ARX200S-GTX	AR-Series VPN Router	09/2025	ARX200S-5.5.4-2.5.rel
10GbE UTM Firewall		09/2025	ATVSTAPL-1.9.4.iso and vfw-x86_64-5.5.4-2.5.app.
AR4050S AR4050S-5G AR3050S	AR-Series UTM Firewalls	09/2025	AR4050S-5.5.4-2.5.rel AR3050S-5.5.4-2.5.rel
AR1050V	AR-Series VPN Router	09/2025	AR1050V-5.5.4-2.5.rel
TQ6702 GEN2-R	Wireless AP Router	09/2025	TQ6702GEN2R-5.5.4-2.5.rel
TQ7403R	Wireless AP Router	09/2025	TQ7403R-5.5.4-2.5.rel

## ISSU (In-Service Software Upgrade) on SBx8100 with CFC960

The 5.5.4-2.5 software version is ISSU compatible with previous software versions.

## Enhancements

This section summarizes the enhancements in AlliedWare Plus version 5.5.4-2.5.

### **ER-6863** *Applies to all AlliedWare Plus devices*

With this software update, OpenSSH version has been upgraded to 9.9p2.

ISSU: Effective when ISSU completed.

### **ER-6918** *Applies to all AlliedWare Plus devices using AMF*

AMF now uses a different type of SSH key for internal operations. Devices running releases **earlier** than version 5.4.5 will no longer be able to:

- Use the **atmf remote-login NODE** command to connect to a device running the new software.
- Use the following commands in a single node working-set (atmf working-set NODE) to a device running the new software:
  - « atmf recover
  - « atmf cleanup
  - « banner login
  - « boot system
  - « boot config
  - « copy
  - « delete
  - « edit
  - « erase factory-default
  - « issu boot
  - « mail
  - « move
  - « mtrace
  - « ping
  - « remote-login (VCS)
  - « start-shell
  - « terminal monitor
  - « test cable-diagnostics tdr interface
  - « traceroute

ISSU: Effective when CFCs upgraded.

**ER-6983** *Applies to all devices running AlliedWare Plus*

With this software update it is now possible to use secondary addresses while the primary address is a DHCP assigned address. For example, you can now configure:

```
awplus(config)# interface eth1
awplus(config-if)# ip address dhcp
awplus(config-if)# ip address 192.168.100.2/24 secondary
```

ISSU: Effective when CFCs upgraded.

**ER-7198** *Applies to all AlliedWare Plus devices, except for AMF Cloud*

Previously, when an interface running a DHCPv6 client in Prefix Delegation mode was shut down and brought back up, the client was incorrectly reinitialized in NDP mode. This issue has now been resolved.

ISSU: Effective when CFCs upgraded.



CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud (VAA)	TQ-R Series				
CR-86716	API	Previously, when the system was very busy, API requests could fail to receive responses, resulting in health check failures. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
CR-86056	API	Previously, the API for monitoring Layer 3 switch ports was not working. This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
CR-86284	API	Previously, Layer 3 switch ports were missing from the switchport API. This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
CR-86648	API	Previously it was possible for file uploads via the HTTP API to sporadically fail mid transfer. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
CR-87093	API, CLI, Update Manager	Previously, using the <b>update resource</b> command on a resource that did not exist, could cause a memory leak. This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
CR-85579	AWC-Lite	Previously, the Top Level Domain (TLD) of Fully Qualified Domain Names (FQDN) did not allow numeric and hyphen characters for Passpoint configurations. This has now been resolved and the following fields now allow setting the TLD of FQDN to numeric and hyphen characters: Passpoint -> IEEE 802.11u -> Domain Name Passpoint -> IEEE 802.11u -> NAI Realm information.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	—	Y	Y	Y	—	Y	Y	Y	Y	Y	Y	—	—	—	—





CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud (VAA)	TQ-R Series				
CR-86425	DHCP Server, DHCP Relay	Previously, a DHCP server could respond to DHCP Request or Inform messages even if it wasn't the authoritative server for the client. This remains the default behavior, but it can now be disabled using the command <b>no ip dhcp globally-authoritative</b> .  Also, if the device acts as both a DHCP server and a relay agent, it won't respond unless it has a DHCP pool configured for the subnet where the request originated.  This issue has been resolved.  ISSU: Effective when CFCs upgraded.	Y	—	—	Y	Y	Y	Y	Y	Y	—	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
CR-87004	DPI	Previously, a system reboot could occur when disabling detailed DPI counters.  This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
CR-82714	DPI, SD WAN	Previously, an ICMP ping probe could fail when DPI Application Sharing was enabled.  This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y
CR-86694	IDS/IPS	Previously, on rare occasions, when enabling IPS protection after a reboot, IPS would remain in the loading state.  This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y
CR-87088	IGMP	Previously, if IGMP snooping was turned off on a VLAN that had a manually configured multicast router port (static mrouter port), a system reboot could occur.  This issue has been resolved.  ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y







CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud (VAA)	TQ-R Series			
CR-86427	PIM-SM	Previously, removing VLANs from upstream or downstream ports could cause PIMd to access invalid memory, resulting in a system reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	—	Y	—	—	Y	Y	—	—	Y	—	Y	—	—	—	—	—	—	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—	—		
CR-87661	PoE	Previously, when the <b>no switchport</b> command (valid from 5.5.5-1) was saved to the startup configuration for a PoE capable port, and the device rebooted, the port would not supply PoE power. This issue has been resolved.	Y	—	—	Y	Y	Y	Y	Y	Y	—	Y	—	—	Y	Y	Y	—	Y	Y	Y	—	Y	Y	—	—	—	—	—	—	—	—	—	—	—	
CR-76202	Port Authentication	Previously, an untagged VLAN would not be dynamically assigned by the RADIUS server when a supplicant was on a trunk port. This issue has been resolved.	Y	—	—	Y	Y	Y	Y	Y	Y	—	—	—	Y	Y	Y	—	—	Y	Y	Y	—	—	Y	—	—	—	—	—	—	—	—	—	—	—	
CR-86567	Port Authentication	Previously, on affected stacked platforms with port authentication configured, it was possible for switch lockup to occur if many supplicants joined in a short period of time. This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	—	Y	—	—	—	—	—	—	—	—
CR-86667	Port Authentication	Previously, when Auth Forwarding rules were added or removed on the ARX200, it could take up to 30 seconds before the changes took effect. This has been resolved and rule changes take effect immediately.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	—	—	—	—	—	—

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud (VAA)	TQ-R Series					
CR-85997	Port Authentication, LACP, Static Aggregators	Previously, port authentication was denied on aggregators on all platforms. This has been corrected to only deny it on platforms where it is unsupported.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
CR-86448	Port Authentication, VLANs	Previously, the default MTU was being set to an incorrect value on VLANs. This issue has been resolved.																												Y									
CR-87120	Port Authentication	Previously, if a VLAN was assigned dynamically using MAC authentication, and the original native VLAN lost all its member ports and shut down, it would cause a VCS timeout and freeze the console. This issue has been resolved. ISSU: Effective when CFCs upgraded.					Y																Y				Y												
CR-85305	Port Configuration	Previously, a SPTXc pluggable may have occasionally failed to initialise properly. This issue has been resolved.	Y	Y	Y					Y	Y						Y			Y	Y			Y	Y	Y		Y											
CR-85722	Port Configuration	Previously, on the x250-18XTm platform, some debug level log messages were generated when a multi-gig port linked up at 5G. This issue has been resolved.																		Y																			
CR-86434	QoS, QSP	Previously, in very rare cases, a QSP action could be mistakenly triggered due to a random error in a hardware counter. A fix has been added to detect and ignore these false errors, and log the event in a trace message. This issue has been resolved.																									Y		Y										

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud (VAA)	TQ-R Series					
CR-85793	Security	This software update addresses the following SECURITY vulnerabilities stated in: CVE-2024-12084 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087 CVE-2024-12088 CVE-2024-12747	—	Y	Y	—	Y	—	—	—	—	—	—	—	—	Y	—	—	Y	Y	—	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
CR-86813	Security	This software update addresses the security vulnerabilities stated in CVE-2025-32728. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
CR-86559	SMTP, 2FA	Previously, the sender's information ("From:" header field) was missing in emails generated from routers for 2FA email one-time password. This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	
CR-86197	Software Licensing	The <b>license update online</b> command has been removed as this functionality is no longer available.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
CR-85760	SSH	Previously, if a space was accidentally appended to a legitimate username when logging in via SSH, this could result in the legitimate user being deleted from the user database preventing subsequent logins using the affected username. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-86049	SSH	This software update addresses SSH vulnerabilities stated in: CVE-2025-26465.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud (VAA)	TQ-R Series			
CR-85665	STOAT	Previously, a memory leak could occur in STOAT when <b>stoat discovery dot1x</b> was configured.  This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
CR-86964	STOAT	Previously, the link speed for interfaces was incorrectly saved in the STOAT database using megabits per second (Mbps) instead of kilobits per second (Kbps).  This issue has been resolved.  ISSU: Effective when CFCs upgraded.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	—	—	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—	Y	
CR-86975	Switching	Previously, some platforms could send packets through copper ports with an inter-packet gap (IPG) smaller than 8 bytes, which could cause the receiving device to drop those packets.  This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	—	—	Y	Y	—	—	—	Y	—	—	—	—	—	—	—	—	—	—	—	—	—	—
CR-86889	System	Previously, in rare cases a system in a busy network could develop memory fragmentation that causes it to run out of available memory, resulting in the device rebooting.  This issue has been resolved.  Memory compaction has been enabled to prevent this issue from occurring.  ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—	Y
CR-87470	Traffic Control	Previously, when a traffic-control rule was applied to an entity with a sub-interface, after a reboot the traffic-control rule would no longer be applied to the sub-interface.  This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	—	—	Y

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud (VAA)	TQ-R Series		
CR-85933	VCStack	Previously, in a VCS stack with routing protocols like OSPF, OSPFv3, RIP, RIPng, or ISIS configured, and switchport interface descriptions set, a VCS failover could cause outdated interface descriptions to remain alongside updated ones in the running configuration after changes were made.  This issue has been resolved.  ISSU: Effective when CFCs upgraded.	—	Y	Y	—	Y	—	—	—	—	—	Y	—	Y	—	—	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—	—	—	—	—	—	—	
CR-87598	VCStack	Previously, under a specific rare condition where a stack member was repeatedly rebooting, it was possible for the VCStack master to undergo an unexpected reboot.  This issue has been resolved.	—	—	Y	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y	Y	Y	—	Y	—	—	—	—	—	—	—	—
CR-85495	Wireless Radio	Previously, the TQ6702 GEN2-R could take a long time to apply the configuration if many VAPs were enabled, and could prevent the TQ-R from being managed by the AWC-Plugin.  This issue has been resolved.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y
CR-87330	Wireless Radio	Previously, the 'Radar detection' field in the output of <b>show wireless ap detail</b> displayed as 'None'.  It has now been updated to show the number of radar detection events, along with additional details such as 'DFS state', 'Channel', 'Since', and 'Detected'.	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	Y

# What's New in Version 5.5.4-2.4

Product families supported by this version:

AMF Cloud	SE540L Series <sup>1</sup>
SwitchBlade x8100: SBx81CFC960	SE250 Series <sup>1</sup>
SwitchBlade x908 Generation 2	SE240 Series <sup>1</sup>
x950 Series	XS900MX Series
x930 Series	GS980MX Series
x550 Series	GS980EM Series
x540L Series	GS980M Series
x530 Series	GS970EMX Series
x530L Series	GS970M Series
x330 Series	10GbE UTM Firewall
x320 Series	ARX200S-GTX
x250 Series <sup>1</sup>	AR4000S-Cloud
x240 Series	AR4050S
x230 Series	AR4050S-5G
x220 Series	AR3050S
IE360 Series	AR1050V
IE340 Series	TQ6702 GEN2-R
IE220 Series	
IE210L Series	

1. Not available in all regions

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-2.4.

Software file details for this version are listed in [Table 1](#) on the next page. You can obtain the software files from the [Allied Telesis Support Portal](#). Log in using your assigned email address and password.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 65](#).

For instructions on how to update the web-based GUI, see [“Accessing and Updating the Web-based GUI” on page 67](#). The GUI offers easy visual monitoring and configuration of your device.



**Caution:** Using a software version file for the wrong device may cause unpredictable results, including disruption to the network.

Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

The following table lists model names and software files for this version. Note that some models are not available in all regions.

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		04/2025	vaa-5.5.4-2.4.iso (VAA OS) vaa-5.5.4-2.4.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-2.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	04/2025	SBx81CFC960-5.5.4-2.4.rel
SBx908 GEN2	SBx908 GEN2	04/2025	SBx908NG-5.5.4-2.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	04/2025	x950-5.5.4-2.4.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	04/2025	x930-5.5.4-2.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2025	x550-5.5.4-2.4.rel
x540L-28XTm x540L-28XS	x540L	04/2025	x540-5.5.4-2.4.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	04/2025	x530-5.5.4-2.4.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	04/2025	x530-5.5.4-2.4.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	04/2025	x330-5.5.4-2.4.rel
x320-10GH x320-11GPT	x320	04/2025	x320-5.5.4-2.4.rel

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

Models	Family	Date	Software File
x250-18XS x250-28XS x250-28XTm	x250	04/2025	x250-5.5.4-2.4.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	04/2025	x240-5.5.4-2.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2025	x230-5.5.4-2.4.rel
x220-28GS x220-52GT x220-52GP	x220	04/2025	x220-5.5.4-2.4.rel
IE360-12GTX IE360-12GHX	IE360	04/2025	IE360-5.5.4-2.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	04/2025	IE340-5.5.4-2.4.rel
IE220-6GHX IE220-10GHX	IE220	04/2025	IE220-5.5.4-2.4.rel
IE210L-10GP IE210L-18GP	IE210L	04/2025	IE210-5.5.4-2.4.rel
SE540L-28XTm SE540L-28XS	SE540L	04/2025	SE540-5.5.4-2.4.rel
SE250-18XTm SE250-28XTm SE250-28XS	SE250	04/2025	SE250-5.5.4-2.4.rel
SE240-10GTXm SE240-10GHXm	SE240	04/2025	SE240-5.5.4-2.4.rel
XS916MXT XS916MXS	XS900MX	04/2025	XS900-5.5.4-2.4.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	04/2025	GS980MX-5.5.4-2.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	04/2025	GS980EM-5.5.4-2.4.rel
GS980M/52 GS980M/52PS	GS980M	04/2025	GS980M-5.5.4-2.4.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	04/2025	GS970EMX-5.5.4-2.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2025	GS970-5.5.4-2.4.rel
AR4000S-Cloud		04/2025	AR-4000S-Cloud-5.5.4-2.4.iso

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

Models	Family	Date	Software File
ARX200S-GTX	AR-Series VPN Router		ARX200S-5.5.4-2.4.rel
10GbE UTM Firewall		04/2025	ATVSTAPL-1.9.4.iso and vfw-x86_64-5.5.4-2.3.app.
AR4050S AR4050S-5G AR3050S	AR-Series UTM Firewalls	04/2025	AR4050S-5.5.4-2.4.rel AR3050S-5.5.4-2.4.rel
AR1050V	AR-Series VPN Router	04/2025	AR1050V-5.5.4-2.4.rel
TQ6702 GEN2-R	Wireless AP Router	04/2025	TQ6702GEN2R-5.5.4-2.4.rel
TQ7403R	Wireless AP Router	04/2025	TQ7403R-5.5.4-2.4.rel

## ISSU (In-Service Software Upgrade) on SBx8100 with CFC960

The 5.5.4-2.4 software version is ISSU compatible with previous software versions.

# Issues Resolved in Version 5.5.4-2.4

This AlliedWare Plus maintenance version includes the following resolved issues ordered by feature:

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series		
CR-85993	AMF	Previously, on the ARX200, if an interface connected to an AMF guestnode was configured with a description, this could result in the guest node displaying an incorrect name in the <b>show atmf guests</b> and <b>show atmf guests detail</b> output. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-84412	CLI	Previously, under rare circumstances, it was possible for the command prompt to terminate abnormally. This issue has been resolved	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	
CR-84675	CLI, SSH, Telnet	Previously, an unexpected system reboot could occur if a Telnet or SSH connection was terminated abnormally. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series			
CR-86047	DHCP Relay	<p>Due to a change in software version 5.5.4-2, an AlliedWare Plus device configured as a DHCP relay agent would include its own IP address in the DHCP server ID option when forwarding a DHCP offer to the client.</p> <p>This behavior has been reverted to the previous default, where the address of the DHCP server is used in the DHCP server ID option.</p> <p>For scenarios where it is preferable for the relay agent to use its own IP address, this can now be configured with the newly introduced command:</p> <p><b>ip dhcp-relay use-dhcp-relay-ip</b></p> <p>ISSU: Effective when CFCs upgraded.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
CR-85670	Environmental Monitoring	<p>Previously, on the IE340L/IE340 Series, the non-PoE variants would report a fault with power supplies under 46V, despite supporting power supplies from 18V.</p> <p>This issue has been resolved</p>	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-82923	EPSR	<p>Previously, when an EPSR ring transitioned to a 'complete' state after a failure, transit nodes could start receiving traffic on the alternate EPSR port.</p> <p>In some cases, host entries were not correctly updated to reflect the old port, causing traffic to be forwarded through the wrong interface</p> <p>This issue has been resolved.</p> <p>ISSU: Effective when CFCs upgraded</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series		
CR-85784	File System, File Transfer	The <b>strict-user-process-control</b> command now has an optional <b>force</b> parameter. If that parameter is set, no password prompt occurs and the command cannot be disabled without completely erasing flash.  In addition, the <b>strict-user-process-control</b> command will now notify the user that they should save their configuration and reboot, to ensure the change takes effect fully.  The <b>force</b> variant is intended for use only when required by specific certifications.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-85909	Findme	Previously, ports that were administratively shut down were not being flashed intermittently when using the Findme feature.  This issue has been resolved	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-85847	Firewall, NAT	Previously, when configuring entities with MAC address configuration only, the commands failed to be added to the running-configuration.  This issue has been resolved	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	-	Y	
CR-85786	IPv6 Multicast Routing, PIMv6	Previously, IPv6 Multicast could experience traffic interruptions due to incorrect blocking entries being added by MLD snooping.  This issue has been resolved	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	

CR	Module	Description	GS970M	GS970EMX	X5900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series		
CR-84776	L2TP, PPP, Tunnels	Previously, on AR4050S, AR4050S-5G, AR3050S, and ARX200S devices configured with L2TPv2/PPPoE AC, if a fatal exception occurred in a process, a secondary fatal exception could occur in the device kernel and prevent the generation of a core file. This issue has been resolved	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-85281	Loop Detection	Previously, ports that had been disabled by loop detection, MAC thrashing, or port security and were later added to an aggregator, would remain disabled. This issue has been resolved. Ports are now re-enabled when added to an aggregator. ISSU: Effective when CFCs upgraded	-	-	-	Y	Y	Y	-	-	-	-	-	Y	Y	-	Y	-	Y	Y	-	Y	Y	-	-	-	Y	-	-	-	-	-	-	-	-	-
CR-86282	Multicast Forwarding HW	Previously, the <b>show platform</b> command output included a display error on switch platforms which support L3 VXLAN, where a line break was missing following the 'L3 VXLAN' line. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	Y	-	Y	-	-	-	-	-	-	-	-

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series	
CR-84080	Multicast Routing	Previously, the VLAN parameter on some IPv6 multicast routes were being incorrectly displayed in the running-configuration with 'vlan' being printed twice, e.g. 'vlanvlan4'.  This would cause the parameter to be rejected when the configuration was saved and the device rebooted.  This issue has been resolved.  ISSU: Effective when CFCs upgraded	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	Y	Y	Y	Y	-	-	-	-	-	-	-
CR-84710	Open VPN	Previously, OpenVPN Client certificate authentication could stop working if you replaced your router and exported the trustpoints to a new unit.  This issue has been resolved	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	-	Y
CR-82935	PIM-SM	Previously, UDP multicast packets may have been dropped intermittently after a <b>clear ip mroute</b> command for a multicast group was executed.  This issue has been resolved	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series
CR-82036	PIM, IGMP, VCStack	<p>From AlliedWare Plus release 5.5.0-2, updates to hardware multicast table entries were performed asynchronously among stack members. This approach improved overall performance, particularly in environments with a very high number of multicast entries. However, in certain deployment scenarios, maintaining synchronized multicast entries across stack members is crucial to ensure accurate and reliable multicast data delivery to receivers connected to different stack members.</p> <p>With this change, you can now configure the system to use synchronous multicast entry manipulation. Enable this feature with the following command:</p> <p>(no) <b>platform sync-mc-ops</b></p> <p>Additionally, the <b>show platform table ipmulti</b> command has been updated to indicate whether multicast join/leave operations were processed synchronously or asynchronously.</p> <p>This issue has been resolved.</p>	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	Y	-	-	-	-	-	-	-
CR-85438	Pluggable Transceivers	<p>Previously, in rare cases, an issue could occur where pluggables would not be correctly detected at startup. Reinserting the pluggable would resolve the issue.</p> <p>This issue has been resolved.</p> <p>ISSU: Effective when CFCs upgraded</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	Y

CR	Module	Description	GS970M	GS970EMX	X5900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series		
CR-85399	Port Authentication, VCStack	Previously, it was possible for an IP connection to cease when a MAC entry aged out for a supplicant connected to a port of a VCStack member.  This issue has been resolved.	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	Y	-	-	-	-	-	-	-	
CR-85760	SSH	Previously, if a space was accidentally appended to a legitimate username when logging in via SSH, this could result in the legitimate user being deleted from the user database preventing subsequent logins using the affected username.  This issue has been resolved.  ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y
CR-85961	System, CLI	Previously, when the switch was under high load and the <b>show platform port</b> command was executed, this could cause switch processing to become overloaded and result in a system reboot.  This issue has been resolved	Y	Y	Y	-	-	-	Y	Y	Y	-	-	-	-	-	-	Y	-	-	Y	-	-	Y	Y	Y	-	Y	-	-	-	-	-	-	-	-
CR-85819	Telnet	Support for the "ip or -4" and "ipv6 or -6" options on the interactive Telnet command was mistakenly removed due to an upgrade of the underlying Telnet package.  Support for these options has been re-added. Additionally, the functionality of the -a option (autologin) now also works as intended.  This issue has been resolved.  ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y

CR	Module	Description	GS970M	GS970EMX	X5900MX	GS980M	GS980MX	GS980EM	IE210L	IE220	IE340/IE340L	IE360	IE210L	SE540L	SE250	SE240	x220	x230, x230L	x240	x320	x330	x530, x530L	x540, x540L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V/ARX200S-GTX	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ-R-Series	
CR-85696	VCStack, Multicast Routing	This software change enhances the <b>strict-user-process-control</b> command, providing tighter control over internal processes and enforcing stricter access restrictions to files intended for internal use only. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-85757	Wireless	Previously, when WEP and auto channel selection was in use on the TQ6702GEN-R, STAs were not able to connect to it with the correct wpa-suppllicant configuration. This issue has been resolved	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y

# What's New in Version 5.5.4-2.3

Product families supported by this version:

AMF Cloud	SE540L Series <sup>1</sup>
SwitchBlade x8100: SBx81CFC960	SE250 Series <sup>1</sup>
SwitchBlade x908 Generation 2	SE240 Series <sup>1</sup>
x950 Series	XS900MX Series
x930 Series	GS980MX Series
x550 Series	GS980EM Series
x540L Series	GS980M Series
x530 Series	GS970EMX Series
x530L Series	GS970M Series
x330 Series	10GbE UTM Firewall
x320 Series	AR4000S-Cloud
x250 Series <sup>1</sup>	AR4050S
x240 Series	AR4050S-5G
x230 Series	AR3050S
x220 Series	AR1050V
IE360 Series	TQ6702 GEN2-R
IE340 Series	
IE220 Series	
IE210L Series	

1. Not available in all regions

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-2.3.

Software file details for this version are listed in [Table 1](#) on the next page. You can obtain the software files from the [Allied Telesis Support Portal](#).

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 65](#).

For instructions on how to update the web-based GUI, see [“Accessing and Updating the Web-based GUI” on page 67](#). The GUI offers easy visual monitoring and configuration of your device.



**Caution:** Using a software version file for the wrong device may cause unpredictable results, including disruption to the network.

Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

The following table lists model names and software files for this version. Note that some models are not available in all regions.

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		01/2025	vaa-5.5.4-2.3.iso (VAA OS) vaa-5.5.4-2.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-0.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	01/2025	SBx81CFC960-5.5.4-2.3.rel
SBx908 GEN2	SBx908 GEN2	01/2025	SBx908NG-5.5.4-2.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	01/2025	x950-5.5.4-2.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	01/2025	x930-5.5.4-2.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2025	x550-5.5.4-2.3.rel
x540L-28XTm x540L-28XS	x540L	01/2025	x540-5.5.4-2.3.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	01/2025	x530-5.5.4-2.3.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	01/2025	x530-5.5.4-2.3.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	01/2025	x330-5.5.4-2.3.rel
x320-10GH x320-11GPT	x320	01/2025	x320-5.5.4-2.3.rel

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

Models	Family	Date	Software File
x250-18XS x250-28XS x250-28XTm	x250	01/2025	x250-5.5.4-2.3.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	01/2025	x240-5.5.4-2.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2025	x230-5.5.4-2.3.rel
x220-28GS x220-52GT x220-52GP	x220	01/2025	x220-5.5.4-2.3.rel
IE360-12GTX IE360-12GHX	IE360	01/2025	IE360-5.5.4-2.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	01/2025	IE340-5.5.4-2.3.rel
IE220-6GHX IE220-10GHX	IE220	01/2025	IE220-5.5.4-2.3.rel
IE210L-10GP IE210L-18GP	IE210L	01/2025	IE210-5.5.4-2.3.rel
SE540L-28XTm SE540L-28XS	SE540L	01/2025	SE540-5.5.4-2.3.rel
SE250-18XTm SE250-28XTm SE250-28XS	SE250	01/2025	SE250-5.5.4-2.3.rel
SE240-10GTXm SE240-10GHXm	SE240	01/2025	SE240-5.5.4-2.3.rel
XS916MXT XS916MXS	XS900MX	01/2025	XS900-5.5.4-2.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	01/2025	GS980MX-5.5.4-2.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	01/2025	GS980EM-5.5.4-2.3.rel
GS980M/52 GS980M/52PS	GS980M	01/2025	GS980M-5.5.4-2.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	01/2025	GS970EMX-5.5.4-2.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2025	GS970-5.5.4-2.3.rel
AR4000S-Cloud		01/2025	AR-4000S-Cloud-5.5.4-2.3.iso

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

Models	Family	Date	Software File
10GbE UTM Firewall		01/2025	ATVSTAPL-1.9.4.iso and vfw-x86_64-5.5.4-2.3.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	01/2025	AR4050S-5.5.4-2.3.rel AR3050S-5.5.4-2.3.rel
AR1050V	AR-Series VPN routers	01/2025	AR1050V-5.5.4-2.3.rel
TQ6702 GEN2-R	Wireless AP Router	01/2025	TQ6702GEN2R-5.5.4-2.3.rel

## ISSU (In-Service Software Upgrade) on SBx8100 with CFC960

The 5.5.4-2.3 software version is **not** ISSU compatible with previous software versions.

## New Features and Enhancements

This section summarizes the new features and enhancements in AlliedWare Plus version 5.5.4-2.3.

To see how to find full documentation about all features on your product, see [“Obtaining User Documentation”](#) on page 59.

This version supports the following enhancements:

### General enhancements

- “Password change required when first logging into a device” on page 38
- “Password strength checked for users at all privilege levels” on page 38
- “DHCP Relay Short Lease Time” on page 38
- “IP Flow Information Export (IPFIX) enhancements” on page 40
- “Restart Notification trap” on page 41
- “Support for more YANG data models” on page 41
- “Improved diagnostics for memory consumption issues” on page 41
- “Testing connectivity to an SNMP manager” on page 42
- “Compatibility of Local RADIUS Server and TQ series access points” on page 42
- “Login accounting periodic updates” on page 43

### Firewall enhancements

- “OpenVPN RADIUS accounting support” on page 44
- “GeoIP support in firewall entities” on page 44
- “Improved support for security processing of TLS1.3-encrypted traffic” on page 45

### Wireless AP router enhancements

- “Support for DPI Web Categorization on the TQ6702 GEN2-R” on page 46
- “Ethernet ports on TQ6702 GEN2-R support 10M link speed” on page 46
- “Support for CCMP cipher with WPA3 encryption on TQ6702 GEN2-R” on page 46
- “Removal of requirement to specify a basic rate on TQ6702 GEN2-R” on page 47
- “Support Dynamic VLAN with MAC-Authentication on TQ6702 GEN2-R” on page 47

### Switch enhancements

- “Support for IPv6 VRF multicast routing” on page 48
- “Mirroring enhancements” on page 49
- “100M support added for SPTXc on x250, SE250, x540L and SE540L series switches” on page 49
- “Mark a switch's PSU or power input as unused” on page 50
- “Denial of Service (DoS) protection added to more switch series” on page 51

## Password change required when first logging into a device

*Applies to all devices running AlliedWare Plus*

From 5.5.4-2.3 onwards, users are prompted to change the login password when they first log into a device that is in factory new state (or a device that has been reset to that state).

Devices that already have a user configuration will not be affected.

## Password strength checked for users at all privilege levels

*Applies to all devices that run AlliedWare Plus*

From 5.5.4-2.3 onwards, the same password check is done for new login passwords for all users, regardless of the user privilege level. Previously, strong password rules were only enforced on users with administrator-level privileges (level 15).

## DHCP Relay Short Lease Time

*Available on: All Firewalls and routers, and all Layer 3 switches running AlliedWare Plus*

From 5.5.4-2.3 onwards, DHCP Relay short lease time is supported.

When a device connects to a network, a DHCP server assigns it an IP address and a 'lease time', which specifies how long the address can be used before renewal. Long lease times can cause issues in dynamic networks where devices move between segments, such as VLANs, as the device may retain an outdated IP address from its previous VLAN, disrupting communication.

The **ip dhcp-relay short-lease** command resolves this by allowing you to reduce lease times, typically to one or two minutes. This forces devices to quickly request a new IP address when changing VLANs, ensuring compatibility with the new segment. This command is particularly useful in networks with high turnover of devices or in environments where IP addresses are scarce.

### The key concepts

The following are key concepts and components involved in DHCP Relay Short Lease Time:

- DHCP Relay** A DHCP Relay is a network helper that makes sure devices in different parts of a network can still connect to a central DHCP server to get IP addresses. It works by taking the IP request from a device, passing it to the DHCP server, and then bringing the server's response back to the device, even if they are on different sections of the network. This allows all devices to get IP addresses from the same server, no matter where they are in the network.

**Renewal time** Renewal time, referred to as T1 in DHCP, is the time at which a DHCP client begins attempting to renew its IP address lease with the DHCP server. This occurs before the lease expires, ensuring the client can continue using the same IP address without interruption. If the renewal is successful, the lease is extended. If it is not, the client will continue to use the current lease until it attempts a rebinding closer to the lease expiration. Typically T1 sets at approximately 50% of the lease time.

**Binding time** Binding time, referred to as T2 in DHCP, is the time when the client, having failed to renew the lease at T1, will attempt to rebind with any available DHCP server to extend its lease before the current lease expires. Typically T2 sets at approximately 87.5% of the lease time.

**Lease time** Lease time in DHCP is the total duration for which an IP address is assigned to a client. During this lease period, two key milestones, T1 (Renewal time) and T2 (Binding time), help manage the lease.

**Asymmetric DHCP lease timing** Asymmetric DHCP Lease Timing refers to a setup where devices on a network have different schedules for when their DHCP leases expire and need to be renewed. This timing is not the same for every device, which means they don't all request a new IP address from the DHCP server at the same time. This is particularly useful in networks where a DHCP Relay is used to manage DHCP communications across different network segments, such as VLANs.

## New commands

The new commands available with this feature are:

### **ip dhcp-relay short-lease-ipv6**

For example, to configure a DHCP Relay on interface vlan1 to set a 2000 seconds valid and 1000 seconds **preferred** lease time for **IPv6**, use the commands:

```
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay short-lease-ipv6 2000 1000
```

### **ip dhcp-relay short-lease**

For example, to configure a DHCP Relay on interface vlan1 to set 200 seconds lease time for IPv4, use the commands:

```
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay short-lease 200
```

## Updated command

You can see the DHCP Relay short-lease information line in the output of the command **show ip dhcp-relay interface <ifname>**

```
awplus#show ip dhcp-relay interface vlan1

DHCP Relay Service is enabled
Use of client side address as source address is disabled
vlan1 is up, line protocol is up
Maximum hop count is 10
Maximum DHCP message length is 1400
DHCP Relay short lease time for IPv4 is 200 seconds <----
DHCP Relay short lease time for IPv6 are 2000/1000 (valid/preferred) seconds <---
Insertion of Relay Agent Option is enabled
Checking of Relay Agent Option is disabled
Insertion of Subscriber-ID auto-MAC is disabled
The Remote Id string for Relay Agent Option is 5254.1992.0861
Relay Information policy is to replace existing relay agent information
List of servers : 192.168.1.33
```

For more information on DHCP for IPv4, see the [DHCP Feature Overview and Configuration Guide](#).

For more information on DHCP IPv6, see the [DHCP for IPv6 \(DHCPv6\) Feature Overview and Configuration Guide](#).

## IP Flow Information Export (IPFIX) enhancements

*Applies to SBx8100 CFC960 control card, x320, x220, GS980MX, GS980EM, and GS980M series switches*

From 5.5.4-2.3 onwards, IPFIX is supported on the above new platforms. Previously, it was supported only on x530 series switches.

In addition, this version supports IPv6 traffic monitoring on the above switches and x530 series switches.

IPFIX is an IETF protocol defined in [RFC 7011](#) that provides a standard for exporting IP flow data from a network for analysis. Network administrators analyze the IP flow data, and make decisions, such as applying QoS policies or maybe adding more bandwidth to network areas that need it.

For more information on IPFIX, see the [IPFIX Feature Overview and Configuration Guide](#).

## Restart Notification trap

*Applies to all devices running AlliedWare Plus*

From 5.5.4-2.3 onwards, the restartNotification trap is supported on system shutdown. This implements the restartNotification trap that exists in AT-SYSINFO-MIB in AlliedWare Plus, and results in an SNMP trap when the administrator reboots the device.

For more information on SNMP MIBs, see [Support for Allied Telesis Enterprise MIBs in AlliedWare Plus](#).

## Support for more YANG data models

*Applies to all devices running AlliedWare Plus*

From 5.5.4-2.3 onwards, new YANG data models are supported, as well as changes to existing models. You can see full details and the latest models at:

<https://github.com/alliedtelesis/yang>.

For more information about using YANG models, see the [NETCONF and RESTCONF Feature Overview and Configuration Guide](#).

## Improved diagnostics for memory consumption issues

*Applies to all AlliedWare Plus devices, except for AMF Cloud*

From 5.5.4-2.3 onwards, diagnostics of low-memory issues have been improved, in the following ways:

- When memory drops sufficiently low, the device will now automatically terminate the non-critical process that has the highest memory consumption. Note that only a non-critical process will be terminated automatically, not a critical process.
- SNMP traps can be generated when available memory drops beneath low, very low and critical thresholds, and when it returns to normal. The traps are:
  - « 1.3.6.1.4.1.207.8.4.4.3.7.0 memoryTraps
  - « 1.3.6.1.4.1.207.8.4.4.3.7.0.1 memoryLowTrap
  - « 1.3.6.1.4.1.207.8.4.4.3.7.0.2 memoryVeryLowTrap
  - « 1.3.6.1.4.1.207.8.4.4.3.7.0.3 memoryCriticalTrap  
(However, note that when the system reaches the critical memory threshold, it reboots before a trap can be sent.)
  - « 1.3.6.1.4.1.207.8.4.4.3.7.0.4 memoryReturnToNormalTrap
  - « 1.3.6.1.4.1.207.8.4.4.3.7.0.5 vcstackId

To enable the traps, use the command:

```
awplus(config)# snmp-server enable trap low-memory
```

- The memory thresholds have been adjusted, to make sure that the device can produce sufficient debugging output before reaching the critical threshold and rebooting.
- A new command enables you to specify a process for the device to terminate if available memory is sufficiently low. This command is intended for use in consultation with Allied Telesis customer support. Using this command will make the device produce a core dump when the process terminates, which makes it easier for Allied Telesis engineers to debug any issues.

The new command is:

```
awplus(config)# low-memory restart <process-name>
```

The process does not have to be running when you enter this command. If it is running at the time the available memory becomes sufficiently low, the device will terminate it.

- On SBx8100, this full feature set is only available on the SBx81CFC960 control card, the SBx81XLEM modular line card, and the modules that plug into the SBx81XLEM. Only the SNMP traps are available on other line cards.

## Testing connectivity to an SNMP manager

*Applies to all AlliedWare Plus devices except AMF Cloud*

From 5.5.4-2.3 onwards, you can enter a command to test connectivity between the AlliedWare Plus device and an SNMP manager. The new command tests the connectivity by sending a one-off coldStart or warmStart trap. The new command is:

```
awplus# test snmp trap snmp coldstart
```

or

```
awplus# test snmp trap snmp warmstart
```

## Compatibility of Local RADIUS Server and TQ series access points

*Applies to all devices that support the local RADIUS server*

From 5.5.4-2.3 onwards, the local (in-built) RADIUS server on AlliedWare Plus devices has been upgraded. As a result of that upgrade, the AlliedWare Plus device may require an extra command if you want to authenticate TQ series APs through the local RADIUS server. This command is needed if you use both web authentication and MAC authentication to authenticate the same AP. Without this command, web authentication may fail.

The command is accessed in RADIUS Server Configuration mode:

```
awplus# configure terminal
```

```
awplus(config)# radius-server local
```

```
awplus(config-radsrv)# nas <ip-address> message-authenticator optional
```

This command is required because the upgraded local RADIUS server changes how message authentication is handled by default. From 5.5.4-2.3 onwards, if the first packet that the server receives from the client contains a valid Message-Authenticator attribute, then by default all subsequent packets from that client must also contain the same Message-Authenticator attribute. If packets don't contain the attribute, the server drops them. This can cause an issue on TQ series APs, because on these APs, MAC authentication's initial packet contains the attribute, and web authentication's initial packet doesn't. This means that web authentication will fail if MAC authentication has already happened.

The new command allows the server to accept packets from a client when the packets don't have a Message-Authenticator attribute, even if the server has already received a packet from that client that contained a Message-Authenticator attribute. This means both web authentication and MAC authentication will succeed, no matter which happens first.

## Login accounting periodic updates

*Applies to all devices running AlliedWare Plus*

From 5.5.4-2.3 onwards, the **aaa accounting login** command supports the **aaa accounting update periodic** command.

### Example

To configure RADIUS login accounting with periodic updates, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group radius
awplus(config)# aaa accounting update periodic <1-65535>
```

The number specifies the interval in minutes at which interim updates will be sent.

For more information on RADIUS, see the [RADIUS Feature Overview and Configuration Guide](#).

For more information on AAA, see the [AAA Feature Overview and Configuration Guide](#).

## OpenVPN RADIUS accounting support

*Available on all devices that support OpenVPN*

From 5.5.4-2.3 onwards, if you use an external RADIUS server when authenticating OpenVPN tunnels, you can enable RADIUS accounting. To do this, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting openvpn default {start-stop|
stop-only|none} group <radius-server-group>
```

You can also enable interim updates using the following command, where the number specifies the interval in minutes at which interim updates will be sent:

```
awplus(config)# aaa accounting update periodic <1-65535>
```

For more information on RADIUS, see the [RADIUS Feature Overview and Configuration Guide](#).

For more information on AAA, see the [AAA Feature Overview and Configuration Guide](#).

## GeoIP support in firewall entities

*Applies to all UTM firewalls and VPN routers running AlliedWare Plus*

From 5.5.4-2.3 onwards, the GeoIP (Geographic IP) feature is supported.

The GeoIP feature is a network security and traffic management tool. It uses IP address geolocation to identify the approximate geographic location of clients or servers by mapping IP address blocks to specific countries or regions.

GeoIP is widely used for purposes such as security, access control, and traffic optimization. For instance, it can restrict access to a service to only those with source IP addresses from a specific region. Similarly, it can block all traffic originating from regions known for frequent malicious or nuisance network activities.

The feature enables you to dynamically add all networks assigned to a specific country to an entity with a single command. These networks are sourced from a third-party provider and updated automatically on a regular basis.

GeoIP is a best-effort service designed to conveniently limit or block traffic based on expected sources or destinations. However, it does not guarantee that all traffic associated with these locations will be detected, nor does it prevent parties from obscuring their true location. Users are encouraged to utilize additional features, such as Advanced IPS, IP Reputation, and Web Categorization, to enhance protection against malicious activity.

## New commands

The following new commands are available:

```
ip subnet dynamic geoip
ipv6 subnet dynamic geoip
geoip update-interval
```

## Examples

1. To configure an entity to select traffic to/from Russia, use the following commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# ip subnet dynamic geoip RU
```

2. To only allow OpenVPN traffic to the device when it comes from a source address associated with Japan:

Create the GeoIP entity:

```
awplus# configure terminal
awplus(config)# zone japan
awplus(config-zone)# network geoip
awplus(config-network)# ip subnet dynamic geoip JP
```

Add the rule:

```
awplus(config)# firewall
awplus(config-firewall)# rule permit openvpn from japan to
wan.wan_int.wan_ip
```

## Improved support for security processing of TLS1.3-encrypted traffic

*Applies to all AlliedWare Plus firewalls that support licensed security features*

From 5.5.4-2.3 onwards, performance of security features on AlliedWare Plus firewalls has improved for TLS1.3-encrypted traffic. This applies to the licensed security features (application control, web control, advanced IPS, IP reputation, URL filtering, and web categorization).

For more information about these features, see the [Advanced Network Protection Feature Overview and Configuration Guide](#).

## Support for DPI Web Categorization on the TQ6702 GEN2-R

From 5.5.4-2.3 onwards, DPI Web Categorization is supported on the TQ6702 GEN2-R Wi-Fi Access Point and VPN router.

Web Categorization helps protect users on the network based on the type of website they access. It enables businesses to manage the types of website their staff can access.

The DPI engine does this by scanning packets traversing the system and identifying HTTP hostnames or TLS server names and passing these to the Web Categorization engine for subsequent processing.

Web Categorization then matches the hostname against custom hosts configured under the 'application' configuration mode, and/or sends it to the third party categorizer for processing. So for example, you could block all 'Gambling' websites. Once a category has been determined, the packet flow will match rules that specify that category in their application field, for example, Firewall, NAT or PBR rules.

For more information on DPI and Web Categorization, see the [Advanced Network Protection Feature Overview and Configuration Guide](#).

## Ethernet ports on TQ6702 GEN2-R support 10M link speed

From 5.5.4-2.3 onwards, the TQ6702 GEN2-R wireless router can link up to a device that advertises a link speed of 10M. The TQ6702 GEN2-R now supports auto-negotiation at 10M Full Duplex on both Ethernet ports. Note that setting 10M as a fixed speed is not supported.

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

From 5.5.4-2.3 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, using a CLI command. For example, to select CCMP on security-ID 1, use the commands:

```
awplus(config)# wireless
awplus(config-wireless)# security 1 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# version wpa3
awplus(config-wireless-sec-wpa-ent)# ciphers ccmp
```

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

From 5.5.4-2.3 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.

To use the CLI to select the legacy rate or rates you want to use, use the commands:

```
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# legacy-rates <list>
```

The rates can be one or more of 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, or 1.

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. To use the CLI to select this, use the commands:

```
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# multicast-tx-rate {1|2|
5.5|6|9|11|18|12|24|36|48|54}
```

## Support Dynamic VLAN with MAC-Authentication on TQ6702 GEN2-R

From 5.5.4-2.3 onwards, Dynamic VLAN is now supported with MAC authentication on a wireless network on the TQ6702 GEN2-R. This makes it possible to use dynamic VLANs with WPA Personal.

Dynamic VLAN lets the TQ6702 GEN2-R dynamically assign the VLAN into which a device's traffic will be classified, once that device has been authenticated. This is achieved by a collaboration between the authenticator (the TQ6702 GEN2-R) and the authentication server (the RADIUS server). When the RADIUS server sends back a RADIUS accept message to the authenticator, it can also include attributes in that message that identify a VLAN to which the authenticated device should be assigned.

Previously, when MAC authentication was used, any VLAN assignment would be based on the VAP that the client connects to, whereas Dynamic VLAN can assign a specific VLAN to each client.

To use the CLI to enable Dynamic VLAN with MAC authentication (on network 1 in this example), use the commands:

```
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth dynamic-vlan enable
```

You can also enable Dynamic VLAN in WPA enterprise security mode. If you have both, the VLAN assigned from the WPA Enterprise authentication will take precedence over the VLAN assigned from MAC authentication.

## Support for IPv6 VRF multicast routing

*Applies to SBx8100 CFC960, SBx908 GEN 2, x950, x930, x540L and x530 series switches*

From 5.5.4-2.3 onwards, IPv6 multicast routing with VRF is supported for MLD, MLD Snooping, PIM-SM, Fast Failover for PIM-SM - all in IPv6 named VRFs. This allows for multiple IPv6 multicast routing tables to co-exist on the same device.

No new limitations exist, but note the existing limit of 100 VLANs that can support MLD.

### Commands

You can use this command to enable multicast routing on a given VRF:

```
ipv6 multicast-routing vrf
```

You can now specify VRF on the following commands:

```
ipv6 multicast vrf VRF route-limit
ipv6 multicast vrf VRF forward-slow-path-packet
ipv6 pim vrf VRF accept-register
ipv6 pim vrf VRF anycast-rp
ipv6 pim vrf VRF bsr-candidate
ipv6 pim vrf VRF cisco-register-checksum
ipv6 pim vrf VRF crp-cisco-prefix
ipv6 pim vrf VRF ignore-rp-set-priority
ipv6 pim vrf VRF jp-timer
ipv6 pim vrf VRF register-rate-limit
ipv6 pim vrf VRF register-rp-reachability
ipv6 pim vrf VRF register-source
ipv6 pim vrf VRF register-suppression
```

```

ipv6 pim vrf VRF rp
ipv6 pim vrf VRF rp-address
ipv6 pim vrf VRF rp-candidate
ipv6 pim vrf VRF rp-register-kat
ipv6 pim vrf VRF spt-threshold
ipv6 pim vrf VRF ssm

```

You can also specify VRF in the following show commands:

```

show ipv6 mld (vrf VRF|global)
show ipv6 pim (vrf VRF|global) sparse-mode
show ipv6 multicast forwarding (vrf VRF|global)
show ipv6 mif (vrf VRF|global)

```

**Monitoring** You can learn more about the associated features and debug commands as described in the following MLD, PIM-SM, and VRF-lite guides:

- [IGMP/MLD Feature Overview and Configuration Guide](#)
- [PIM Sparse Mode for IPv6 \(PIM-SMv6\) Feature Overview and Configuration Guide](#)
- [VRF-lite Feature Overview and Configuration Guide](#)

## Mirroring enhancements

*Applies to SBx908 GEN 2, x950, x930, x550, x540L, x530, x530L, x330, x320, x250, x240, x230, x220, IE340, IE220, IE210L and XS900MX series switches*

From 5.5.4-2.3 onwards, the number of allowable mirror ports has been increased on some devices.

For more information on mirroring, see the [Mirroring Feature Overview and Configuration Guide](#)

## 100M support added for SPTXc on x250, SE250, x540L and SE540L series switches

From 5.5.4-2.3 onwards, AlliedWare Plus supports a link speed of 100M on SPTXc transceivers on the following XS switch models: x250-18XS, x250-28XS, SE250-18XS, SE250-28XS, x540L-28XS and SE540L-28XS.

The following speed/duplex settings are supported:

Speed	Duplex
Autonegotiation at 100M	Autonegotiation
Autonegotiation at 100M	Full
Fixed at 100M	Autonegotiation

## Mark a switch's PSU or power input as unused

*Applies to x530, GS980MX, x320-10GH, GS980EM/10H, IE340 and IE360 Series switches*

From 5.5.4-2.3 onwards, you can mark a switch's redundant PSU or power input as unused, if you have intentionally not plugged in that PSU. This may be helpful, because otherwise the switch treats an unused PSU or power input as an environmental fault. The fault is displayed in output from commands such as **show system**, and in some configurations, the environmental fault may trigger an alarm. Marking a PSU or power input as unused prevents this.

To mark a PSU or power input as unused, use the new command:

```
awplus(config)# system psu [member <1-8>] psu <1-4> unused
```

where:

- **member** is the stack member ID in a VCStack
- **psu <1-4>** is the numerical ID of the PSU or power input.

To see whether a PSU or power input has been marked as unused, use the new command:

```
awplus# show system psu config
```

Also note the following important points about this feature:

- The configuration is applied after the switch's code has started to run so an initial alarm may be raised, which will then be cleared.
- On IE360 and IE340 series switches, the voltage input sensor for the relevant PSU will be treated as unavailable, so the PSU will no longer be monitored and will not show in the output of **show system**.
- On switches where the voltage input sensor for the relevant PSU is treated as unavailable, no high or low threshold alarms will be generated for the sensor while it is marked as unused.
- IE series switches have some sensors that trigger SNMP traps or alarm monitoring events when power is applied or removed. These traps and events are not affected by this enhancement. In general, if a PSU is marked as unused, we expect that power will not be applied or removed during normal operation.
- On x530 and GS980MX series switches with dual fixed PSUs, the fixed PSU bay will be marked as 'power not required', to prevent alarms for the PSU power input regardless of state.
- The x320-10GH switch has three PSU inputs treated as fixed PSU slots. These will be marked as optional. When setting them to unused, the fixed PSU bay will be marked as 'power not required', to prevent alarms for the PSU power input regardless of state.
- On switches where this feature marks a PSU bay as 'power not required', SNMP traps may still be sent when the power status of the PSU changes state. However, the traps will always be AT-ENVMONv2-MIB::atEnvMonv2PsbAlarmClearedNotify. If the bay was not marked as 'power not required', instead an AT-ENVMONv2-MIB::atEnvMonv2PsbAlarmSetNotify trap would be sent if power was removed.
- A warning will be logged and printed to the CLI if a PSU that is detected as powered is marked as unused.

## Denial of Service (DoS) protection added to more switch series

*Applies to x230, x220, IE210, GS980M, GS970M*

From 5.5.4-2.3 onwards, DoS protection has been added to the above series of switches. DoS protection is designed to detect, prevent, or mitigate Denial of Service (DoS) attacks. DoS attacks can include Ping of Death, Smurf, SYN Flood, and Teardrop attacks.

To enable DoS protection on (for example) port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# {ipoptions|land|ping-of-death|smurf
broadcast <ip-address>|synflood|teardrop} action {shutdown|
trap|mirror}
```

where **action** is whether to shut the port down, send an SNMP trap, or send the packets to a mirror port.

# Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that may affect your device or network behavior if you upgrade:

- [Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches](#)
- [Changes that may affect device or network configuration](#)

It also describes the new version's compatibility with previous versions for:

- [Software release licensing](#)
- [Upgrading a VCStack with rolling reboot](#)
- [Forming or extending a VCStack with auto-synchronization](#)
- [AMF software version compatibility](#)
- [Upgrading all devices in an AMF network](#)

Please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.2-3.x version, please check the 5.5.3-0.x, 5.5.3-1.x and 5.5.3-2.x release notes. Release notes are available from our website, including:

- [5.5.4-x.x release notes](#)
- [5.5.3-x.x release notes](#)
- [5.5.2-x.x release notes](#)
- [5.5.1-x.x release notes](#)
- [5.5.0-x.x release notes](#)
- [5.4.9-x.x release notes](#)
- [5.4.8-x.x release notes](#)
- [5.4.7-x.x release notes](#)
- [5.4.6-x.x release notes](#)

## Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches

These switches can only be upgraded to the most recent firmware versions from specified older firmware versions. If you attempt to upgrade from other older firmware versions, the firmware becomes corrupt and the switch will not boot up.

**The solution** Before upgrading to the latest firmware version, upgrade to one of the specified older versions. See [“Details for SBx908 GEN2 and x950 Series” on page 53](#) and [“Details for x930 Series” on page 54](#) for details.

### Affected Products

The following models could be affected:

x930 Series running any bootloader version	x950 Series running bootloader versions older than 6.2.24	SBx908 GEN2 running bootloader versions older than 6.2.24
x930-28GTX	x950-28XSQ	SBx908 GEN2
x930-28GPX	x950-28XTQm	
x930-52GTX		
x930-52GPX		
x930-28GSTX		

For SBx908 GEN2 and x950 Series, the restriction only applies to switches running bootloader versions older than 6.2.24.

## Recovering from upgrading from an incompatible version

If you try to upgrade from an incompatible firmware version, the switch will not finish booting up. If this happens, you can recover by using the bootloader menu to boot with a compatible version from an alternative source, such as a USB stick. See the [Bootloader and Startup Feature Overview and Configuration Guide](#) for details.

### Details for SBx908 GEN2 and x950 Series

For these switches, switches where the bootloader is older than 6.2.24 are affected. If your bootloader is older than 6.2.24, you **cannot** upgrade to the most recent firmware version directly from:

- 5.4.9-1.x
- 5.4.9-0.x
- any version before 5.4.8-2.12.

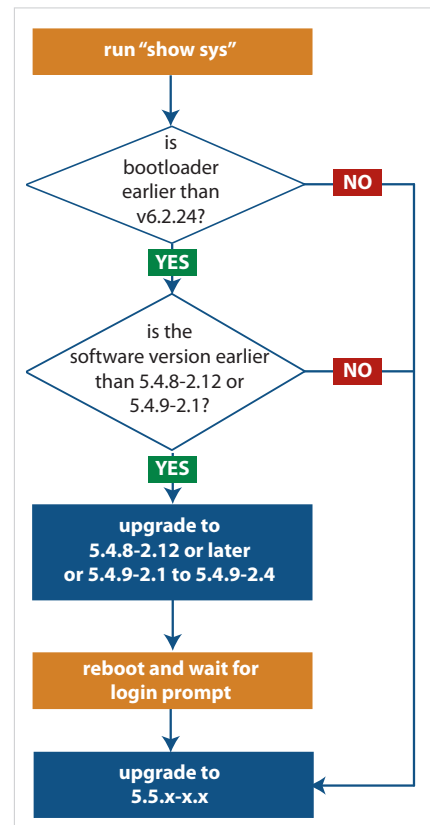
Instead, before upgrading from one of those versions to the current version, make sure your switch is running one of these specified versions:

- 5.4.8-2.12 or a later 5.4.8-2.x version
- 5.4.9-2.1 to 5.4.9-2.4.

If it is not, upgrade to one of these versions before upgrading to the most recent firmware version.

To see your bootloader and current software version, check the “Bootloader version” and “Software version” fields in the command:

```
awplus# show system
```



## Details for x930 Series

For these switches, **versions 5.5.1-2.1** and later are affected, on switches with all bootloaders. You **cannot** upgrade to most recent firmware version directly from:

- 5.5.1-1.3 or earlier
- 5.5.1-0.x
- 5.5.0-2.11 or earlier
- 5.5.0-1.x
- 5.5.0-0.x
- any version before 5.4.9-2.7.

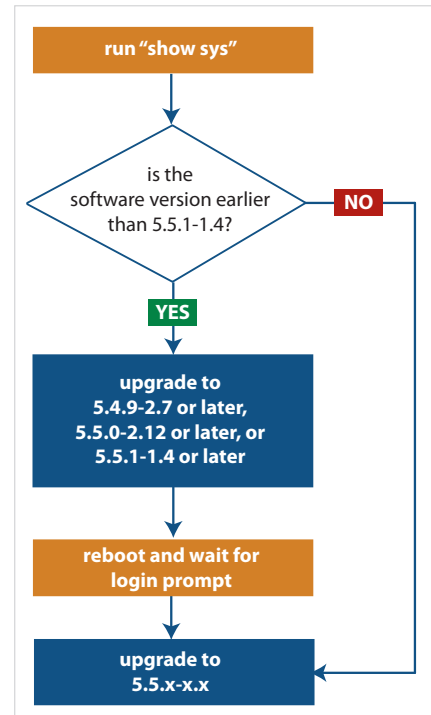
Instead, before upgrading from one of those versions to most recent firmware version, make sure your switch is running one of these specified versions:

- 5.4.9-2.7 or a later 5.4.9-2.x version
- 5.5.0-2.12 or a later 5.5.0-2.x version
- 5.5.1-1.4 or a later 5.5.1-1.x version.

If it is not, upgrade to one of these versions before upgrading to most recent firmware version.

To see your current firmware version, check the “Software version” field in the command:

```
awplus# show system
```



## Changes that may affect device or network configuration

The following changes may require you to modify your device or network configuration when you upgrade to this release.

Summary	Affected devices	Detail
VRF configuration reordered in running config	All devices that support VRF	From 5.5.4-0.1 onwards, VRF configuration is printed near the start of running configuration files. This makes sure that AlliedWare Plus creates the VRF instances before running commands that use those VRFs.

Summary	Affected devices	Detail
DES deprecated for TACACS+ server key encryption	All devices that support TACACS+	<p>From 5.5.4-0.1 onwards, newly-created TACACS+ shared keys are stored as AES-encrypted keys. It is no longer possible to create a DES-encrypted key. If the device's running-config contains a DES key, the device will automatically convert it to an AES key.</p> <p>This means that if the running-config contains this command:</p> <pre>tacacs-server key 8 &lt;DES-obfuscated-string&gt;</pre> <p>the device will convert it to this command:</p> <pre>tacacs-server key 9 &lt;AES-obfuscated-string&gt;</pre>

## Command 'license update online' no longer available

*Applies to all AlliedWare Plus devices and all firmware versions.*

The **license update online** command is no longer available for downloading licenses due to changes in Allied Telesis' license management portal. This change is applicable to all firmware versions, not just the latest.

Summary	Affected devices	Detail
<b>license update online</b> command no longer available.	All AlliedWare Plus devices with subscription licenses across all firmware versions, including previous versions.	Starting January 2025, the <b>license update online</b> command will no longer be available for downloading licenses. To obtain licenses, please contact your authorized Allied Telesis support center. After obtaining the license, use the <b>license update file</b> command to install it.

## Software release licensing

*Applies to SBx908 GEN2 and SBx8100 Series switches*

Please ensure you have a 5.5.4 license on your switch if you are upgrading to 5.5.4-x.x on your SBx908 GEN2 or SBx8100 switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- ["Licensing this Version on an SBx908 GEN2 Switch" on page 61](#)
- ["Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 63.](#)

## Upgrading a VCStack with rolling reboot

*Applies to all stackable AlliedWare Plus switches, except SBx8100*

This version supports VCStack “rolling reboot” upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

### For SBx908 GEN2, x950 and x550 Series switches

You can use rolling reboot to upgrade to this version from:

- All versions from 5.5.0-x.x onwards

On these switches, you **cannot** use rolling reboot to upgrade to this version from any version earlier than 5.5.0-0.x.

### For x530 Series switches using DAC to stack

If you are using DACs (Direct Attach Cables) to connect stack members, you can use rolling reboot to upgrade to this version from:

- All versions from 5.5.0-x.x onwards
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

### For other switches and for x530 switches using SFP+ to stack

Otherwise, you can use rolling reboot to upgrade to this version from:

- All versions from 5.4.5-x.x onwards
- 5.4.4-1.x

### To use rolling reboot

First enter the **boot system** command, which will install the new release file on all stack members. Then enter the **reboot rolling** command.

## Forming or extending a VCStack with auto-synchronization

*Applies to all stackable AlliedWare Plus switches*

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

If auto-synchronization is not supported between the software versions on the devices in your stack, you need to make sure all devices are running the same version before you connect the stack together.

### For SBx908 GEN2, x950 and x550 Series switches

Auto-synchronization is supported between this version and:

- All versions from 5.5.0-x.x onwards

On these switches, auto-synchronization is not supported between this version and any version earlier than 5.5.0-0.x.

**For CFC960 cards  
in an SBx8100  
system**

If you want to combine CFC960 v2 and earlier CFC960 cards in a chassis or stack, make sure that the earlier cards are running 5.5.0-x.x or later before you combine them. This applies whether you:

- add a CFC960 v2 card to a chassis or stack that contains earlier CFC960 cards, or
- add an earlier CFC960 card to a chassis or stack that contains CFC960 v2 cards.

Auto-synchronization will not update the software on the earlier CFC960 cards.

Note that this situation only applies if your chassis or stack includes CFC960 v2 cards that are labeled "SBx81CFC960 v2" on the front panel of the card. All cards that are labeled "SBx81CFC960" are referred to as earlier cards, even if their documentation refers to them as version 2.

If you do combine cards that are running incompatible software, then remove the CFC960 v2 card or cards, update the software on the other cards, and re-install the CFC960 v2 cards.

**For x530 Series  
switches using  
DAC to stack**

If you are using DACs (Direct Attach Cables) to connect stack members, auto-synchronization is supported between this version and:

- All versions from 5.5.0-x.x onwards
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

**For other switches  
and for x530  
switches using  
SFP+ to stack**

Otherwise, auto-synchronization is supported between this version and:

- All versions from 5.4.7-x.x onwards
- 5.4.6-2.x
- 5.4.6-1.2 and all later 5.4.6-1.x versions.

It is not supported between this version and 5.4.6-1.1 or **any** earlier releases.

## AMF software version compatibility

*Applies to all AlliedWare Plus devices*

We strongly recommend that all nodes in an AMF network run the same software release. However, if this is not possible, then nodes running this version are compatible with nodes running:

- All versions from 5.4.4-x.x onwards
- 5.4.3-2.6 or later.

## Upgrading all devices in an AMF network

*Applies to all AlliedWare Plus devices*

**This version supports upgrades across AMF networks.** There are two methods for upgrading firmware on an AMF network:

- Reboot-rolling, which upgrades and reboots each node in turn
- Distribute firmware, which upgrades each node, but does not reboot them. This lets you reboot the nodes at a minimally-disruptive time.

You can use either reboot-rolling or distribute firmware to upgrade to this software version, from 5.4.3-2.6 and later.

However, if you use reboot-rolling or distribute firmware to upgrade an AMF network, and any of the devices are running 5.4.7-1.1 or later, then you must initiate the upgrade from a device that is running 5.4.7-1.1 or later. Otherwise, the devices running 5.4.7-1.1 or later will not be upgraded.

If you are using rolling-reboot, we recommend limiting it to working-sets of 42 nodes or fewer.

In summary, the process for upgrading firmware on an AMF network is:

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
  - a. create a working-set of the nodes you want to upgrade
  - b. enter the command **atmf reboot-rolling <location>** or **atmf distribute-firmware <location>** where **<location>** is the location of the .rel files.
  - c. Check the console messages to make sure that all nodes are "release ready". If they are, follow the prompts to perform the upgrade.

## Obtaining User Documentation

For full AlliedWare Plus documentation, [click here to visit our online Resource Library](#). For AlliedWare Plus products, the Library includes the following documents:

- **Feature Overview and Configuration Guides** - find these by searching for the feature name and then selecting Configuration Guides in the left-hand menu.
- **Datasheets** - find these by searching for the product series and then selecting Datasheets in the lefthand menu.
- **Installation Guides** - find these by searching for the product series and then selecting Installation Guides in the lefthand menu.
- **Command References** - find these by searching for the product series and then selecting Reference Guides in the lefthand menu.

## Verifying the Release File

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

```
awplus(config)# crypto verify <filename> <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 [Hash values for 5.5.4-2.5](#) below or in the release's sha256sum file, which is available from the [Allied Telesis Support Portal](#).

### 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.**

All switch models of a particular series run the same release file and therefore have the same hash. For example, all x930 Series switches have the same hash.

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

Table: Hash values for 5.5.4-2.5

Product family	Software File	Hash
AMF Cloud-	vaa-5.5.4-2.5.rel	a9fefce95c09c7b8ad825a6c42c6cd0f52f3bf4b6e40d317f40c061c4734f894
SBx8100	SBx81CFC960-5.5.4-2.5.rel	d641e8f74542ff35aad324ed136dfa45fc8661eb4f250d032ab79ace3960104f
SBx908 GEN2	SBx908NG-5.5.4-2.5.rel	657dee4d9bf5f7a6cecedfad03956c7cc86c090dedba47f68d9f051661177f49
x950	x950-5.5.4-2.5.rel	657dee4d9bf5f7a6cecedfad03956c7cc86c090dedba47f68d9f051661177f49
x930	x930-5.5.4-2.5.rel	ef8266d3905f8579eb4ff0c997aef36949443b192911438241b1694a18d1e71f
x550	x550-5.5.4-2.5.rel	aa06b7345b0aa781ee24f157702034bd09c654fed1a707828d8963332c0b5a8d
x540L	x540-5.5.4-2.5.rel	ee7ec53a6e4eae3cfa21eab7a8d5b731145f3a93ce876476173c17565b80c6e1
x530 & x530L	x530-5.5.4-2.5.rel	8b088cf38d26703af8ff8ce930279afce3b8619ad3b0d34f59ff9d5171ee03db

Table: Hash values for 5.5.4-2.5

Product family	Software File	Hash
x330	x330-5.5.4-2.5.rel	7eef979fb183a171a2f9dbdd001c66f9cfd27c17052b8fe6ac097711c4e4053
x320	x320-5.5.4-2.5.rel	8b088cf38d26703af8ff8ce930279afce3b8619ad3b0d34f59ff9d5171ee03db
x250	x250-5.5.4-2.5.rel	9294ea72cbf0648ae4a0b2dcfbb52c19001fc806245569e617e8397abc525c0d
x240	x240-5.5.4-2.5.rel	2c9a125ce0f457cbe9a4cbc5f2be76d7d5267c7db5fd4a5278065bde0668a69
x230 & x230L	x230-5.5.4-2.5.rel	bdf5428c06c44f4042a2e7983ad0a3207c5763d4a2d8493e716b0f1a6e27f87e
x220	x220-5.5.4-2.5.rel	7033216b55c4712ee3de045eb58d74d250de5ad846ba21c908b49c946d188304
IE360	IE360-5.5.4-2.5.rel	9c04b126b955299f19139f025ada47e778e9ffda75241c300572612dca2bd60d
IE340 & IE340L	IE340-5.5.4-2.5.rel	91f804063a192e711a5476fc56483ad09c4b5a8866e4704aa5bd91efb29cc2bf
IE220	IE220-5.5.4-2.5.rel	caee5c1d267c3eb871e962822828f9c39db26415e15b4ed6e8028f8073f80424
IE210L	IE210-5.5.4-2.5.rel	bdf5428c06c44f4042a2e7983ad0a3207c5763d4a2d8493e716b0f1a6e27f87e
SE540L	SE540-5.5.4-2.5.rel	ee7ec53a6e4eae3cfa21eab7a8d5b731145f3a93ce876476173c17565b80c6e1
SE250	SE250-5.5.4-2.5.rel	9294ea72cbf0648ae4a0b2dcfbb52c19001fc806245569e617e8397abc525c0d
SE240	SE240-5.5.4-2.5.rel	2c9a125ce0f457cbe9a4cbc5f2be76d7d5267c7db5fd4a5278065bde0668a69
XS900MX	XS900-5.5.4-2.5.rel	f6bb114fb8c01db6e4cee2785304753f4650f2d3a309d84575b1f311cd396186
GS980MX	GS980MX-5.5.4-2.5.rel	8b088cf38d26703af8ff8ce930279afce3b8619ad3b0d34f59ff9d5171ee03db
GS980EM	GS980EM-5.5.4-2.5.rel	8b088cf38d26703af8ff8ce930279afce3b8619ad3b0d34f59ff9d5171ee03db
GS980M	GS980M-5.5.4-2.5.rel	7033216b55c4712ee3de045eb58d74d250de5ad846ba21c908b49c946d188304
GS970EMX	GS970EMX-5.5.4-2.5.rel	7eef979fb183a171a2f9dbdd001c66f9cfd27c17052b8fe6ac097711c4e4053
GS970M	GS970-5.5.4-2.5.rel	bdf5428c06c44f4042a2e7983ad0a3207c5763d4a2d8493e716b0f1a6e27f87e
AR4050S-5G	AR4050S-5.5.4-2.5.rel	0532f40ce0267400cb8236a4f96f2cdb105ea0b0ac3807a289c5ca10aa252831
AR4050S	AR4050S-5.5.4-2.5.rel	0532f40ce0267400cb8236a4f96f2cdb105ea0b0ac3807a289c5ca10aa252831
AR3050S	AR3050S-5.5.4-2.5.rel	0532f40ce0267400cb8236a4f96f2cdb105ea0b0ac3807a289c5ca10aa252831
AR1050V	AR1050V-5.5.4-2.5.rel	40b76b287fdd871724c1873d26daded78cf41c8525ffeb535e2112531920a42a
TQ6702 GEN2-R	TQ6702GEN2R-5.5.4-2.5.rel	cdbb4442be083c7eadacbef91d968a3118bb29a315b90f329b178ac7a38246a2

# Licensing this Version on an SBx908 GEN2 Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a switch
- Obtain a release license for a switch
- Apply a release license on a switch
- Confirm release license application

## 1. Obtain the MAC address for a switch

A release license is tied to the MAC address of the switch.

Switches may have several MAC addresses. Use the **show system mac license** command to show the switch MAC address for release licensing:

```
awplus#show system mac license
MAC address for licensing:
eccd.6d9d.4eed
```

## 2. Obtain a release license for a switch

Contact your authorized Allied Telesis support center to obtain a release license.

## 3. Apply a release license on a switch

Use the **license certificate** command to apply a release license to your switch.

Note the license certificate file can be stored on internal flash memory, or an external SD card, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

## 4. Confirm release license application

On a stand-alone switch, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked switch, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches. The following example shows output on an SBx908 GEN2 switch:

```
awplus#show license

Board region: Global

Index          : 1
License name   : Base License
Customer name  : Base License
Type of license : Full
License issue date : 20-Mar-2024
Features included : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                   EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                   L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                   RADIUS-100, RIP, VCStack, VRRP

Index          : 2
License name   : 5.5.4
Customer name  : ABC Consulting
Quantity of licenses : 1
Type of license : Full
License issue date : 20-Mar-2024
License expiry date : N/A
Release       : 5.5.4
```

# Licensing this Version on an SBx8100 Series CFC960 Control Card

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a control card
- Obtain a release license for a control card
- Apply a release license on a control card
- Confirm release license application

If your CFC960 control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

## 1. Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license
MAC address for licensing:

Card                MAC Address
-----
1.5                 eccd.6d9e.3312
1.6                 eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

## 2. Obtain a release license for a control card

Contact your authorized Allied Telesis support center to obtain a release license.

## 3. Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

#### 4. Confirm release license application

On a stand-alone chassis, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked chassis, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus#show license
OEM Territory : ATI USA
Software Licenses
-----
Index                : 1
License name         : Base License
Customer name        : ABC Consulting
Quantity of licenses : 1
Type of license      : Full
License issue date   : 20-Mar-2024
License expiry date  : N/A
Features included    : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                    : Virtual-MAC, VRRP

Index                : 2
License name         : 5.5.4
Customer name        : ABC Consulting
Quantity of licenses : -
Type of license      : Full
License issue date   : 20-Mar-2024
License expiry date  : N/A
Release              : 5.5.4
```

# Installing this Software Version



**Caution:** This software version requires a release license for the SBx908 GEN2 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 61](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 63.](#)

To install and enable this software version on a switch or AR series device, use the following steps:

1. Copy the software version file (.rel) onto your TFTP server.
2. If necessary, delete or move files to create space in the switch’s Flash memory for the new file. To see the memory usage, use the command:

```
awplus# show file systems
```

To list files, use the command:

```
awplus# dir
```

To delete files, use the command:

```
awplus# del <filename>
```

You cannot delete the current boot file.

3. Copy the new release from your TFTP server onto the switch.

```
awplus# copy tftp flash
```

Follow the onscreen prompts to specify the server and file.

4. Move from Privileged Exec mode to Global Configuration mode, using:

```
awplus# configure terminal
```

Then set the switch to reboot with the new software version:

Product	Command
SBx8100 with CFC960	<code>awplus (config)# boot system SBx8100-5.5.4-2.5.rel</code>
SBx908 GEN2	<code>awplus (config)# boot system SBx908NG-5.5.4-2.5.rel</code>
x950 series	<code>awplus (config)# boot system x950-5.5.4-2.5.rel</code>
x930 series	<code>awplus (config)# boot system x930-5.5.4-2.5.rel</code>
x550 series	<code>awplus (config)# boot system x550-5.5.4-2.5.rel</code>
x540L series	<code>awplus (config)# boot system x540-5.5.4-2.5.rel</code>
x530 series	<code>awplus (config)# boot system x530-5.5.4-2.5.rel</code>
x330 series	<code>awplus (config)# boot system x330-5.5.4-2.5.rel</code>
x320 series	<code>awplus (config)# boot system x320-5.5.4-2.5.rel</code>
x250 series	<code>awplus (config)# boot system x250-5.5.4-2.5.rel</code>
x240 series	<code>awplus (config)# boot system x240-5.5.4-2.5.rel</code>
x230 series	<code>awplus (config)# boot system x230-5.5.4-2.5.rel</code>
x220 series	<code>awplus (config)# boot system x220-5.5.4-2.5.rel</code>

Product	Command
IE360 series	<code>awplus (config)# boot system IE360-5.5.4-2.5.rel</code>
IE340 series	<code>awplus (config)# boot system IE340-5.5.4-2.5.rel</code>
IE220 series	<code>awplus (config)# boot system IE220-5.5.4-2.5.rel</code>
IE210L series	<code>awplus (config)# boot system IE210-5.5.4-2.5.rel</code>
SE540L series	<code>awplus (config)# boot system SE540-5.5.4-2.5.rel</code>
SE250 series	<code>awplus (config)# boot system SE250-5.5.4-2.5.rel</code>
SE240 series	<code>awplus (config)# boot system SE240-5.5.4-2.5.rel</code>
XS900MX series	<code>awplus (config)# boot system XS900-5.5.4-2.5.rel</code>
GS980M series	<code>awplus (config)# boot system GS980M-5.5.4-2.5.rel</code>
GS980EM series	<code>awplus (config)# boot system GS980EM-5.5.4-2.5.rel</code>
GS980MX series	<code>awplus (config)# boot system GS980MX-5.5.4-2.5.rel</code>
GS970EMX series	<code>awplus (config)# boot system GS970EMX-5.5.4-2.5.rel</code>
GS970M series	<code>awplus (config)# boot system GS970-5.5.4-2.5.rel</code>
AR4050S-5G	<code>awplus (config)# boot system AR4050S-5.5.4-2.5.rel</code>
AR4050S	<code>awplus (config)# boot system AR4050S-5.5.4-2.5.rel</code>
AR3050S	<code>awplus (config)# boot system AR3050S-5.5.4-2.5.rel</code>
AR1050V	<code>awplus (config)# boot system AR1050V-5.5.4-2.5.rel</code>
ARX200S-GTX	<code>awplus (config)# boot system ARX200S-5.5.4-2.5.rel</code>
TQ6702 GEN2-R	<code>awplus (config)# boot system TQ6702GEN2R-5.5.4-2.5.rel</code>

Return to Privileged Exec mode and check the boot settings, using:

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

5. Reboot using the new software version.

```
awplus# reload
```

# Accessing and Updating the Web-based GUI

This section describes how to access the GUI to manage and monitor your AlliedWare Plus switch.

The GUI is a convenient tool for monitoring your device's status and performing basic management tasks. Its dashboard provides at-a-glance monitoring of traffic and other key metrics.

On AR4050S and AR3050S firewalls, you can use the GUI to create an advanced application-aware firewall with features such as Application control and Web control. Alternatively, you can configure real-time threat protection with URL filtering, Intrusion Prevention and Malware protection.

On select AlliedWare Plus devices, you can also optimize the performance of your Allied Telesis APs through Vista Manager mini.

## Browse to the GUI

**Note:** In version 5.5.2-2.1, AlliedWare Plus was enhanced so that only strong cipher suites can be used for accessing the Device GUI. This may prevent some very old browsers from accessing 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:

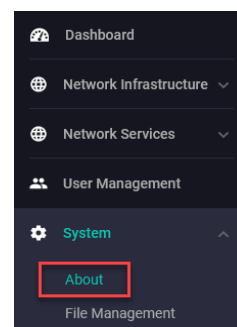
- « on switches: 169.254.42.42
- « on AR-Series: 192.168.1.1

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**. The version to use with 5.5.4-2.x is 2.20.0.

If you have an earlier version, update it as described in “Update the GUI on switches” on page 68 or “Update the GUI on AR-Series devices” on page 69.



## 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 GUI filename to use with AlliedWare Plus v5.5.4-2.x is `awplus-gui_554_38.gui`.

The file is not device-specific; the same file works on all devices. Make sure that the version string in the filename (e.g. 554) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

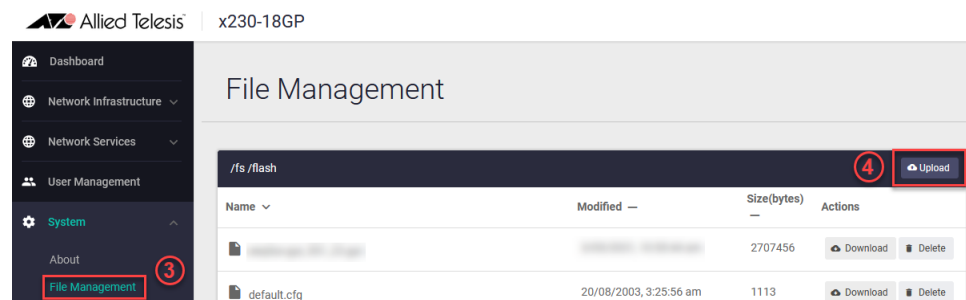
Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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 Support 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 **System > CLI** to access the command line interface, 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, then 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. Log into the GUI and use **System > CLI** to access the command line interface.
2. Use the following commands to download the new GUI:

```
awplus> enable  
awplus# update webgui now
```
3. Browse to the GUI and check that you have the latest version now, on the **System > About** page. You should have v2.20.0 or later.

