Release Notes

Allied Telesis™

AlliedWare Plus Software Version 5.5.5-2.x

- AMF Plus Cloud
- SBx81CFC960
- SBx908 GEN3
- 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
- IE560 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
- 10GbE UTM Firewall app
- ARX200S Series
- AR4000S-Cloud
- AR4050S-5G
- AR4050S
- AR3050S
- AR1050V
- TQR Series

5.5.5-2.1, 5.5.5-2.2, 5.5.5-2.3, 5.5.5-2.4

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/**
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**

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**

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**.

©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/**

Content

What's New in Version 5.5.5-2.4

Product families supported by this version:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 3
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 and x230L Series
x220 Series
IE560-12GSX
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series[1]
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall app
ARX200S Series
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQR Series

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-2.4.

Software file details for this version are listed in Table 1. 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 76.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 78. 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:

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		04/2046	vaa-5.5.5-2.4.iso (VAA OS) vaa-5.5.5-2.4.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-2.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	04/2026	SBx81CFC960-5.5.5-2.4.rel
SBx908 GEN3	SBx908 GEN3	04/2026	SBx90xGEN3-5.5.5-2.4.rel
SBx908 GEN2	SBx908 GEN2	04/2026	SBx908NG-5.5.5-2.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	04/2026	x950-5.5.5-2.4.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	04/2026	x930-5.5.5-2.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2026	x550-5.5.5-2.4.rel
x540L-28XTm x540L-28XS	x540L	04/2026	x540-5.5.5-2.4.rel

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

Models	Family	Date	Software File
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	04/2026	x530-5.5.5-2.4.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	04/2026	x530-5.5.5-2.4.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	04/2026	x330-5.5.5-2.4.rel
x320-10GH x320-11GPT	x320	04/2026	x320-5.5.5-2.4.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	04/2026	x250-5.5.5-2.4.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	04/2026	x240-5.5.5-2.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2026	x230-5.5.5-2.4.rel
x220-28GS x220-52GT x220-52GP	x220	04/2026	x220-5.5.5-2.4.rel
IE560-12GSX	IE560	04/2026	IE560-5.5.5-2.4.rel
IE360-12GTX IE360-12GHX	IE360	04/2026	IE360-5.5.5-2.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	04/2026	IE340-5.5.5-2.4.rel
IE220-6GHX IE220-10GHX	IE220	04/2026	IE220-5.5.5-2.4.rel
IE210L-10GP IE210L-18GP	IE210L	04/2026	IE210-5.5.5-2.4.rel
SE540L-28XTm SE540L-28XS	SE540L	04/2026	SE540-5.5.5-2.4.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	04/2026	SE250-5.5.5-2.4.rel
SE240-10GTXm SE240-10GHXm	SE240	04/2026	SE240-5.5.5-2.4.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	04/2026	XS900-5.5.5-2.4.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	04/2026	GS980MX-5.5.5-2.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	04/2026	GS980EM-5.5.5-2.4.rel
GS980M/52 GS980M/52PS	GS980M	04/2026	GS980M-5.5.5-2.4.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	04/2026	GS970EMX-5.5.5-2.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2026	GS970-5.5.5-2.4.rel
AR4000S-Cloud		04/2026	AR-4000S-Cloud-5.5.5-2.4.iso
ARX200S-GT ARX200S-GTX	ARX200S	04/2026	ARX200S-5.5.5-2.4.rel
10GbE UTM Firewall app		04/2026	ATVSTAPL-1.13.1.iso and vfw-x86_64-5.5.5-2.4.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	04/2026	AR4050S-5.5.5-2.4.rel AR3050S-5.5.5-2.4.rel
AR1050V	AR-Series VPN routers	04/2026	AR1050V-5.5.5-2.4.rel
TQ7613-R	TQR	04/2026	TQ7613R-5.5.5-2.4.rel
TQ7403-R	TQR	04/2026	TQ7403R-5.5.5-2.4.rel
TQ6702 GEN2-R	TQR	04/2026	TQ6702GEN2R-5.5.5-2.4.rel
TQ6702e GEN2-R	TQR	04/2026	TQ6702eGEN2R-5.5.5-2.4.rel
TQ3403-R	TQR	04/2026	TQ3403R-5.5.5-2.4.rel

Caution: Software version 5.5.5-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.5 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.5 license installed, that license also covers all later 5.5.5 versions. Such switches will not need a new license before upgrading to later versions.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Version on an SBx908 GEN2 Switch" on page 72.
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

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

The 5.5.5-2.4 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.5-2.4

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

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89023	**AMF**	Previously, when running AMF secure-mode the **`atmf working-set`** command may not have worked correctly after the AMF Master had renewed its AMF secure-mode certificate. 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-89087	**AMF**	Previously, the *Reboot Updated Devices* action in Vista Manager's firmware upgrade feature could, in rare cases, cause issues with AMF working sets. 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-89311	**AWC**	Previously, when an AP used the **wireless ap-configuration pull ap local** command to retrieve WPA-Enterprise AP profile settings (WPA2/WPA3 with CCMP or GCMP) from AWC, incorrect values were returned. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	-	Y	Y

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89312	**AWC**	Previously, the *beacon-protection* setting configured in the AP profile on the embedded wireless controller was not applied to the AP when the AP retrieved its configuration using the **wireless ap-configuration pull ap local** command from AWC. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	-	-	Y	Y	-	-	Y	Y
CR-89317	**AWC**	Previously, when an AP pulled its configuration from the embedded wireless controller using the **`wireless ap-configuration pull ap local`** command, the compatibility mode value defined in the AP profile was not applied to the AP. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	-	Y	Y
CR-89318	**AWC**	Previously, when the MAC filter configuration was deleted from an AP profile on the embedded wireless controller, the change was not applied to the AP when using the **wireless ap-configuration pull ap local** command. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	-	Y	Y

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89319	**AWC**	Previously, there were two issues affecting NTP on the embedded wireless controller: **1**. When the NTP configuration was removed from the AP-profile to apply the deletion to TQR, it was failing to be removed internally, which meant this change was not being applied to the AP via the pull command. **2**. When the **no ntp designated-server enable** command was configured in the embedded wireless controller AP profile and applied to the AP, the AP still attempted time synchronization, leading to unstable clock readings. These issues have been resolved. In addition, since the TQR models do not support the **ntp designated-server period** command, a default value of 10 is set when applying the AP profile to the TQR platforms.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	-	Y	Y
CR-89730	**AWC**	Previously, when an AP profile was configured with the **no initialization-button enable** command on the embedded wireless controller, the setting was not applied to the APs managed by that profile. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	-	Y	Y

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89320	**AWC**	Previously, the *max-clients* setting configured in the AP profile on the embedded wireless controller was not applied to the AP when using the **wireless ap-configuration pull ap local** command. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	-	Y	Y
CR-88570	**BGP**	Previously, configuring BGP aggregate summary routes with the **`as-set`** parameter option could invalidate internal data structures, resulting in a system reboot and undefined behavior. 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
CR-89178	**BGP**	Previously, a change made under an earlier CR (CR-81867) introduced a separate issue where BGP instances which only had neighbours configured with peer-groups and no individual peers could fail to open the TCP listening socket for BGP, resulting in the peers failing to ever establish. 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
CR-88472	**BGP, VCStacking**	Previously, following a stack failover, BGP peers configured as passive could incorrectly initiate an outgoing TCP connection. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89679	**CCC**	Previously, if the cloud-client feature stopped unexpectedly, the device could restart rather than trying to restart the feature itself. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	-	-	-	-	Y	-	-	-	Y	-	-	-	Y	-	-	-	-	Y	Y	-	Y	Y	Y	Y	-	-	-	-	-	-	-
CR-89890	**Device GUI, API**	You can now set the URL filter check interval through the Device GUI. Previously, this option did not function correctly due to an API request formatting issue.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	Y	Y
ER-7454	**DNS Server**	With this software release, it is now possible to specify the IP source address and/or egress interface for DNS forwarding, configurable per domain server using the command below: **`ip name-server <addr> [suffix-list <domain-list>] [source-address <src-addr>] [interface <ifname>]`**	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-89449	**EPSR, BFD**	Previously, a problem with the BFD ACL MAC mask could prevent BFD packets from being forwarded in some cases. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	Y	Y	Y	-	-	Y	-	-	Y	-

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89001	**HTTP service**	Previously, configuring **HTTP port none** or **HTTP secure-port none** could result in high CPU load. 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
CR-88914	**HTTP Service**	Previously, when the HTTP service was running without being bound to a specific IPv4 or IPv6 address, and the device had at least one IPv6 interface configured, IP or IPv6 address changes could cause brief, unintended service interruptions. 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
CR-89133	**Mail/CLI**	Previously, when executing the **`mail`** command, due to a software error it was possible to delete the recipient "To:" prompt. 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-88632	**Multicast Forwarding**	Previously, learning large numbers of multicast streams on the SBx908Gen3 could take longer than expected. The **`platform multicast-ratelimit 500`** command could be used to improve learning time, and this value is now the default under this CR, resulting in faster multicast stream learning. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
ER-7453	**NTP**	DHCP and DHCPv6 are able to dynamically assign IP addresses, as well as additional configuration for the client, such as an NTP server address. With this change, support has been added to dynamically receive an NTP server address automatically over the network via DHCPv6. 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
CR-88979	**PKI**	Previously, the **est-url** command was incorrectly not accepting IPv6 addresses, preventing EST servers using IPv6 from working. 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
CR-87197	**PoE**	Previously, the HANP `"last negotiated"` timestamps were not being displayed for affected platforms. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-89110	**PoE**	Previously, the PoE amber LED would incorrectly be turned off when an over-current event occurred on a port. This issue has now been resolved. Additionally the **show power-inline** command output now displays the correct status of `"denied"` in this situation.	-	-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	Y	Y	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89323	**Policy Based Routing**	Previously, certain specific valid IP addresses (x.x.x.127, x.x.x.224-239) were incorrectly being deemed as invalid, while other specific invalid addresses (127.x.x.x, 224-239.x.x.x) were incorrectly being deemed as valid, when set as the next hop for policy-based-routing. This occurred due to an incorrect byte-order (endianness) calculation when validating IP addresses. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	Y
CR-89112	**Port Authentication**	Previously, when acting as a NAS, affected platforms would occasionally fail to forward traffic from a supplicant that had recently roamed. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-87694	**Port Configuration**	Previously during boot up, on rare occasions a port may have failed to link up on affected platforms. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89160	**Private VLAN, UFO**	Previously, when a Private VLAN Unknown Unicast Flooding Only (UFO) interface was configured on an interface, either in access or trunk mode, the **show interface status** command output would display "unknown" for the Vlan ID field. This issue has now been resolved, and the Vlan field of the **`show interface status`** command now displays "**`trunk`**" for trunked interfaces, or the VLAN number for access interfaces. 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	-	-	-	-	-	-	-
CR-88679	**RMON, WebAPI**	Previously, when configuring RMON collection on a device via the WebAPI (for example, via Vista Manager), an additional **`owner`** parameter could be added to the device running configuration. If the configuration was saved and the device rebooted, an error would occur during boot because the invalid **`owner`** parameter was rejected. 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	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89740	**SMTP, OAuth**	Previously, it was not possible to use OAuth codes that were >1024 characters (such as those generated by Microsoft) due to the limit being set too low. This issue is now resolved, and auth codes larger than 1024 characters are now supported. ISSU: Effective when CFCs upgraded.	Y	Y	-	-	-	Y	Y	Y	-	-	-	-	-	Y	Y	-	-	-	Y	-	Y	-	-	-	-	-	-	-	-	-	-	-	-
CR-89749	**SMTP, OAuth**	Previously, when OAuth for email was enabled the device console would periodically freeze up for small periods, and an error message could be generated. This issue has been resolved, and the console freeze and error message no longer occur. ISSU: Effective when CFCs upgraded.	Y	Y	-	Y	-	-	-	-	-	-	Y	Y	-	-	-	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-
CR-88931	**Software Licensing**	Previously, subscription licenses distributed with .lic file extensions that were for permanent features, such as MACsec, could be incorrectly rejected when applied to the system with an error: "% Error: The file is invalid." This issue has been resolved. Now, permanent .lic subscription licenses can be installed as expected. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	Y	Y	-	Y	Y	-	-	Y	Y	-	-	Y	-	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89124	**Software Licensing**	Previously, subscription licenses distributed with .lic file extensions that were installed onto the system would be erased by the **erase factory-default** command and would no longer appear in the output of **show license external** due to a software bug. This issue has now been resolved. Additionally, the warning prompt that is displayed when executing the **erase factory-default** command has been updated to more accurately describe the impact of the command. The new warning prompt is: *This command will erase all NVS, all flash contents except for the boot release, a GUI resource file, and installed licenses, and then reboot the device.* *Proceed ? (y/n):* 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-89729	**SSH, File System**	Previously, deleting existing users from the local user database and then creating a new user configured for SSH access could result in SSH login failures after saving the configuration and rebooting. 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	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2 / x908GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-86804	**Switchports**	Previously, on rare occasions, fiber pluggables connected to an XEM2-12XSv2 could experience elevated FCS errors. The software now monitors for this condition and automatically resets the port to restore normal operation.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	-	-	-	-	-	-
CR-89417	**System**	Previously, certain specific serial numbers of PWR600 could fail to be recognized by AlliedWare Plus due to a parsing error of the PSU checksum. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-
CR-88594	**TCP**	Previously, an internal driver issue could cause TCP retransmissions to be stalled. This issue is now resolved. ISSU: Effective when CFCs upgraded.	-	-	Y	Y	Y	-	-	-	-	-	Y	-	Y	Y	-	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	-	-	-	-	-	-	-
CR-87507	**VCStack**	Previously, in rare cases when a backup stack member was rebooted, if the stack master happened to be trying to retrieve **`show stack`** related command output from the member being rebooted, it could get stuck and not correctly process the member leaving the stack, and could result in a duplicate master when the member rejoined. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-

What's New in Version 5.5.5-2.3

Product families supported by this version:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 3
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 and x230L Series
x220 Series
IE560-12GSX
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series[1]
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall app
ARX200S Series
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQR Series

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-2.3.

Software file details for this version are listed in Table 1. 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 76.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 78. 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:

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		02/2026	vaa-5.5.5-2.3.iso (VAA OS) vaa-5.5.5-2.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-2.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	02/2026	SBx81CFC960-5.5.5-2.3.rel
SBx908 GEN3	SBx908 GEN3	02/2026	SBx90xGEN3-5.5.5-2.3.rel
SBx908 GEN2	SBx908 GEN2	02/2026	SBx908NG-5.5.5-2.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	02/2026	x950-5.5.5-2.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	02/2026	x930-5.5.5-2.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	02/2026	x550-5.5.5-2.3.rel
x540L-28XTm x540L-28XS	x540L	02/2026	x540-5.5.5-2.3.rel

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

Models	Family	Date	Software File
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	02/2026	x530-5.5.5-2.3.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	02/2026	x530-5.5.5-2.3.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	02/2026	x330-5.5.5-2.3.rel
x320-10GH x320-11GPT	x320	02/2026	x320-5.5.5-2.3.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	02/2026	x250-5.5.5-2.3.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	02/2026	x240-5.5.5-2.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	02/2026	x230-5.5.5-2.3.rel
x220-28GS x220-52GT x220-52GP	x220	02/2026	x220-5.5.5-2.3.rel
IE560-12GSX	IE560	02/2026	IE560-5.5.5-2.3.rel
IE360-12GTX IE360-12GHX	IE360	02/2026	IE360-5.5.5-2.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	02/2026	IE340-5.5.5-2.3.rel
IE220-6GHX IE220-10GHX	IE220	02/2026	IE220-5.5.5-2.3.rel
IE210L-10GP IE210L-18GP	IE210L	02/2026	IE210-5.5.5-2.3.rel
SE540L-28XTm SE540L-28XS	SE540L	02/2026	SE540-5.5.5-2.3.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	02/2026	SE250-5.5.5-2.3.rel
SE240-10GTXm SE240-10GHXm	SE240	02/2026	SE240-5.5.5-2.3.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	02/2026	XS900-5.5.5-2.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	02/2026	GS980MX-5.5.5-2.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	02/2026	GS980EM-5.5.5-2.3.rel
GS980M/52 GS980M/52PS	GS980M	02/2026	GS980M-5.5.5-2.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	02/2026	GS970EMX-5.5.5-2.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	02/2026	GS970-5.5.5-2.3.rel
AR4000S-Cloud		02/2026	AR-4000S-Cloud-5.5.5-2.3.iso
ARX200S-GT ARX200S-GTX	ARX200S	02/2026	ARX200S-5.5.5-2.3.rel
10GbE UTM Firewall app		02/2026	ATVSTAPL-1.13.1.iso and vfw-x86_64-5.5.5-2.3.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	02/2026	AR4050S-5.5.5-2.3.rel AR3050S-5.5.5-2.3.rel
AR1050V	AR-Series VPN routers	02/2026	AR1050V-5.5.5-2.3.rel
TQ7613-R	TQR	02/2026	TQ7613R-5.5.5-2.3.rel
TQ7403-R	TQR	02/2026	TQ7403R-5.5.5-2.3.rel
TQ6702 GEN2-R	TQR	02/2026	TQ6702GEN2R-5.5.5-2.3.rel
TQ6702e GEN2-R	TQR	02/2026	TQ6702eGEN2R-5.5.5-2.3.rel
TQ3403-R	TQR	02/2026	TQ3403R-5.5.5-2.3.rel

Caution: Software version 5.5.5-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.5 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.5 license installed, that license also covers all later 5.5.5 versions. Such switches will not need a new license before upgrading to later versions.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Version on an SBx908 GEN2 Switch" on page 72.
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

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

The 5.5.5-2.3 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.5-2.3

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

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2 / x908Gen3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-87948	**AMF**	Previously, in AMF topologies with AMF Cross-links connected to leaf nodes, in some circumstances duplicate node ID scenarios were not being handled correctly resulting in the affected node not joining the AMF network. 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	-	-	-	-	-	-	-
CR-88810	**AWC-Lite, Wireless**	Previously, entering the command **`wireless ap-configuration pull ap local`** followed by a **`"?"`** for the help menu, could result in a system reboot. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	Y	-	Y	Y	-	-	-	Y
CR-88930	**DHCP Client, CCC Client**	Previously, if CCC auto-config failed on a factory clean device, the IP address assigned by DHCP on the interface for bootstrapping was lost. This issue has now been resolved. Now if CCC auto-config fails the IP address assigned by DHCP during auto-config persists. 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	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2 / x908Gen3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-89001	**HTTP Service**	Previously, configuring **HTTP port none** or **HTTP secure-port none** could result in high CPU load. 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-88940	**Logging**	Previously, if you ran **no shutdown** on a static aggregator member port while its aggregator was shut down, the command would fail and create a flood of syslog messages 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	-	-	-	-
CR-88960	**Mail**	Previously, it was possible to backspace and delete the subject field when using the **mail to** command. 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-89041	**PKI**	Previously, for affected platforms the enrollment timer for certificates using EST or SCEP was not being restarted after 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	-
ER-71067	**SSH**	OpenSSH has been upgraded to 10.2p1 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	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2 / x908Gen3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-88717	**Storm Control**	Previously, the **`storm-control`** command was not accepted for certain ports on SBx908 GEN3. This issue is now resolved, and storm-control is able to be configured on all ports.	-	-	-	-	-	Y	-	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-
CR-87729	**Switching**	Previously, when a port was shut down on affected platforms, it was possible for another port (on the same PHY) to lose a packet. This issue has been resolved	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-77657	**System, LEDs**	Previously, the USB LED on affected platforms was not operating correctly when a USB device was connected. The expected behaviour of the USB LED is for it to be on when a USB device is detected and flashing when the device is accessed. This issue has been resolved	-	-	Y	-	Y	-	-	-	-	-	-	-	-	Y	Y	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-88331	**VCStack**	Previously, when a VCStack member was rebooted, an unexpected reboot could occur on the VCStack master. 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	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2 / x908Gen3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-88875	**VCStack**	Previously, interface counters for every port were being queried when syncing the PoE path in apteryx, resulting in an unnecessarily high level of hardware lookups which increased system load. The increased system load could cause this call to timeout on large stacks with many ports, resulting in the PoE sync failing to complete and error logs generated. This issue has been resolved. ISSU: Effective when CFCs upgraded	-	-	-	-	Y	-	-	-	-	-	-	-	Y	-	-	Y	-	-	-	Y	Y	Y	Y	-	Y	-	-	-	-	-	-	-	-
CR-88819	**VCStack**	Previously, on rare occasions, it was possible for a system reboot to occur on a backup member when performing a rolling reboot of a VCStack. This issue has been resolved.	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	Y	Y	-	Y	-	-	-	-	-	-	-
CR-88875	**VCStack**	Previously, interface counters for every port were being queried when syncing the PoE path in apteryx, resulting in an unnecessarily high level of hardware lookups which increased system load. The increased system load could cause this call to timeout on large stacks with many ports, resulting in the PoE sync failing to complete and error logs generated. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	Y	-	-	-	-	-	-	Y	-	Y	-	-	Y	-	-	-	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-	-

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2 / x908Gen3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-88819	**VCStack**	Previously, on rare occasions, it was possible for a system reboot to occur on a backup member when performing a rolling reboot of a VCStack. This issue has been resolved.	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	Y	Y	-	Y	-	-	-	-	-	-	-
CR-88708	**VCStack, ACL**	Previously, during configuration replay on bootup, if a switchport was configured with **`access-group x`** for a non-existent ACL, in rare cases this could result in another ACL being lost from the configuration on that stack member. 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	-	-	-	-	-	-	-

What's New in Version 5.5.5-2.2

Product families supported by this version:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 3
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 and x230L Series
x220 Series
IE560-12GSX
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series[1]
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall app
ARX200S Series
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQR Series

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-2.2.

Software file details for this version are listed in Table 1. 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 76.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 78. 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:

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		12/2025	vaa-5.5.5-2.2.iso (VAA OS) vaa-5.5.5-2.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-2.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	12/2025	SBx81CFC960-5.5.5-2.2.rel
SBx908 GEN3	SBx908 GEN3	12/2025	SBx90xGEN3-5.5.5-2.2.rel
SBx908 GEN2	SBx908 GEN2	12/2025	SBx908NG-5.5.5-2.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	12/2025	x950-5.5.5-2.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	12/2025	x930-5.5.5-2.2rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	12/2025	x550-5.5.5-2.2.rel
x540L-28XTm x540L-28XS	x540L	12/2025	x540-5.5.5-2.2.rel

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

Models	Family	Date	Software File
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	12/2025	x530-5.5.5-2.2.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	12/2025	x530-5.5.5-2.2.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	12/2025	x330-5.5.5-2.2.rel
x320-10GH x320-11GPT	x320	12/2025	x320-5.5.5-2.2.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	12/2025	x250-5.5.5-2.2.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	12/2025	x240-5.5.5-2.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	12/2025	x230-5.5.5-2.2.rel
x220-28GS x220-52GT x220-52GP	x220	12/2025	x220-5.5.5-2.2.rel
IE560-12GSX	IE560	12/2025	IE560-5.5.5-2.2.rel
IE360-12GTX IE360-12GHX	IE360	12/2025	IE360-5.5.5-2.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	12/2025	IE340-5.5.5-2.2.rel
IE220-6GHX IE220-10GHX	IE220	12/2025	IE220-5.5.5-2.2.rel
IE210L-10GP IE210L-18GP	IE210L	12/2025	IE210-5.5.5-2.2.rel
SE540L-28XTm SE540L-28XS	SE540L	12/2025	SE540-5.5.5-2.2.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	12/2025	SE250-5.5.5-2.2.rel
SE240-10GTXm SE240-10GHXm	SE240	12/2025	SE240-5.5.5-2.2.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	12/2025	XS900-5.5.5-2.2.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	12/2025	GS980MX-5.5.5-2.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	12/2025	GS980EM-5.5.5-2.2.rel
GS980M/52 GS980M/52PS	GS980M	12/2025	GS980M-5.5.5-2.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	12/2025	GS970EMX-5.5.5-2.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	12/2025	GS970-5.5.5-2.2.rel
AR4000S-Cloud		12/2025	AR-4000S-Cloud-5.5.5-2.2.iso
ARX200S-GT ARX200S-GTX	ARX200S	12/2025	ARX200S-5.5.5-2.2.rel
10GbE UTM Firewall app		12/2025	ATVSTAPL-1.13.1.iso and vfw-x86_64-5.5.5-2.2.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	12/2025	AR4050S-5.5.5-2.2.rel AR3050S-5.5.5-2.2.rel
AR1050V	AR-Series VPN routers	12/2025	AR1050V-5.5.5-2.2.rel
TQ7613-R	TQR	12/2025	TQ7613R-5.5.5-2.2.rel
TQ7403-R	TQR	12/2025	TQ7403R-5.5.5-2.2.rel
TQ6702 GEN2-R	TQR	12/2025	TQ6702GEN2R-5.5.5-2.2.rel
TQ6702e GEN2-R	TQR	12/2025	TQ6702eGEN2R-5.5.5-2.2.rel
TQ3403-R	TQR	12/2025	TQ3403R-5.5.5-2.2.rel

Caution: Software version 5.5.5-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.5 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.5 license installed, that license also covers all later 5.5.5 versions. Such switches will not need a new license before upgrading to later versions.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Version on an SBx908 GEN2 Switch" on page 72.
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

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

The 5.5.5-2.2 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.5-2.2

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

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2 / x908Gen3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
OAUTHS MTP-16	**Mail**	**Enhancement** AlliedWare Plus version 5.5.5-2.2 supports OAuth 2.0 for Google and Microsoft Mail Client. For more information, see the Mail (SMPT) Feature Overview and Configuration Guide.	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-88814	**MRP**	Previously, when MRP was configured on a port, spanning-tree would be disabled. However, when MRP was removed from the port, spanning-tree was not being re-enabled. This issue has been resolved.	-	-	-	-	-	Y	-	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-
CR-88510	**OpenFlow**	Previously on the SBx908 GEN3, Openflow incorrectly showed a maximum speed of 0 for interfaces capable of 25G, or 400G. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-
CR-88315	**PKI**	Previously, reloading new PKI certificates required manual intervention to restart the HTTP server. This issue is now resolved, and the HTTP server automatically restarts to apply the updated certificates. ISSU: Effective when CFC 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

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2 / x908Gen3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-88713	**PPP, USB Modem**	Previously, when a PPP interface on a USB modem was shut down, the interface was not being stopped correctly, which meant that it could not be restarted again without rebooting the device. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	-
ER-7350	**USB Modem**	**Enhancement** This enhancement adds support on the ARX200S for the NCXX UX302NC USB modem.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-
CR-88345	**VCStack**	Previously, if a VCStack member left the stack during the processing of a config update, the interface configuration for that stack member would be missing after the VCStack member rejoined. This issue is now resolved, and the interface configuration is retained and applied correctly once the member rejoins. ISSU: Effective when CFC ISSU complete.	Y	Y	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	-	-	-	-	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-
CR-88830	**VLAN**	Previously, configuring and de-configuring VLANs could result in a small memory leak. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	-

What's New in Version 5.5.5-2.1

Product families supported by this version:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 3
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 and x230L Series
x220 Series
IE560-12GSX
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series1
SE240 Series1
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall app
ARX200S Series
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQR Series

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-2.1.

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 76.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 78. 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:

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		11/2025	vaa-5.5.5-2.1.iso (VAA OS) vaa-5.5.5-2.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-2.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2025	SBx81CFC960-5.5.5-2.1.rel
SBx908 GEN3	SBx908 GEN3	11/2025	SBx90xGEN3-5.5.5-2.1.rel
SBx908 GEN2	SBx908 GEN2	11/2025	SBx908NG-5.5.5-2.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	11/2025	x950-5.5.5-2.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	11/2025	x930-5.5.5-2.1rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2025	x550-5.5.5-2.1.rel
x540L-28XTm x540L-28XS	x540L	11/2025	x540-5.5.5-2.1.rel

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

Models	Family	Date	Software File
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	11/2025	x530-5.5.5-2.1.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	11/2025	x530-5.5.5-2.1.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	11/2025	x330-5.5.5-2.1.rel
x320-10GH x320-11GPT	x320	11/2025	x320-5.5.5-2.1.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	11/2025	x250-5.5.5-2.1.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	11/2025	x240-5.5.5-2.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2025	x230-5.5.5-2.1.rel
x220-28GS x220-52GT x220-52GP	x220	11/2025	x220-5.5.5-2.1.rel
IE560-12GSX	IE560	11/2025	IE560-5.5.5-2.1.rel
IE360-12GTX IE360-12GHX	IE360	11/2025	IE360-5.5.5-2.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	11/2025	IE340-5.5.5-2.1.rel
IE220-6GHX IE220-10GHX	IE220	11/2025	IE220-5.5.5-2.1.rel
IE210L-10GP IE210L-18GP	IE210L	11/2025	IE210-5.5.5-2.1.rel
SE540L-28XTm SE540L-28XS	SE540L	11/2025	SE540-5.5.5-2.1.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	11/2025	SE250-5.5.5-2.1.rel
SE240-10GTXm SE240-10GHXm	SE240	11/2025	SE240-5.5.5-2.1.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	11/2025	XS900-5.5.5-2.1.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	11/2025	GS980MX-5.5.5-2.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2025	GS980EM-5.5.5-2.1.rel
GS980M/52 GS980M/52PS	GS980M	11/2025	GS980M-5.5.5-2.1.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	11/2025	GS970EMX-5.5.5-1.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2025	GS970-5.5.5-2.1.rel
AR4000S-Cloud		11/2025	AR-4000S-Cloud-5.5.5-2.1.iso
ARX200S-GT ARX200S-GTX	ARX200S	11/2025	ARX200S-5.5.5-2.1.rel
10GbE UTM Firewall app		11/2025	ATVSTAPL-1.13.1.iso and vfw-x86_64-5.5.5-2.1.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	11/2025	AR4050S-5.5.5-2.1.rel AR3050S-5.5.5-2.1.rel
AR1050V	AR-Series VPN routers	11/2025	AR1050V-5.5.5-2.1.rel
TQ7613-R	TQR	11/2025	TQ7613R-5.5.5-2.1.rel
TQ7403-R	TQR	11/2025	TQ7403R-5.5.5-2.1.rel
TQ6702 GEN2-R	TQR	11/2025	TQ6702GEN2R-5.5.5-2.1.rel
TQ6702e GEN2-R	TQR	11/2025	TQ6702eGEN2R-5.5.5-2.1.rel
TQ3403-R	TQR	11/2025	TQ3403R-5.5.5-2.1.rel

Caution: Software version 5.5.5-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.5 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.5 license installed, that license also covers all later 5.5.5 versions. Such switches will not need a new license before upgrading to later versions.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Version on an SBx908 GEN2 Switch" on page 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

The SBx908 GEN3 switch does not require a release license.

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

The 5.5.5-2.1 software version is **not** ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.5-2.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 70.

Changes to AMF Plus software version compatibility

Applies to all devices running AMF Plus

From version 5.5.5-2.1 onwards, improvements in AMF Plus security mean that earlier versions are not fully compatible with recent versions. If you upgrade part of your network, you need to upgrade it all. See "AMF Plus software version compatibility" on page 65 for details.

EST certificate management

Applies to all devices running AlliedWare Plus

From version 5.5.5-2.1 onwards, AlliedWare Plus supports Enrollment over Secure Transport (EST) certificate management. EST allows certificates to be signed over a secure HTTP channel. These certificates will be renewed automatically, greatly reducing the maintenance burden of keeping certificates valid on network devices.

How to create a trustpoint based on a certificate signed over EST

Use the following steps to create a trustpoint based on an EST service. This example creates a trustpoint named 'timaru'.

1. Enter configuration mode.

```
awplus> enable
awplus# configure terminal
```

Note that PKI commands require maximum user privileges to execute.

2. Declare a trustpoint named 'timaru' and enter trustpoint configuration mode.

```
awplus(config)# crypto pki trustpoint timaru
```

You can use any name for the trustpoint, so long as the first character is alphanumeric, and all characters are alphanumeric, underscores, dashes, or periods.

Do not use the names 'local', 'default-selfsigned' or 'default-system' for the trustpoint. These names have special meanings. For all other trustpoint names, this command just instantiates the trustpoint by initializing its storage container.

3. Declare that the trustpoint will use an EST server for signing.

```
awplus(ca-trustpoint)# enrollment est
```

This command affects the process, but doesn't immediately cause any action to be taken. In other words, this command does not result in certificate generation; it only affects how certificate generation will be done later.

4. Specify the EST server to communicate with.

```
awplus(ca-trustpoint)# est-url https://est.example.com:8443
```

5. Enter the username and password for communicating with the EST server.

These commands are required if the EST server requires authentication.

```
awplus(ca-trustpoint)# est-username timaru-user
awplus(ca-trustpoint)# est-password timaru-password
```

6. Declare the keypair that the trustpoint will use.

```
awplus(ca-trustpoint)# rsakeypair timaru-server-key
```

This step specifies that the trustpoint uses the key pair 'timaru-server-key' when enrolling the server (creating its certificate). This command does not create the key pair. If the key pair does not exist, it is created later when you run the **crypto pki enroll** command. You can specify the key length here, but if the key already exists with a different length, the parameter is ignored.

7. Leave trustpoint configuration mode.

```
awplus(ca-trustpoint)# end
```

8. If necessary, install the certificate authority (CA) used to sign the root certificate.

```
awplus# crypto pki import default-system
```

If the certificate the server uses for TLS was not signed by one of the default set of root CA certificates, then the CA used to sign that certificate must be installed as a trusted root CA certificate.

9. Retrieve the CA certificate that the EST server will use to sign the server certificate.

```
awplus# crypto pki authenticate timaru
```

10. Create the server certificate.

```
awplus# crypto pki enroll timaru
```

This command creates the server certificate. This is a single-step process for a trustpoint with an EST certificate authority. This process:

- Creates the server certificate for the local device using the RSA key pair specified in the trustpoint parameters.
- Generates the key pair if the key pair specified in the **rsakeypair** command does not exist.
- Creates a new key pair named after the trustpoint if the **rsakeypair** command was not executed for this trustpoint.

By default, the subject name of the server certificate has the CN (common name) field set to the fully qualified domain name of the system, since that is commonly required when other systems validate the subject name. However, you can substitute a subject name of your choice by using the **subject** command in trustpoint-configuration mode. The device will then communicate with the EST server to have its own server certificate signed.

At this point, the trustpoint is set up. It contains the:

- trustpoint's EST root CA certificate
- root RSA public/private keys
- trustpoint's own server certificate, signed by the EST root CA certificate.

Change to how sysName MIB value is set

From version 5.5.5-2.1 onwards, the **hostname** command no longer sets the sysName MIB value. Instead, use the following new command to set the MIB value:

```
awplus(config)# snmp-server system-name
```

Note that the new **snmp-server system-name** command does not set the hostname. The hostname and the sysName MIB value are now independent of each other.

Support for @ character in usernames

Applies to all devices that run AlliedWare Plus

From version 5.5.5-2.1 onwards, usernames in a device's local user database can include the @ character. This also makes it possible to use @ in the username when logging into the device with RADIUS user authentication. Note that you can only use an @ character in the middle of the username, not at the beginning or end.

For more information about usernames, see Getting Started with the AlliedWare Plus Command Line Interface.

SBx908 GEN3 enhancements

Version 5.5.5-2.1 onwards supports the following enhancements on SBx908 GEN3 switches.

Bulk firmware upgrades using AMF Plus

From version 5.5.5-2.1 onwards, it is possible for all AMF Plus master nodes to use the AMF Plus bulk firmware upgrade processes to upgrade SBx908 GEN3 switches. Previously, only an SBx908 GEN3 master could use these AMF Plus processes to upgrade other SBx908 GEN3 switches.

There are two bulk upgrade processes:

- 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.

For more information about AMF Plus, see the AMF Plus and AMF Feature Overview and Configuration Guide.

Multiple mirror ports

From version 5.5.5-2.1 onwards, the SBx908 GEN3 supports multiple mirror ports. You can also configure an aggregator as the mirror port.

For more information about mirroring, see the Mirroring Feature Overview and Configuration Guide.

Precision Time Protocol

From version 5.5.5-2.1 onwards, the SBx908 GEN3 supports the end-to-end (e2e) delay mechanism in PTP Transparent Clock.

Precision Time Protocol (PTP) is an Ethernet or IP-based protocol for synchronizing time clocks on a collection of network devices using a Transmitter/Receiver distribution mechanism.

For more information, see the Precision Time Protocol (PTP) and Transparent Clock Feature Overview and Configuration Guide.

DoS attack prevention support

From software version 5.5.5-2.1 onwards, the SBx908 GEN3 supports Denial of Service (DoS) attack prevention. Six different DoS attacks can be detected: IP Options, Land, Ping-of-Death, Smurf, Synflood, and Teardrop.

When the attack is detected, three different actions are available:

1. Shut down the port for one minute
2. Cause an SNMP trap
3. Send traffic to the mirror port

Syntax `dos {ipoptions|land|ping-of-death|smurf broadcast <ip-address>|synflood|teardrop} action {shutdown|trap|mirror}`

For example, to configure ping-of-death DoS detection on port1.1.1, and shut down the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.1.1
awplus(config-if)# dos ping-of-death action shutdown
```

By default, DoS attack detection is not configured on any switch port interface.

Support for more route entries

From version 5.5.5-2.1 onwards, you can increase the number of Layer 3 route entries the SBx908 GEN3 supports. This is done through a new silicon profile called profile1. The following table shows the differences between the default silicon profile and the new profile.

Item	Default profile	Profile1
IPv4 routes	16K	60K
IPv6 routes	8K	30K
Forwarding database (FDB) entries	256K	128K

The FDB entries are split between L2 and L3 as shown in the following table, depending on whether fdb-l3-hosts mode is enabled or not:

Profile	When fdb-l3-hosts is enabled (default)		When fdb-l3-hosts is disabled	
	L2	L3	L2	L3
Default	160K	96K + 16K route entries	256K	16K from route entries
Profile1	96K	32K + 16K route entries	128K	16K from route entries

Commands To enable the new silicon profile, use the command:

```
awplus(config)# platform silicon-profile profile1
```

To enable fdb-l3-hosts mode, use the command:

```
awplus(config)# platform fdb-l3-hosts
```

After using either of these commands, save the configuration and reboot the switch.

To see whether the new silicon profile is enabled or not, use the command:

```
awplus# show platform
```

Up to 600 VRF-lite instances

From version 5.5.5-2.1 onwards, the SBx908 GEN3 supports up to 600 VRF-lite instances, when using silicon profile 1. The default silicon profile supports approximately 63 instances.

To enable silicon profile 1, use the command:

```
awplus(config)# platform silicon-profile profile1
```

For more information about enabling and configuring VRF-lite, see the VRF-lite Feature Overview and Configuration Guide.

Turn off speed autonegotiation on XEM3-8CQ

From version 5.5.5-2.1 onwards, the SBx908 GEN3 supports a fixed speed of 40G on the XEM3-8CQ module. This enables the module's ports to interoperate with the 40G ports on the SBx81XLEM/Q2.

To configure this, go into Interface Configuration mode for the desired port and use the command:

```
awplus(config-if)# speed 40000
```

Note that these ports always use full duplex, so you do not have to specify the duplex setting.

Enhanced Transmission Selection (ETS)

Support for up to 12 QoS scheduler-sets applies to:

- *SBx908 GEN3, x540L, SE540, x530, x530L, GS980MX, x250, SE250, x240, and SE240 Series switches*

Support for:

- *configuring a WRR weight of a QoS scheduler-set with a minimum weight of 1*
- *the percent keyword*

applies to SBx908 GEN3, SBx8100, x540L, SE540, x530, x530L, GS980MX, x250, SE250, x240, SE240, x320, GS980EM, x220, and GS980M Series switches

From version 5.5.5-2.1 onwards, you can configure WRR groups using percentage-based weights. In addition, the ranges for sets and weights have been updated. This is part of work to implement Enhanced Transmission Selection (ETS) in our devices.

ETS is a traffic management feature defined in the IEEE 802.1Qaz standard. It helps network switches manage how different types of traffic share bandwidth on a single physical link. ETS works alongside other Data Center Bridging (DCB) technologies to improve performance in data center environments.

At its core, ETS allows administrators to assign minimum bandwidth guarantees to different traffic classes as a percentage of link bandwidth. This ensures that critical applications always get the resources they need, even when the network is busy. ETS also supports bandwidth sharing when some traffic classes are idle, helping to make the most of available capacity.

New Commands

To configure a WRR group with percentage-based weights, use the following command:

```
awplus(config)# mls qos scheduler-set <1-12> wrr-queue group
<1-2> percent <1-100> queues [0][1][2][3][4][5][6][7]
```

For example, to configure wrr-queue group 2 applying a 25% weight to queues 0 and 1 for scheduler-set 1, use the commands:

```
awplus# configure terminal
awplus(config)# mls qos scheduler-set 1 wrr-queue group 2
percent 25 queues 0 1
```

To configure wrr-queue group 2 applying a 50% weight to queue 2 for scheduler-set 1, use the commands:

```
awplus# configure terminal
awplus(config)# mls qos scheduler-set 1 wrr-queue group 2
percent 50 queues 2
```

The switch will empty twice as many packets from queue 2 as it will from queues 0 and 1.

Updated Commands

The **scheduler-set** range has been changed from 1-4 to 1-12. This changes the following commands:

```
awplus(config)# mls qos scheduler-set <1-12> priority-queue
...
awplus(config#) mls qos scheduler-set <1-12> wrr-queue ...
awplus(config-if#) mls qos scheduler-set <1-12>
```

The minimum wrr-queue **weight** range has been changed from 6-255 to 1-255. This changes the following command:

```
awplus(config#) mls qos scheduler-set <1-12> wrr-queue group
<1-2> weight <1-255> queues [0][1][2]3][4][5][6][7]
```

The following **show** commands now show additional information:

`show mls qos scheduler-set`

- will display WRR percentage-based weights with a % suffix to differentiate from regular WRR weights.

`show mls qos scheduler-set`

- will now display a warning when the WRR percentage-based weights of a group do not sum to 100%.

`show mls qos interface`

- will now display if CIR is enabled on a queue. If it is enabled, the CIR rate (as a percentage of line rate) and action will be displayed.

Further documentation

For more information, see the Quality of Service (QoS) Feature Overview and Configuration Guide.

Media Redundancy Protocol (MRP) Enhancements

Applies to SBx908 GEN3, x540L and x530 Series

From version 5.5.5-2.1 onwards, MRP includes the following enhancements:

- support for x530, x540L, and SBx908 GEN3 Series switches.
- support for Multiple Rings with a common MRP manager on these switches.

What is MRP used for?

MRP is a standardized redundancy protocol used in Industrial Ethernet ring networks. Ethernet technology does not allow physical loops, as they cause packets to circulate endlessly and overload the network. This means providing media redundancy within an Ethernet network requires the use of a protocol that is able to monitor and resolve the physical loops introduced by redundant pathways.

Media redundancy is primarily used to avoid single points of failure in industrial communication networks. If a failure occurs on a redundant structure, the network falls back to a secondary state in which communication is still viable, and repair can be made to restore the system to the previous fault-free state.

MRP is specified for ring networks with up to 50 devices. It guarantees fully predictable switchover behavior. Allied Telesis switches support worst-case switch-over times of 200 or 500ms.

For more information, see the Media Redundancy Protocol (MRP) Feature Overview and Configuration Guide.

Mirroring with VLAN filtering

Applies to SBx908 GEN2, x950, x930, and x230 Series

From version 5.5.5-2.1 onwards, a new command is available that allows you to mirror traffic on a specific VLAN.

```
mirror interface <source-port> vlan <2-4090>
```

Previously, if you wanted to mirror traffic on a specific VLAN, you had to use an ACL with a copy-to-mirror action. However, due to how ACLs work—stopping at the first match—this approach prevented any subsequent permit or deny rules from being evaluated. As a result, you couldn't mirror VLAN traffic and apply additional filtering rules in the same ACL.

To address this limitation, the new command:

- Enables VLAN-based mirroring using ACLs.
- Allows the copy-to-mirror action to occur without terminating ACL processing, so additional rules can still be evaluated.
- Clears any previous mirroring setup.
- Wraps the ACL logic into a single, user-friendly command, simplifying configuration.
  - « The command automatically generates a hardware ACL with a reserved name based on the VLAN ID and port name. The ACL mirrors traffic to a specified VLAN.

Example To mirror traffic on VLAN 12, for example:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# mirror interface port1.0.1 vlan12
```

This configuration mirrors traffic from interface port1.0.1 on VLAN 12 to the current interface port1.0.5. Only traffic tagged with VLAN 12 will be mirrored, allowing for more targeted monitoring. This differs from full interface mirroring, which captures all traffic (regardless of VLAN) on the source port.

For more information, see the Mirroring Feature Overview and Configuration Guide.

Priority-based Flow Control (PFC)

Applies to x540L Series

From version 5.5.5-2.1 onwards, you can enable Priority-based Flow Control (PFC) to let traffic be paused for one or more egress queues, while allowing traffic to continue to flow on other queues.

Modern data centers and enterprise networks rely heavily on Ethernet for high-speed communication. However, traditional Ethernet does not guarantee lossless transmission. This can be a problem for applications that are sensitive to packet loss, such as storage traffic (e.g., iSCSI, RoCE) or real-time data streams.

PFC addresses this issue by enabling selective pausing of traffic based on priority. Unlike traditional flow control mechanisms that pause all traffic on a link, PFC allows network devices to pause specific classes of traffic while allowing others to continue. This fine-grained control helps prevent congestion-related packet loss without compromising overall throughput.

If your network carries mixed traffic types, such as storage, voice, and general data, PFC can help ensure that critical traffic flows are protected from congestion, improving performance and reliability.

New Commands

PFC Global Configuration

To enable the PFC service, use the following command:

```
service pfc
```

To disable the PFC service, use the following command:

```
no service pfc
```

PFC Interface Configuration

While you are in Interface Configuration mode for a switchport (including switchports that are aggregator members):

To enable PFC on an interface, use the following command (default is **auto**):

```
pfc mode {on|off|auto}
```

Note: To enable PFC on an interface, set the mode to **on**. Auto mode is not supported in version 5.5.5-2.x and behaves the same as **off** in this version. In a future software version, the auto mode will allow for auto-negotiation of PFC settings using DCBX.

To set PFC on an interface to the default (**auto** - currently the equivalent of **off**), use the following command:

```
no pfc mode
```

To enable PFC for a priority on an interface, use the following command (default is none):

```
pfc priority <0-7>
```

Show Commands

To view information about the buffer information relevant to PFC, use the following command:

```
show platform mem QosBufferConfig
```

Further documentation

For more information, see the Priority-based Flow Control (PFC) Feature Overview and Configuration Guide.

Converting switch ports to Layer 3 router ports

Applies to IE560, IE340, IE360, and IE220 Series

From version 5.5.5-2.1 onwards, AlliedWare Plus supports the **no switchport** command on these products.

What does the **no switchport** command do?

On an Ethernet switch, ports are usually used to connect devices like computers or other switches. By default, these ports operate at Layer 2, which means they handle things like MAC addresses and VLANs—basically, they help devices talk within the same local network.

When you use the command **no switchport**, you're telling the switch: "I want this port to act like a router port instead." This changes it to Layer 3, which means it can have an IP address and participate in routing between different networks.

Here's some reasons why you would use this command:

- **Enable Layer 3 routing**: This command turns off Layer 2 switching and turns on Layer 3 routing for the port. After that, you can assign an IP address to the port.
- **Make the port act like a router**: The port works like an Ethernet interface on a router, so you can set it up as a default gateway.
- **Use for traffic monitoring**: In some set ups, you apply 'no switchport' to a port used for traffic monitoring (like port mirroring) or as part of a link aggregation group.
- **Avoid STP**: When you convert a port to a Layer 3 routed port, it drops out of the Spanning Tree Protocol (STP) domain. This makes network design simpler in certain cases

Examples

To enable Layer 3 routing on port 1.0.5, use the commands:

```
awplus# configure terminal
awplus(config)# interface port 1.0.5
awplus(config-if)# no switchport
```

To display information about internal VLANs used by the no switchport feature, use the command:

```
awplus# show vlan internal
```

```
awplus#show vlan internal
VID   Used By
----------------------
3996  port1.0.5
3997  port1.0.4
3998  port1.0.3
3999  port1.0.2
4000  port1.0.1
```

PTP Peer-to-Peer Transparent Clock support

Applies to IE560, IE360, IE340 Series

From version 5.5.5-2.1 onwards, AlliedWare Plus supports Peer-to-Peer Transparent Clock (TC) on the IE560, IE360, and IE340 platforms. This enhancement enables highly accurate time synchronization across distributed systems and supports a wide range of industrial and networking applications.

What are Transparent Clocks?

Transparent Clocks are network devices that help improve timing accuracy by measuring and correcting the time it takes for PTP messages to pass through them.

There are two types:

1. End-to-End Transparent Clock (E2E TC)
   - « Measures the residence time (how long a PTP message stays in the device).
   - « Adds this time to the correction field in the PTP message.
   - « Helps secondary clocks calculate total delay from the master.
2. Peer-to-Peer Transparent Clock (P2P TC)
   - « Measures link delay between directly connected devices.
   - « Exchanges messages with its peers to calculate delay.
   - « Adds both link delay and residence time to the correction field.

Why P2P TC is preferable when supported

Higher Precision

P2P TC calculates delay for each network segment individually, which leads to more accurate time synchronization—especially in large or complex topologies.

Reduced Error Accumulation

Because each link is corrected independently, timing errors don't build up across multiple hops like they can in E2E TC.

Better for Dynamic Networks

P2P TC adapts better to changing network conditions (e.g., varying traffic loads or link characteristics).

Better scalability

Peer-to-Peer Transparent Clock is more scalable because it measures and corrects delay at each network hop, preventing error accumulation and maintaining accuracy in large, multi-hop topologies.

For more information, see the PTP and Transparent Clock Feature Overview and Configuration Guide.

Support for 256 BGP routes on IE560 and IE360 Series

From version 5.5.5-2.1 onwards, the premium license on IE560 and IE360 Series switches supports 256 BGP/BGP4+ routes.

Specifying the IEEE PoE standard per port

Applies to:

- *x240-10GHXm, x240-18GHXm, x240-26GHXm*
- *SE240-10GHXm, SE240-18GHXm, SE240-26GHXm*
- *all IE360 Series switches that support PoE*

From version 5.5.5-2.1 onwards, it is possible to specify the IEEE Power over Ethernet standard for individual ports on the listed switches. Specifying the standard can increase power reliability in these switches when powering IEEE 802.3at (class 4) PDs.

The new functionality may also be useful if there is a problem powering a device that uses a "pre-BT" power option - a high-power option developed before IEEE 802.3bt.

To configure this, use the new command **power-inline ieee-std**. For example, to configure IEEE 802.3at on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# power-inline ieee-std at
```

Command options are:

- **bt** (IEEE-802.3bt - the default)
- **at** (IEEE 802.3at)
- **prebt** (pre-BT: other high-power options developed before IEEE 802.3bt).

If you use this command on x240-52GHXm or SE240-52GHXm, it will have no effect. The following log message will be produced:

2025 Nov 06 08:02:02 user.warning awplus POE[1149]: Changing the supported PoE IEEE standard is not supported on interface port1.0.1

For more information about configuring PoE, see the Power over Ethernet Feature Overview and Configuration Guide.

Support for Secure Mode on x240 and x230 Series

From version 5.5.5-2.1 onwards, x240 and x230 Series switches support crypto Secure Mode. When in Secure Mode, the following are disabled:

- Telnet
- SSHv1
- SNMPv1/v2
- All privilege levels except 1 and 15
- Algorithms that are not supported under FIPS, including MD5, RSA-1 and DSA
- The ability to store passwords in cleartext and to specify an **enable** password

Secure Mode is disabled by default. To enable it, use the commands:

```
awplus#configure terminal
awplus(config)# crypto secure-mode
```

However, to ensure a fully secure system, we recommend following the "How to enable Secure Mode" procedure described in Getting Started with the AlliedWare Plus Command Line Interface.

Manage up to 50 AMF Plus nodes on the ARX200S-GTX

From version 5.5.5-2.1 onwards, the ARX200S-GTX supports up to 50 AMF Plus **nodes** when configured as an AMF Plus Master.

This enhancement allows for greater scalability in AMF Plus-managed networks using this platform.

For more information about AMF Plus, see the AMF Plus Feature Overview and Configuration Guide.

Wireless Controller able to control TQR Series

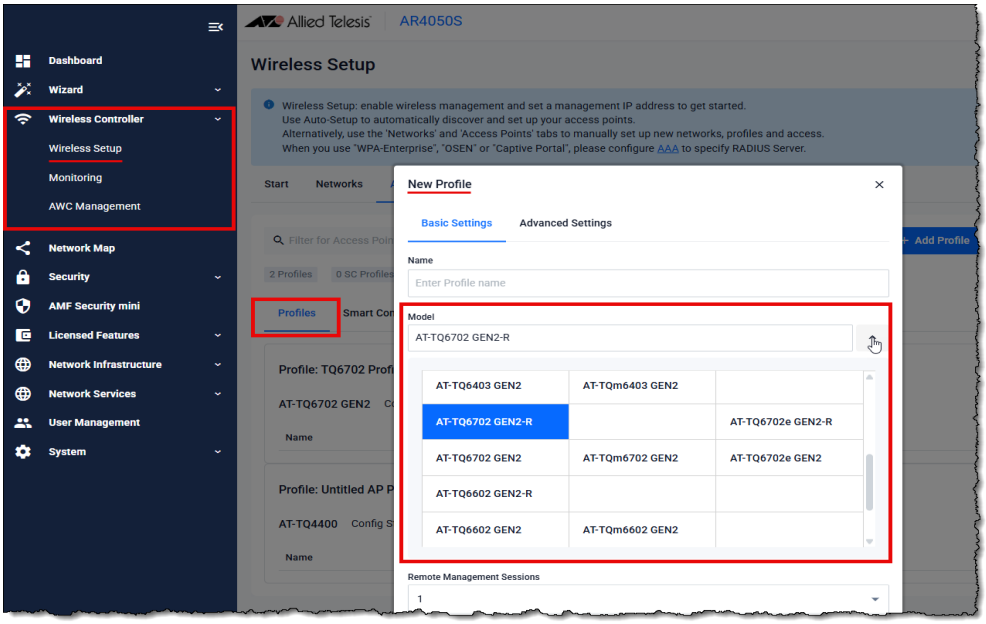
Applies to all devices that support the Wireless Controller

From version 5.5.5-2.1 onwards, you can use the Wireless Controller to configure TQR Series access points, as well as TQ Series access points.

The Wireless Controller was previously known as Vista Manager mini. It allows you to use a one of a range of AlliedWare Plus switches and routers to configure the access points in your network. You can use the Wireless Controller directly from the Wireless Controller menu in the Device GUI, or through CLI commands.

Configuration through the Device GUI

The Wireless Controller is available to configure TQR Series devices from Device GUI version 2.22.0 onwards.



Command change: **hwtype** command

Adding the TQR Series to the list of access points that can be controlled means the **hwtype** command now supports TQR Series APs, such as:

Parameter	Access point model
at-tq6702gen2-r	TQ6702 GEN2-R
at-tq7403-r	TQ7403-R

For example, to configure the AP hardware type as AT-TQ6702 GEN2-R for AP profile 3, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
```

```
awplus(config-wireless)# ap-profile 3
awplus(config-wireless-ap-prof)# hwtype at-tq6702gen2-r
```

New command: **bridge** command

The Wireless Controller's AP Profile for TQR series access points now includes a new command that lets you control which network bridge each virtual access point (VAP) connects to. This feature is only supported on TQR Series devices. The new command is:

```
bridge <0-300>
```

By specifying bridge membership, you can manage how wireless traffic is routed across your network.

For example, to set which bridge a VAP is a member of, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# bridge 0
```

Notes on the new bridge command:

The new **bridge** command is defined at the network level. It associates the SSID's data with the correct bridge interface on the TQR Series device. When this command is present, the VAP for that network will be moved or added to the specified bridge.

If (and only if) the bridge ID is 0, the Wireless Controller will also apply the native VLAN configuration from the Network settings to the bridge.

The new bridge command only applies to the Wireless Controller. You can also configure bridging directly on TQR Series devices. This means you can use either of these methods:

- This new network-level configuration on the Wireless Controller, to add or move the VAP between bridges.
- The existing bridge commands on each TQR Series device, to add, move, or remove VAPs from bridges.

Note: This new command exists only at the network level, but it will be included in the profile when the network is linked to a profile, similar to how an SSID is handled.

Wireless Controller on TQR series

Applies to TQR Series

From version 5.5.5-2.1 onwards, the Wireless Controller is available on TQR Series devices. This allows you to manage other TQ and TQR Series devices within your network directly from the Wireless Controller menu in the Device GUI, or through CLI commands.

In the Device GUI, TQR Series devices also include a Wireless menu, which lets you configure the TQR Series device's own wireless settings.

The Wireless Controller provides centralized visibility and control of wireless devices. Key features include:

- *Wireless Setup*

  Quickly enable wireless management by assigning a management IP address. Use Auto-Setup to automatically discover and configure access points, or manually create networks and profiles through the Networks and Access Points tabs.

- *Monitoring*

  View the real-time status of wireless access points and connected clients. Easily identify unauthorized or failed APs, schedule immediate or delayed configuration or firmware updates, and reboot devices as needed.

- *AWC Management*

  Continuously analyze access point locations and signal strength with Autonomous Wave Control (AWC). It uses intelligent algorithms to automatically adjust wireless output and channel selection to deliver optimal performance and a better user experience.

Wireless commands

This enhancement adds support for all wireless CLI commands on TQR series. To start configuring the Wireless Controller with the CLI, go into wireless mode:

```
awplus# configure terminal
awplus(config)# wireless
```

Enable pre-authentication features on multiple VAPs on TQR Series

Applies to TQR Series devices

From version 5.5.5-2.1 onwards, TQR Series devices support pre-authentication on all Virtual Access Points (VAPs, numbers 0-15).

Pre-authentication shortens the authentication time during roaming by sharing authentication information between APs in advance.

Until now, this feature has only been supported on VAP0 for all radios. From 5.5.5-2.1 onwards, it is supported on all VAPs, for all radios.

What changes have been made?

This feature can now be enabled on VAPs numbered 0-15.

Notes about configuration of this feature through the AWC plugin in Vista Manager EX:

- The AWC plugin will support this feature from version 3.16.0 onwards.
- If a TQR Series device is managed by an unsupported AWC plugin version, VAP0's pre-authentication settings will apply and those of VAP1–15 will be disabled.

- If you upgrade to a supported AWC plugin version, the plugin will apply each VAP's pre-authentication setting.
- If you downgrade to an unsupported AWC plugin version, all VAPs use VAP0's pre-authentication setting.

Examples Pre-authentication is enabled by default. To enable or disable it on a WPA enterprise configuration, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 1 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# pre-authentication enable
```

For more information about wireless configuration of TQR Series APs, see Wireless Management for the TQR series using the Device GUI.

Set IEEE 802.11r key holder AP list on TQR Series

Applies to TQR Series devices

From version 5.5.5-2.1 onwards, TQR Series devices support the "Key Holder List" feature. This is a list of candidate access points for roaming - the potential next access points that a device can connect to when roaming. This list is required by IEEE 802.11r (Fast Roaming). This enhancement enables you to create this list on TQR Series devices.

The TQR series list is called the **Key Holder List custom**.

This feature is supported for local wireless control on TQR series devices only. It is not supported when using the Wireless Controller to configure other APs.

Key Holder List command

You can add a BSSID to the **Key Holder List custom** in WPA Enterprise mode, using the following new command.

```
key-holder-list entry <bssid>
```

Examples To add a BSSID to the **Key Holder List custom**, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 1 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# key holder list entry
001a.0000.cdef
```

To delete a BSSID from the **Key Holder List custom**, use these commands:

```
awplus# configure terminal
awplus(config)# wireless
```

```
awplus(config-wireless)# security 1 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# no key-holder-list entry
001a.0000.cdef
```

If you do not specify the BSSID, all entries will be deleted:

```
awplus(config-wireless-sec-wpa-ent)# no key-holder-list entry
```

Interaction with the AWC Plugin in Vista Manager EX

The AWC plugin automatically generates a list called the **Key Holder List**. Whether a TQR Series device uses this list or the **Key Holder List custom** list depends on whether the AWC plugin is used for managing the TQR Series device:

- If the AWC plugin applies settings to the TQR Series device, the device uses the Key Holder List. It deletes the Key Holder List custom if it exists.
- If you create a Key Holder List custom on the TQR Series device, the device uses that list. It deletes the Key Holder List if it exists.

For more information about wireless configuration of TQR series APs, see Wireless Management for the TQR series using the Device GUI.

Bridge VAPs and eth1 by default on TQR series

From version 5.5.5-2.1 onwards, new TQR Series devices have bridging configured by default. Now, all default VAPs and the eth1 interface are added to the bridge interface br0, so that all traffic is bridged between these interfaces.

This change gives the TQR Series access points the same initial bridging configuration as TQ Series access points.

Note that if a device has an eth2 interface, that is not added to the bridge automatically.

What are the changes?

The default configuration for TQR devices using AlliedWare Plus has the following changes:

- eth1 is placed in br0
- The device tries to use DHCP to obtain an IP address for br0
- If DHCP fails, the device uses the static IP address of 192.168.1.1/24 on br0
- All VAP interfaces are placed in br0.

For more information about bridging, see the Bridging Feature Overview and Configuration Guide.

For more information about basic configuration of TQR series APs, see Getting Started with the TQR Series Wireless Router.

Virtual IP Address for Captive Portal on TQR series

From version 5.5.5-2.1 onwards, TQR series products support a virtual IP address for Captive Portal.

Previously, the Captive Portal feature on the TQR products used the IP address of the VAP as the management IP address. This posed a security risk.

What changes have been made?

This feature uses a virtual IP for Captive Portal authentication, thereby hiding the management IP address of the TQR Series device from clients.

Examples To configure a virtual IP address for Captive Portal, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# captive-portal virtual-ip
192.168.1.1
```

To display the AP-profile configuration for a wireless network, use the command:

```
awplus# show wireless ap-profile local brief
```

```
awplus#show wireless ap-profile local brief
ID       Description     Radio 1    Radio 2    Radio 3
---      -----------     -------    -------    -------
1                        Enable     Enable     Disable
```

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 Plus software version compatibility
- Upgrading all devices in an AMF Plus network

Finally, it lists Country support for TQR Series.

Please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.4-2.x version, please check the 5.5.5-0.x and 5.5.5-1.x release note as well. Release notes are available from our website, including:

- 5.5.5-x.x release notes
- 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 61 and "Details for x930 Series" on page 62 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.

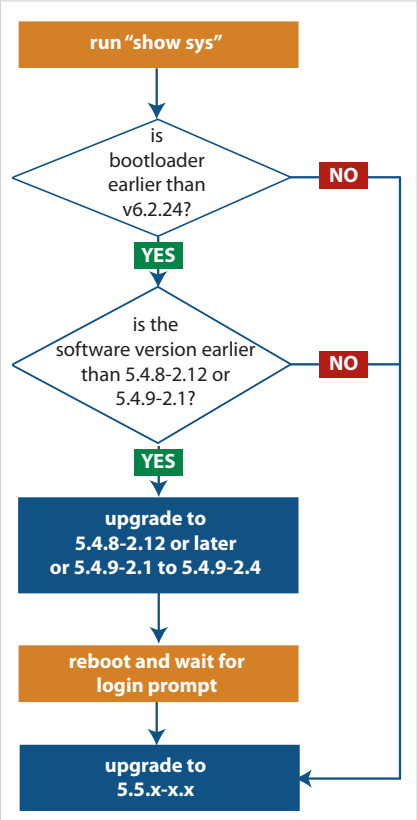
Instead, before upgrading from one of those versions to the current version, make sure your switch is running one of these specified versions:

- 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:

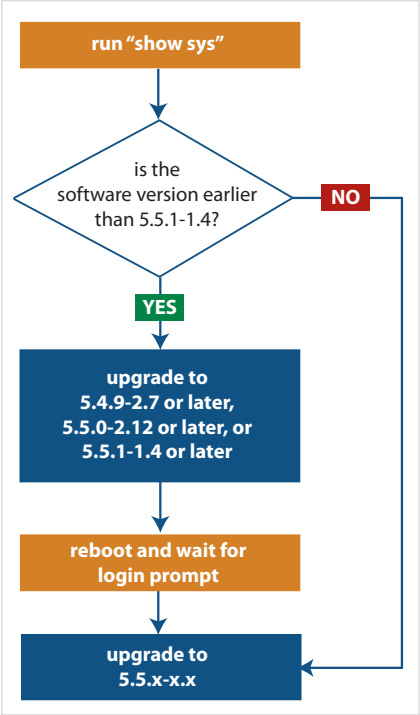
```
awplus# show system
```



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 **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
license update online command no longer available.	All AlliedWare Plus devices with subscription licenses across all firmware versions, including previous versions.	Since January 2025, the **license update online** command is no longer available for downloading licenses. To obtain licenses, please contact your authorized Allied Telesis support center. After obtaining the license, use the **license update file** command to install it.
x240 bootup time increased	x240 series	From 5.5.5-1.2 onwards, the time taken for x240 series switches to boot has increased, to allow for boot-up of stacked switches. On standalone units, you can reduce bootup time by entering **no stack 1 enable**.

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.5 license on your switch if you are upgrading to 5.5.5-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 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

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 Plus software version compatibility

Applies to all AlliedWare Plus devices

We strongly recommend that all nodes in an AMF Plus network run the same software version.

AMF Plus security has been increased in 5.5.5-2.1. This change means that once **any** node in an AMF network is upgraded to 5.5.5-2.1, **all** nodes should run one of the following AlliedWare Plus maintenance versions (or later):

- 5.5.1-2.17 (available from the Allied Telesis Support Portal)
- 5.5.3-0.7 (available on request)
- 5.5.3-2.8 (available on request)
- 5.5.4-0.6 (available on request)
- 5.5.4-1.9 (available on request)
- 5.5.4-2.5 (available from the Allied Telesis Support Portal)
- 5.5.5-0.2 (available from the Allied Telesis Support Portal)
- 5.5.5-1.2 (available from the Allied Telesis Support Portal)
- 5.5.5-2.1 (available from the Allied Telesis Support Portal)

Effect if products are not upgraded

Devices running older versions can still join the AMF Plus network. However, the following functionality will not be supported:

- Remote login: Using the command **atmf remote-login <node>** to or from a node with the older security.
- Using the following commands in a single-node working-set (the command **atmf working-set <node>**) to or from a node with the older security:
  - 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)

- terminal monitor
- test cable-diagnostics tdr interface
- traceroute

Upgrading all devices in an AMF Plus network

Applies to all AlliedWare Plus devices

This version supports upgrades across AMF Plus networks. There are two methods for upgrading firmware on an AMF Plus network - both called "bulk upgrades" in this section:

- 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.

This version introduces a mismatch between firmware versions when doing bulk upgrades. In particular, **upgrading your AMF Plus master to 5.5.5-2.1 may stop you from using the master to upgrade other devices**, depending on which firmware versions the other devices are running.

This is because the bulk upgrade process uses encryption keys and the key types have changed.

The change has been done in two stages:

1. Recent previous versions added the new key type while keeping the old one
2. This version removed the old key type.

Table 1 below lists versions that have only the old keys (column A), have both keys (column B), and only the new keys (column C).

Table 1-1: Firmware versions categorized by whether they have the old or new keys

old keys only	both key types	new keys only
A	B	C
5.5.1-2.15 and earlier	5.5.1-2.17	5.5.1-2.18 and later
5.5.3-0.6 and earlier	5.5.3-0.7	
5.5.3-2.6 and earlier	5.5.3-2.7	
5.5.4-0.5 and earlier	5.5.4-0.6	
5.5.4-1.8 and earlier	5.5.4-1.9	
5.5.4-2.4 and earlier	5.5.4-2.5 to 5.5.4-2.6	5.5.4-2.7 and later
5.5.5-0.1 and earlier	5.5.5-0.2 to 5.5.5-0.5	5.5.5-0.6 and later
	5.5.5-1.2 to 5.5.5-1.4	5.5.5-1.5 and later
		5.5.5-2.1 and later

Why this matters for bulk upgrades

The bulk upgrade process uses keys to secure the connection between:

- the device that you are running the bulk upgrade command on ("the source"), and
- the devices you are upgrading ("the destinations").

The source and destinations must run firmware versions with matching keys. With reference to Table 1-1, the following firmware versions match:

Source	Destinations
All versions from Column A from Table 1-1	All versions from Column A from Table 1-1
Column B	Column A
Column B	Column B
Column B	Column C
Column C	Column B
Column C	Column C

The following firmware versions do not match:

Source	Destinations
Column A	Column B
Column A	Column C
Column C	Column A

Examples

Here are some examples that will work for upgrading devices to 5.5.5-2.1:

- Using reboot-rolling on a master that runs 5.5.5-0.5 (column B), to upgrade devices running 5.5.5-0.1 (column A)
- Using reboot-rolling on a master that runs 5.5.5-2.1 (column C), to upgrade devices running 5.5.5-0.5 (column B)

How to upgrade from earlier software versions

If you need to upgrade when the source and destinations are incompatible, we recommend the following procedure:

1. Upgrade your AMF Plus master to a version in column B.
2. From the AMF Plus master, use reboot-rolling or distribute firmware to upgrade all devices **except** the master to 5.5.5-2.1. See "Procedure for using reboot-rolling or distribute-firmware" on page 68.
3. Once all other nodes have been upgraded, upgrade the master to 5.5.5-2.1.

Example

For example, to upgrade all devices from 5.5.5-0.1 to 5.5.5-2.1, you can:

1. Upgrade your AMF Plus master to 5.5.5-0.5 (from column B)
2. From the AMF Plus master, use reboot-rolling or distribute-firmware to upgrade all devices except the master to 5.5.5-2.1

3. Once all other nodes have been upgraded, upgrade the master to 5.5.5-2.1.

Procedure for using reboot-rolling or distribute-firmware

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

In summary, the procedure for upgrading firmware on an AMF Plus 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 Plus upgrade method is most suitable.

3. Initiate the AMF Plus 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.

Country support for TQR Series

The TQR Series access points support the following countries. An * indicates that 6GHz cannot be selected in these countries on that AP.

TQ7613-R	TQ7403-R	TQ6702 GEN2-R	TQ6702e GEN2-R	TQ3403-R
Austria	Australia	Australia	Australia	Australia
Belgium	Austria	Austria	Austria	Austria
Bulgaria*	Belgium	Belgium	Belgium	Belgium
Croatia	Bulgaria*	Bulgaria	Bulgaria	Bulgaria*
Cyprus*	Canada	Canada	Canada	Croatia
Czech Republic	Croatia	China	Croatia	Cyprus*
Denmark	Cyprus*	Croatia	Cyprus	Czech Republic
Estonia*	Czech Republic	Cyprus	Czech Republic	Denmark
Finland	Denmark	Czech Republic	Denmark	Estonia*
France	Estonia*	Denmark	Ecuador	Finland
Germany	Finland	Estonia	Estonia	France
Greece	France	Finland	Finland	Germany
Hungary*	Germany	France	France	Greece
Ireland	Greece	Germany	Germany	Hong Kong
Italy*	Hong Kong	Greece	Greece	Hungary*
Japan	Hungary*	Hong Kong	Hungary	Ireland
Latvia	Ireland	Hungary	India	Italy*
Lithuania*	Italy*	India	Indonesia	Japan
Luxembourg	Japan	Ireland	Ireland	Latvia
Malta*	Latvia	Italy	Italy	Lithuania*
Netherlands	Lithuania*	Japan	Japan	Luxembourg
Poland*	Luxembourg	Latvia	Latvia	Malaysia
Portugal	Malaysia	Lithuania	Lithuania	Malta*
Romania	Malta*	Luxembourg	Luxembourg	Netherlands
Slovakia Republic*	Netherlands	Malaysia	Malaysia	New Zealand
Slovenia*	New Zealand	Malta	Malta	Poland*
Spain	Poland*	Netherlands	Mexico	Portugal
Sweden*	Portugal	New Zealand	Netherlands	Romania
	Romania	Poland	New Zealand	Singapore
	Singapore	Portugal	Peru	Slovakia Republic*
	Slovakia Republic*	Romania	Philippines	Slovenia*
	Slovenia*	Singapore	Poland	Spain
	Spain	Slovakia Republic	Portugal	Sweden*
	Sweden*	Slovenia	Romania	Taiwan
	Taiwan	Spain	Saudi Arabia	Thailand
	Thailand	Sweden	Singapore	United Kingdom
	United Kingdom	Taiwan	Slovakia Republic	USA
	USA	Thailand	Slovenia	
		United Kingdom	Spain	
		USA	Sweden	
		Vietnam	Taiwan	
			Thailand	
			United Arab Emirates	
			United Kingdom	
			USA	

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

Verifying the Release File

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 5.5.5-2.4 below or in the release file'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. For more information, see Getting Started with the AlliedWare Plus Command Line Interface.

Table: Hash values for 5.5.5-2.4

Product family	Software File	Hash
AR1050V	AR1050V-5.5.5-2.4.rel	d51cc7d4b7ed0ae9dd8a9a5a55bef3ad79f93014ec35d25187f3353ae4aa8ebe
AR3050S	AR3050S-5.5.5-2.4.rel	28da982fc38620c3848a3a077ae32d5bcb75a92f10a81d6b6f026bf62b024c7a
AR4050S and AR4050S-5G	AR4050S-5.5.5-2.4.rel	28da982fc38620c3848a3a077ae32d5bcb75a92f10a81d6b6f026bf62b024c7a
ARX200S	ARX200S-5.5.5-2.4.rel	a076a42948dbd2de375918c5a3340fcd9a7c5fd5d160ef9aca27fd3db171ef1f
GS970M	GS970-5.5.5-2.4.rel	27174c11ec43114f33c4a36427c86dc939fe0fa8baa96073b7e614c82a6d220d
GS970EMX	GS970EMX-5.5.5-2.4.rel	8abf422422a191189abcf3db0a404d2ce5e18e07b0f36af6ad2a4db48b4ef224

Product family	Software File	Hash
GS980EM	GS980EM-5.5.5-2.4.rel	f81ddd2a8d7ec66dd318e0529dbfd7d7bedc32b7de1f182a9b28ca4bf74871c8
GS980M	GS980M-5.5.5-2.4.rel	b2874375852bbe91c903d2f1c634f16ee09ab8c28c6f8c35ad2dfd6ebe5be50e
GS980MX	GS980MX-5.5.5-2.4.rel	f81ddd2a8d7ec66dd318e0529dbfd7d7bedc32b7de1f182a9b28ca4bf74871c8
IE210	IE210-5.5.5-2.4.rel	27174c11ec43114f33c4a36427c86dc939fe0fa8baa96073b7e614c82a6d220d
IE220	IE220-5.5.5-2.4.rel	6010640873a1174318d1ac429588dc80fbc24e914bf83384a805d3fd6fcc3f59
IE340	IE340-5.5.5-2.4.rel	8af5ac27f4841ac9269ead0b29c09677273d0f26fe50db6cecc433564419c5be
IE360	IE360-5.5.5-2.4.rel	ec9757698aa09a2aee30738bbe25f110a353895d4f4150f808b2e16d1b984dcb
IE560	IE560-5.5.5-2.4.rel	e9142cf46c172358e0113012c5794cce717f72b72a9e3617863543dad6daea90
SBx81CFC960	SBx81CFC960-5.5.5-2.4.rel	438b7ef72350547bb12b47021d3ee30395d8baa18d66e031f37007cd16f84c1d
SBx908 GEN2	SBx908NG-5.5.5-2.4.rel	5697f57f1da38239ae3adc167ffd49201a4044a304d573de3d5eb15b68542917
SBx908 GEN3	SBx90xGEN3-5.5.5-2.4.rel	daa803d55aac1dae3cef3192f7e04e7e3c7bb89237d45c62828f98abdf2e522b
SE240	SE240-5.5.5-2.4.rel	24e6ffaf48f1885e7332776540e820adfad21e7727d6a1161f6d4e611ecc961f
SE250	SE250-5.5.5-2.4.rel	d27ae416e02ed7578c477b66c22a39d6bace6bb407fffea28440a885793cb3c8
SE540L	SE540-5.5.5-2.4.rel	30a323739cc16ce1c360cec31e0e73062a34f37051d3f41b0b6226967f422e0e
TQ3403-R	TQ3403R-5.5.5-2.4.rel	ff2826d8d32f15e444a727cb60cc70d3a5c13b7c44bcd88608df224e2f43a424
TQ6702e GEN2-R	TQ6702eGEN2R-5.5.5-2.4.rel	ebcad18364bdc092fdd632c4bbc08ffca0204fb20db390c2d47fd34196744b40
TQ6702 GEN2-R	TQ6702GEN2R-5.5.5-2.4.rel	101ce475d6ddec48d1f4bb6393602a160613e9434027b334ac94adc8afd3fc40
TQ7403-R	TQ7403R-5.5.5-2.4.rel	dc7cda61cb6b3e1b4a2ebbb3dd8be87463b1bb191fe044af5b4c4bd223686351
TQ7613-R	TQ7613R-5.5.5-2.4.rel	f6e45173e925bd6e1b2198e850eebf5553b665f7cc5109a45bea593dd08f2963
AMF Plus Cloud	vaa-5.5.5-2.4.rel	956167ea8d60ea7a562d2cc896b4e395200d5f4cd5cfb8d884e5af2e8678c06e
x220	x220-5.5.5-2.4.rel	b2874375852bbe91c903d2f1c634f16ee09ab8c28c6f8c35ad2dfd6ebe5be50e
x230	x230-5.5.5-2.4.rel	27174c11ec43114f33c4a36427c86dc939fe0fa8baa96073b7e614c82a6d220d
x240	x240-5.5.5-2.4.rel	24e6ffaf48f1885e7332776540e820adfad21e7727d6a1161f6d4e611ecc961f
x250	x250-5.5.5-2.4.rel	d27ae416e02ed7578c477b66c22a39d6bace6bb407fffea28440a885793cb3c8
x320	x320-5.5.5-2.4.rel	f81ddd2a8d7ec66dd318e0529dbfd7d7bedc32b7de1f182a9b28ca4bf74871c8
x330	x330-5.5.5-2.4.rel	8abf422422a191189abcf3db0a404d2ce5e18e07b0f36af6ad2a4db48b4ef224
x530 and x530L	x530-5.5.5-2.4.rel	f81ddd2a8d7ec66dd318e0529dbfd7d7bedc32b7de1f182a9b28ca4bf74871c8
x540L	x540-5.5.5-2.4.rel	30a323739cc16ce1c360cec31e0e73062a34f37051d3f41b0b6226967f422e0e
x550	x550-5.5.5-2.4.rel	c597b2dd6f603d0ba74157676250cbe1fb23b934e4d504cd2859f830d0aa0396

Product family	Software File	Hash
x560	x560-5.5.5-2.4.rel	30a323739cc16ce1c360cec31e0e73062a34f37051d3f41b0b6226967f422e0e
x930	x930-5.5.5-2.4.rel	4a216b857b8d92a302be8f1a4cfabe32892b50394a3aa3e30d3349f2dd478ec9
x950	x950-5.5.5-2.4.rel	5697f57f1da38239ae3adc167ffd49201a4044a304d573de3d5eb15b68542917
XS900MX	XS900-5.5.5-2.4.rel	bf0205a996a9b1c422f1658df6d38fff6bd4f975f463035e8710d902ebeff3f0

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                  : 5.5.5
Customer name                 : ABC Consulting
Quantity of licenses          : 1
Type of license               : Full
License issue date            : 05-May-2025
License expiry date           : N/A
Release                       : 5.5.5
```

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                   : 5.5.5
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 05-May-2025
License expiry date            : N/A
Release                        : 5.5.5
```

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 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

To update the firmware:

1. Copy the software version file (.rel) onto your TFTP server or your USB drive.

2. If necessary, delete or move files to create space in 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 or your USB drive onto the device.

   To copy the release file from a TFTP server to flash memory, enter Privileged Exec mode and enter the command:

   ```
   awplus# copy tftp flash
   ```

   To copy the release file from a USB device, when your current directory is the top-level flash directory, enter the command:

   ```
   awplus# copy usb:<source-filename> flash
   ```

   On SBx8100 Series switches, you only need to copy the new release to the Active SBx81CFC960 Control Fabric Card (CFC). If your SBx8100 system has a standby CFC installed, the new release file, the configuration file, and all licenses are automatically synchronized from the Active CFC.

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	awplus(config)# boot system SBx8100-5.5.5-2.4.rel
SBx908 GEN3	awplus(config)# boot system SBx90xGEN3-5.5.5-2.4.rel
SBx908 GEN2	awplus(config)# boot system SBx908NG-5.5.5-2.4.rel
x950 series	awplus(config)# boot system x950-5.5.5-2.4.rel
x930 series	awplus(config)# boot system x930-5.5.5-2.4.rel
x550 series	awplus(config)# boot system x550-5.5.5-2.4.rel
x540L series	awplus(config)# boot system x540-5.5.5-2.4.rel
x530 series	awplus(config)# boot system x530-5.5.5-2.4.rel

Product	Command
x330 series	awplus(config)# boot system x330-5.5.5-2.4.rel
x320 series	awplus(config)# boot system x320-5.5.5-2.4.rel
x250 series	awplus(config)# boot system x250-5.5.5-2.4.rel
x240 series	awplus(config)# boot system x240-5.5.5-2.4.rel
x230 series	awplus(config)# boot system x230-5.5.5-2.4.rel
x220 series	awplus(config)# boot system x220-5.5.5-2.4.rel
IE560 series	awplus(config)# boot system IE560-5.5.5-2.4.rel
IE360 series	awplus(config)# boot system IE360-5.5.5-2.4.rel
IE340 series	awplus(config)# boot system IE340-5.5.5-2.4.rel
IE220 series	awplus(config)# boot system IE220-5.5.5-2.4.rel
IE210L series	awplus(config)# boot system IE210-5.5.5-2.4.rel
SE540L series	awplus(config)# boot system SE540-5.5.5-2.4.rel
SE250 series	awplus(config)# boot system SE250-5.5.5-2.4.rel
SE240 series	awplus(config)# boot system SE240-5.5.5-2.4.rel
XS900MX series	awplus(config)# boot system XS900-5.5.5-2.4.rel
GS980M series	awplus(config)# boot system GS980M-5.5.5-2.4.rel
GS980EM series	awplus(config)# boot system GS980EM-5.5.5-2.4.rel
GS980MX series	awplus(config)# boot system GS980MX-5.5.5-2.4.rel
GS970EMX series	awplus(config)# boot system GS970EMX-5.5.5-2.4.rel
GS970M series	awplus(config)# boot system GS970-5.5.5-2.4.rel
AR4050S-5G	awplus(config)# boot system AR4050S-5.5.5-2.4.rel
AR4050S	awplus(config)# boot system AR4050S-5.5.5-2.4.rel
AR3050S	awplus(config)# boot system AR3050S-5.5.5-2.4.rel
AR1050V	awplus(config)# boot system AR1050V-5.5.5-2.4.rel
ARX200S series	awplus(config)# boot system ARX200S-5.5.5-2.4.rel
TQ7613-R	awplus(config)# boot system TQ7613R-5.5.5-2.4.rel
TQ7403-R	awplus(config)# boot system TQ7403R-5.5.5-2.4.rel
TQ6702 GEN2-R	awplus(config)# boot system TQ6702GEN2R-5.5.5-2.4.rel
TQ6702e GEN2-R	awplus(config)# boot system TQ6702eGEN2R-5.5.5-2.4.rel
TQ3403-R	awplus(config)# boot system TQ3403R-5.5.5-2.4.rel

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

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

6. 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 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 the Wireless Controller (was Vista Manager mini).

Browse to the GUI

Note: In version 5.5.2-2.2, 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
```

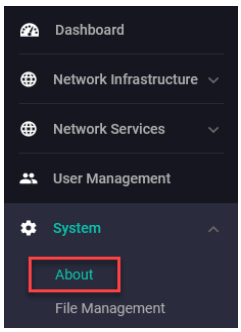
   Alternatively, on unconfigured devices you can use the default address, which is:

   - on switches: 169.254.42.42
   - on firewalls, routers and access points: 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 5.5.5-2.x is **2.22.0** or later.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 79 or "Update the GUI on routers and firewalls" on page 80.

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 v5.5.5-2.x is awplus-gui_555_40.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. 555) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

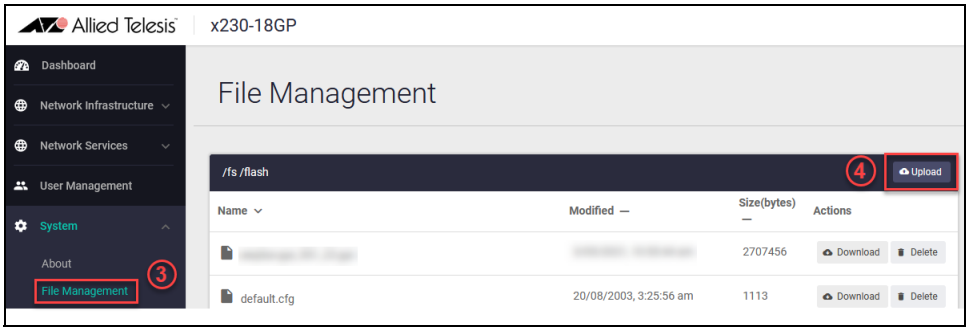
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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 routers and firewalls

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 v2.22.0 or later.