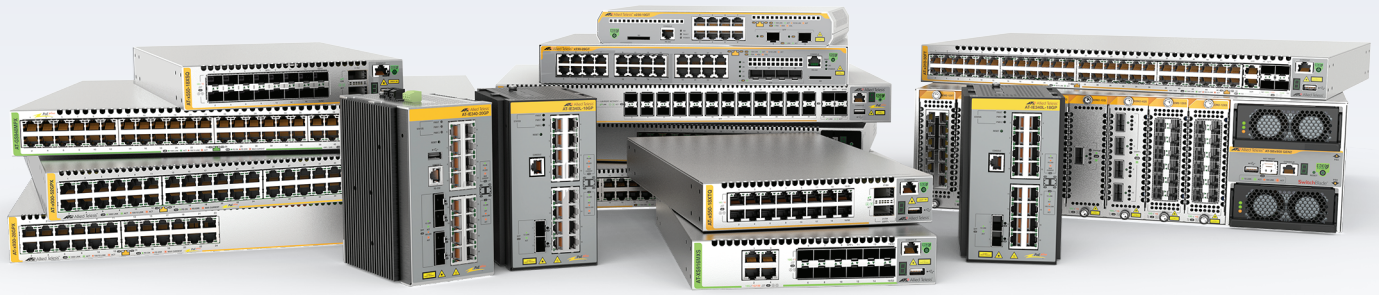
Release Note for AlliedWare Plus Software Version 5.5.5-1.x



AlliedWare Plus OPERATING SYSTEM

AMF Plus Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 Series
x220 Series
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series
SE250 Series
SE240 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall app
ARX200S Series
AR4000S-Cloud
AR4050S-5G
AR4050S
AR3050S
AR1050V
TQ7403-R
TQ6702 GEN2-R
TQ6702e GEN2-R

» 5.5.5-1.2 » 5.5.5-1.3

Acknowledgments

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

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see **www.openssl.org/**

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**.

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 5.5.5-1.3

Product families supported by this version:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
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 Series
x220 Series
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
TQ7403-R
TQ6702 GEN2-R
TQ6702e GEN2-R

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-1.3.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the Allied Telesis Support Portal. 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 37.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 39 . 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		10/2025	vaa-5.5.5-1.3.iso (VAA OS) vaa-5.5.5-1.3vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-1.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2025	SBx81CFC960-5.5.5-1.3.rel
SBx908 GEN2	SBx908 GEN2	10/2025	SBx908NG-5.5.5-1.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	10/2025	x950-5.5.5-1.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	10/2025	x930-5.5.5-1.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2025	x550-5.5.5-1.3.rel
x540L-28XTm x540L-28XS	x540L	10/2025	x540-5.5.5-1.3.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	10/2025	x530-5.5.5-1.3.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	10/2025	x530-5.5.5-1.3.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	10/2025	x330-5.5.5-1.3.rel
x320-10GH x320-11GPT	x320	10/2025	x320-5.5.5-1.3.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	10/2025	x250-5.5.5-1.3.rel

Table 1: Models and software file names

Models	Family	Date	Software File
x240-10GTXm x240-10GHXm x240-26GHXm	x240	10/2025	x240-5.5.5-1.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2025	x230-5.5.5-1.3.rel
x220-28GS x220-52GT x220-52GP	x220	10/2025	x220-5.5.5-1.3.rel
IE360-12GTX IE360-12GHX	IE360	10/2025	IE360-5.5.5-1.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	10/2025	IE340-5.5.5-1.3.rel
IE220-6GHX IE220-10GHX	IE220	10/2025	IE220-5.5.5-1.3.rel
IE210L-10GP IE210L-18GP	IE210L	10/2025	IE210-5.5.5-1.3.rel
SE540L-28XTm SE540L-28XS	SE540L	10/2025	SE540-5.5.5-1.3.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	10/2025	SE250-5.5.5-1.3.rel
SE240-10GTXm SE240-10GHXm	SE240	10/2025	SE240-5.5.5-1.3.rel
XS916MXT XS916MXS	XS900MX	10/2025	XS900-5.5.5-1.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	10/2025	GS980MX-5.5.5-1.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2025	GS980EM-5.5.5-1.3.rel
GS980M/52 GS980M/52PS	GS980M	10/2025	GS980M-5.5.5-1.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	10/2025	GS970EMX-5.5.5-1.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2025	GS970-5.5.5-1.3.rel
AR4000S-Cloud		10/2025	AR-4000S-Cloud-5.5.5-1.3.iso
ARX200S-GTX	ARX200S	10/2025	ARX200S-5.5.5-0.4.rel

Table 1: Models and software file names

Models	Family	Date	Software File
10GbE UTM Firewall		10/2025	ATVSTAPL-1.10.1.iso and vfw-x86_64-5.5.5-1.3.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	10/2025	AR4050S-5.5.5-1.3rel AR3050S-5.5.5-1.3.rel
AR1050V	AR-Series VPN routers	10/2025	AR1050V-5.5.5-1.3.rel
TQ7403-R	Wireless AP Router	10/2025	TQ7403R-5.5.5-1.3.rel
TQ6702 GEN2-R TQ6702e GEN2-R	Wireless AP Router	10/2025	TQ6702GEN2R-5.5.5-1.3.rel TQ6702GEN2R-5.5.5-1.3.rel

Caution: Software version 5.5.5-1.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 33.
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 35.

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

The 5.5.5-1.3 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.5-1.3

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	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-87580	**AMF**	Previously, a command line interface error could occur while resizing the terminal window. 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-87775	**API, Apteryx, NETCONF**	Previously, in some instances API calls to certain nodes would fail if the full web API path to the node was requested due to the way the data for these nodes was provided. 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
CR-87135	**CLI, Link Aggregation**	Previously, ports added to an aggregator did not appear in the output of the **`show platform port`** 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
CR-87175	**CPU, Switchports**	Previously, connecting or disconnecting switchports could result in higher than expected CPU utilisation. 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	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-87791	**Device GUI, Device Security, HTTP service**	Previously, on TQ-R platforms, the HTTP server could disable indefinitely when the manager password was changed. This has been corrected to re-enable after a few seconds.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y
ER-7198	**DHCPv6, IPv6**	Previously, when an interface running a DHCPv6 client in Prefix Delegation mode was shut down and brought back up, the client was incorrectly reinitialized in NDP mode. This issue has now been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	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-86805	**IGMP, Tunnel**	Previously, on devices configured with tunnels, IGMP could stop working on VLAN interfaces. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	Y
CR-87592	**IPsec, ISAKMP**	Previously, VPN connections from some Windows clients could fail to establish if the client sent a large number of root certificates, which exceeded the maximum packet size accepted by the router. This issue has now been resolved, and the maximum packet size has been increased.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	Y	Y
CR-87254	**Pluggable Transceivers**	Previously, the SP10TMI module could fail to link up on the x330 platform. This issue has been resolved.	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	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-87679	**PoE**	Previously, executing the **`show platform power-inline`** command on an x240-52GHXm or x250/x540L-28XHm would result in I/O errors recorded in the log. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	Y	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-86567	**Port Authentication**	Previously, on affected stacked platforms with port authentication configured, it was possible for switch lockup to occur if many supplicants joined in a short period of time. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	Y	-	-	-	-	-	-	-
CR-87577	**Port Authentication**	Previously, the **`auth supplicant-audit enable`** command was missing from some IE platforms. This issue has been resolved.	-	-	-	-	-	Y	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-87620	**Port Configuration**	Previously, AT-SPSX could fail to link up on SFPP ports when configured for 1000MFull. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-87694	**Port Configuration**	Previously, after 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	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-
ER-4913	**RADIUS**	With this software revision, login to console, Telnet, and SSH with user names including '@' characters (e.g. email address) are now supported. 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	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	SE540/SE540L	SE250	SE240	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200	TQ-R Series
CR-87629	**SSH**	Previously, in extremely rare circumstances, it was possible for an unexpected reboot to occur when disconnecting via SSH, on a TQ6702 Gen2-R TQ Router. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y
CR-86975	**Switching**	Previously, some platforms could send packets through copper ports with an inter-packet gap (IPG) smaller than 8 bytes, which could cause the receiving device to drop those packets. This issue has been resolved.	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-87470	**Traffic Control**	Previously, when a traffic-control rule was applied to an entity with a sub-interface, after a reboot the traffic-control rule would no longer be applied to the sub-interface. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	Y	Y
CR-87598	**VCStack**	Previously, under a specific rare condition where a stack member was repeatedly rebooting, it was possible for the VCStack master to undergo an unexpected reboot. This issue has been resolved.	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	Y	-	-	-	-	-	-	-
CR-87770	**Wireless Radio**	Previously, when the same MAC filter list was applied to different networks/VAPs, it was duplicated in the wireless configuration for each network. This may have resulted in fewer MAC filter entries being able to be applied to the device. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y

What's New in Version 5.5.5-1.2

Product families supported by this version:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
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 Series
x220 Series
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
TQ7403-R
TQ6702 GEN2-R

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-1.2.

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 37.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 39. 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		08/2025	vaa-5.5.5-1.2.iso (VAA OS) vaa-5.5.5-1.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-1.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2025	SBx81CFC960-5.5.5-1.2.rel
SBx908 GEN2	SBx908 GEN2	08/2025	SBx908NG-5.5.5-1.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	08/2025	x950-5.5.5-1.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	08/2025	x930-5.5.5-1.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2025	x550-5.5.5-1.2.rel
x540L-28XTm x540L-28XS	x540L	08/2025	x540-5.5.5-1.2.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	08/2025	x530-5.5.5-1.2.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	08/2025	x530-5.5.5-1.2.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	08/2025	x330-5.5.5-1.2.rel
x320-10GH x320-11GPT	x320	08/2025	x320-5.5.5-1.2.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	08/2025	x250-5.5.5-1.2.rel

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

Models	Family	Date	Software File
x240-10GTXm x240-10GHXm x240-26GHXm	x240	08/2025	x240-5.5.5-1.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2025	x230-5.5.5-1.2.rel
x220-28GS x220-52GT x220-52GP	x220	08/2025	x220-5.5.5-1.2.rel
IE360-12GTX IE360-12GHX	IE360	08/2025	IE360-5.5.5-1.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	08/2025	IE340-5.5.5-1.2.rel
IE220-6GHX IE220-10GHX	IE220	08/2025	IE220-5.5.5-1.2.rel
IE210L-10GP IE210L-18GP	IE210L	08/2025	IE210-5.5.5-1.2.rel
SE540L-28XTm SE540L-28XS	SE540L	08/2025	SE540-5.5.5-1.2.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	08/2025	SE250-5.5.5-1.2.rel
SE240-10GTXm SE240-10GHXm	SE240	08/2025	SE240-5.5.5-1.2.rel
XS916MXT XS916MXS	XS900MX	08/2025	XS900-5.5.5-1.2.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	08/2025	GS980MX-5.5.5-1.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	08/2025	GS980EM-5.5.5-1.2.rel
GS980M/52 GS980M/52PS	GS980M	08/2025	GS980M-5.5.5-1.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	08/2025	GS970EMX-5.5.5-1.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2025	GS970-5.5.5-1.2.rel
AR4000S-Cloud		08/2025	AR-4000S-Cloud-5.5.5-1.2.iso
ARX200S-GT ARX200S-GTX	ARX200S	08/2025	ARX200S-5.5.5-1.2.rel

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

Models	Family	Date	Software File
10GbE UTM Firewall app		08/2025	ATVSTAPL-1.12.1.iso and vfw-x86_64-5.5.5-1.2.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	08/2025	AR4050S-5.5.5-1.2.rel AR3050S-5.5.5-1.2.rel
AR1050V	AR-Series VPN routers	08/2025	AR1050V-5.5.5-1.2.rel
TQ7403-R	TQR Wireless AP Router	08/2025	TQ7403R-5.5.5-1.2.rel
TQ6702 GEN2-R	TQR Wireless AP Router	08/2025	TQ6702GEN2R-5.5.5-1.2.rel

Caution: Software version 5.5.5-1.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 33 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 35.

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

The 5.5.5-1.2 software version is **not** ISSU compatible with previous software versions.

OpenSSH

As part of this software update, **OpenSSH** has been upgraded to **version 9.9p2**. This upgrade is supported starting from version 5.5.5-1.1.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.5-1.2:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 31.

AMF Plus host key change

Applies to all AlliedWare Plus devices

From version 5.5.5-1.2 onwards, the type of host keys used by AMF Plus have changed. You do not have to change your AMF Plus network because of this, but devices running releases **earlier than 5.4.5-0.1** are not fully compatible with devices running 5.5.5-1.2 onwards. See "AMF Plus software version compatibility" on page 29 for details.

Using an ACL to deny or permit Directed Broadcasts

Applies to all AlliedWare Plus devices that support ACLs

From version 5.5.5-1.2 onwards, IP directed broadcasts can be restricted using an Access Control List (ACL).

Directed broadcasts can be useful (e.g., for Wake-on-LAN), but they can also be abused (e.g., for network attacks like smurf attacks). This means it's useful to limit which source IP addresses are allowed to send these broadcasts.

What is an IP Directed Broadcast?

An IP directed broadcast is a broadcast message that is sent to all devices in a specific subnet, but is sent from outside that subnet.

How it works

A device outside the target subnet sends a packet to the subnet's broadcast address. Routers and devices outside the subnet treat this packet like a normal message and forward it as a unicast message.

When the packet reaches a device inside the target subnet (and that device has directed broadcast enabled), it changes the packet into a Layer 2 broadcast message. This means it sends the message to all devices in the subnet using a special MAC address: FF:FF:FF:FF:FF:FF.

Security Control with an ACL

You can use an ACL to decide which source IP addresses are allowed to send these broadcasts. If a packet comes from an IP that's not allowed, it gets blocked (dropped). If it's allowed, it gets forwarded. By default, if a packet doesn't match any rule in the ACL, it's blocked.

To use an ACL:

1. Create the desired named or numbered software ACL

For example, to permit only directed broadcasts from 10.1.1.1/32, you can use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard Example-ACL
awplus(config-ip-std-acl)# permit 10.1.1.1/32
awplus(config-ip-std-acl)# exit
```

2. Apply the ACL to Directed Broadcasts on an interface (for example, VLAN2):

```
awplus(config)# interface vlan2
awplus(config-if)# ip directed-broadcast Example-ACL
```

Static numbering for device Resource ID

Applies to x530DP-28GHXm, x530DP-52GHXm, x930, x950, SBx908 GEN2 and SBx8100 Series

From version 5.5.5-1.2 onwards, the Resource ID for each bay and board will persist through reboots. The Resource ID is a unique identifier assigned to resources within a device for easy reference. There are two classes of resources: 'bay' and 'board.' Bay resources are associated with sensors that monitor a device bay and provide events based on a GPIO input. Board resources consist of sensors that are attached to a specific board.

You can use the following command to view Resource IDs:

```
awplus# show system environment
```

Previously, Resource IDs were assigned sequentially as they were added. Fixed Resource IDs received the initial numbers (1-5 in the example below), while hot swappable boards were added based on detection order. If a board was swapped in later, it would get the last Resource ID and might receive a different ID upon reboot.

Now, the Resource ID of bays will be fixed to the board index that the bay belongs to, and boards will be fixed to the board index that the board belongs to, plus 100.

Table 2: Previous Resource IDs list (example for the x950-28XTQm):

```
Resource ID: 1   Name: PSU Bay A (AT-PWR600)
Resource ID: 2   Name: PSU Bay B ()
Resource ID: 3   Name: Fan Bay A (AT-FAN05)
Resource ID: 4   Name: Fan Bay B (AT-FAN05)
Resource ID: 5   Name: AT-x950-28XTQm
Resource ID: 6   Name: AT-PWR600
Resource ID: 7   Name: AT-FAN05
Resource ID: 8   Name: AT-FAN05
Resource ID: 9   Name: AT-XEM2-4QS  Bay: 1
```

Table 3: After rebooting, the list could change to this:

```
Resource ID: 1   Name: PSU Bay A (AT-PWR600)
Resource ID: 2   Name: PSU Bay B ()
Resource ID: 3   Name: Fan Bay A (AT-FAN05)
Resource ID: 4   Name: Fan Bay B (AT-FAN05)
Resource ID: 5   Name: AT-x950-28XTQm
Resource ID: 6   Name: AT-XEM2-4QS  Bay: 1
Resource ID: 7   Name: AT-PWR600
Resource ID: 8   Name: AT-FAN05
Resource ID: 9   Name: AT-FAN05
```

Table 4: Now, the list will change to this - and not change after reboots:

```
Resource ID: 2   Name: PSU Bay A (AT-PWR600)
Resource ID: 3   Name: PSU Bay B ()
Resource ID: 4   Name: Fan Bay A (AT-FAN05)
Resource ID: 5   Name: Fan Bay B (AT-FAN05)
Resource ID: 100  Name: AT-x950-28XTQm
Resource ID: 101  Name: AT-XEM2-4QS  Bay: 1
Resource ID: 102  Name: AT-PWR600
Resource ID: 104  Name: AT-FAN05
Resource ID: 105  Name: AT-FAN05
```

The Resource ID can be observed in the output of the **show system environment** command.

Increase in the number of AMF Plus and AWC nodes for x540L series switches

From version 5.5.5-1.2 onwards, x540L series switches support an increased number of AMF Plus and AWC nodes (APs). Now a total of 100 AMF Plus nodes and/or APs are supported. This total is flexible. For example, you can buy licenses for 20 AMF Plus nodes and 80 APs, or for 30 AMF Plus nodes and 70 APs, and so on.

UDP transport for PTP on x530 and x530L series switches

From version 5.5.5-1.2 onwards, x530 and x530L Series switches support PTP (Precision Time Protocol) over UDP transport.

This feature is an extension to our existing PTP support. Previously, PTP operated only over Layer 2 (L2) transport. With this release, PTP packets can now also be transported using Layer 4 (UDP), supporting both unicast and multicast transmission.

Configuration notes

PTP over UDP works for both IPv4 and IPv6 and the packets can be unicast or multicast.

To enable PTP over UDP with IPv4, use the following command:

```
ptp-clk transparent transport-type udp v4 delay-mechanism e2e
step-type onestep
```

For IPv4, the following multicast addresses are supported:

- 224.0.1.129
- 224.0.1.130
- 224.0.1.131
- 224.0.1.132

To enable PTP over UDP with IPv6, use the following command:

```
ptp-clk transparent transport-type udp v6 delay-mechanism e2e
step-type onestep
```

For IPv6, the following multicast address is supported:

- FF0x::181

Benefits

PTP over UDP offers several key advantages over traditional Layer 2 (Ethernet-based) transport:

1. Network Flexibility: Enables time synchronization across routed Layer 3 networks, ideal for large or segmented environments.

2. IPv4/IPv6 Compatibility: Supports both protocols, ensuring adaptability and future readiness.

3. Multicast and Unicast Options: Offers flexible deployment models for both broad and targeted synchronization.

4. Infrastructure Integration: Easier to manage with existing network devices, firewalls, and QoS policies.

5. Cloud and Virtualization Friendly: Better suited for modern data centres and hybrid cloud environments.

6. Standards-Based: Compliant with IEEE 1588-2008 (PTPv2), ensuring broad interoperability.

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

PTP end-to-end transparent clock on x240, x250 and x540L series switches

From version 5.5.5-1.2 onwards, Transparent Clock support is now available on the x240, x250, and x540L platforms.

What is PTP Transparent Clock?

The Precision Time Protocol (PTP), defined by the IEEE 1588-2008 standard (PTPv2), enables precise time synchronization across networked devices. A Transparent Clock improves timing accuracy by measuring and correcting for the time a PTP packet spends traversing a network switch. This ensures minimal jitter and drift in time-sensitive applications

Commands used with PTP Transparent Clock:

- clock-port
- ptp-clk
- ptp global
- show ptp data transparent
- show ptp port

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

Dynamic ACLs via port authentication on IE340 series switches

From version 5.5.5-1.2 onwards, dynamic ACLs (Access Control Lists) via Port Authentication are supported on the IE340 switch.

What is Dynamic ACL via port authentication?

It's a way to control network access more precisely for devices (called supplicants) that connect to switch ports and get authenticated using methods like:

- 802.1X
- MAC-based Authentication
- Web-based Authentication

Key concepts

Dynamic ACLs are rules that are:

- applied automatically to a switch port when a device is authenticated.
- defined on the RADIUS server (based on username or MAC address).
- removed when the device disconnects or becomes unauthenticated.

These ACLs can filter traffic based on:

- IPv4/IPv6 addressing, and protocols like ICMP, UDP, TCP, etc.

Dynamic ACLs can work alongside static ACLs, but once dynamic ACLs are active, you can't add new static ACLs to that port.

A real-world example

Employee: Bob (HR Manager). Bob connects his laptop to an Ethernet port. He’s authenticated via MAC-based authentication.

The RADIUS server sends an ACL to:

- allow access to HR systems.
- block access to development servers.

Bob gets the correct network access based on his role.

For more information on ACLs and port authentication, see the AAA and Port Authentication Feature Overview and Configuration Guide.

PIM-SSM support for AR and ARX Series

Applies to AR4000S-Cloud, AR-Series, ARX200S Series devices

From version 5.5.5-1.2 onwards, the AR4000S-Cloud, AR-Series, and ARX200S Series firewalls and routers support PIM-SSM. The following commands are supported:

```
ip pim ssm default
ipv6 pim ssm default
```

Note that SSM mapping cannot be used on these devices, which means that multicast hosts must use:

- IPv4 hosts: IGMPv3, not IGMPv1 or v2
- IPv6 hosts: MLDv2.

For more information, see the PIM-SM Feature Overview and Configuration Guide.

Fixed secondary IP address on DHCP-configured eth interfaces

Applies to AR4050S, AR3050S, AR1050V, AR4000S-Cloud, 10GbE UTM Firewall app, ARX200S Series and TQR Series

From version 5.5.5-1.2 onwards, you can configure a secondary IP address on eth interfaces that use DHCP to obtain their IP addresses.

For more information, see the Dynamic Host Configuration Protocol Feature Overview and Configuration Guide.

Manage up to 50 APs using Vista Manager mini on the ARX200S-GTX

From version 5.5.5-1.2 onwards, Vista Manager mini supports the management of up to 50 APs on the ARX200S-GTX firewall. 20 APs can be managed for free, and up to an additional 30 APs with a feature license (up to the 50 AP maximum); see the datasheet for license details.

For more information, see the AWC with Vista Manager mini User Guide.

Increase in supported operating temperature range for the ARX200S-GTX

From version 5.5.5-1.2 onwards, the supported operating temperature range is 0-60 degrees Celsius. Previously the maximum supported operating temperature was 50 degrees Celsius. This change does not require any user configuration.

Automatic notification of new maintenance releases for wireless devices

Applies to AR4050S-5G, TQ6702 GEN2-R and TQ7403-R devices

From version 5.5.5-1.2 onwards, the AlliedWare Plus Update Manager will periodically check for newer maintenance firmware release files and new GUI files. If a newer file is available you will see a notification via an alert log message which will appear on the CLI. The GUI will also display a banner message.

Note that the firmware file notification is only for maintenance firmware releases, not minor or major releases. For example, if your device is running 5.5.5-1.2, you will be notified when 5.5.5-1.2 becomes available, but not when 5.5.5-2.1 does.

You must download the file and install it. You can download it using the commands:

```
awplus# update awplus_maint_rel now
awplus# update webgui now
```

When the device downloads a new firmware file, it saves it to the root flash directory. You can then set this as the current boot image. For step-by-step instructions, see "Installing this Software Version" on page 37.

When the device downloads a new GUI file, it saves the file and then restarts the HTTP server with the new version.

You can disable either or both of the notifications by using the commands:

```
awplus# configure terminal
awplus(config)# firmware-update notify-interval never
awplus(config)# gui notify-interval never
```

For more information about the update manager, see the Update Manager Feature Overview and Configuration Guide.

MAC filtering per VAP support for TQR Series

From version 5.5.5-1.2 onwards, MAC Filtering has been enhanced to allow configuration per Virtual Access Point (VAP) on TQR series wireless AP routers.

Previously, MAC Filtering was limited to a single list per AP profile. With this update, administrators can assign individual MAC filter lists to specific networks, which correspond to specific VAPs. This enables more precise control over device access across multiple SSIDs.

Key enhancements

- **Per-VAP MAC Filtering**: Apply MAC filter lists at the network level, allowing unique rules per VAP.
- **Flexible List Management**: Define up to 48 MAC filter lists, each with a unique ID, optional description, and a set of MAC addresses.
- **Permit/Deny Rules**: Each list can permit or deny access. If applied at the AP profile level, its rule overrides the list-level setting.
- **Extended CLI Support**: The CLI now supports MAC Filtering configuration at both the AP profile and network levels.

This feature is especially useful in environments with multiple SSIDs, where different access policies are needed for different user groups or device types—such as separating guest and corporate traffic.

Note: When both AP profile and VAP-level filters are configured, the AP profile setting takes precedence and overrides the VAP-level setting.

New commands

There are two new commands available:

rule {permit|deny}

This command sets whether the selected MAC filter list permits or denies access. For example, to set the rule to 'permit' for mac-filter 1:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# mac-filter 1
awplus(config-wireless-mac-flt)# rule permit
```

wireless-mac-filter-id

This command enables MAC filtering on a specific VAP. You can specify either:

- A **MAC filter list ID**, or
- The key word **profile**, which tells the VAP to use the MAC filter configured in the AP profile.

For example, to apply the global MAC filter (configured in the AP profile) to VAPs using network 100, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 100
awplus(config-wireless-network)# wireless-mac-filter-id
profile
```

Updated command

show wireless wireless-mac-filter

This command now lets you choose to display a MAC filter ID or range of IDs:

```
awplus# show wireless wireless-mac-filter [<macfilter-id>|all]
[brief]
```

```
...
WIRELESS MAC FILTER ID 100:
  Description ................... Floor 1
  Rule ........................... deny
  Entries ........................ 3
  Entries ........................ 2
    MAC address    Description
    -------------- ---------------
    1234.5678.abcd PC lab 1
    0987.6543.abcd guest
    abcd.9876.5432

WIRELESS MAC FILTER ID 200:
  Description ...................
  Entries ........................ 0
```

RADIUS over TLS support for TQR Series

From version 5.5.5-1.2 onwards, RADIUS over TLS is supported on TQR Series wireless AP routers. RadSec is an extension to the RADIUS authentication protocol that uses Transport Layer Security (TLS) as the transport protocol. It provides improved security over the standard RADIUS protocol.

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

FindMe support for TQR Series

From AlliedWare Plus version 5.5.5-1.2 onwards, the **FindMe** feature is supported on the TQR Series.

Find a device using the CLI

Use this command to physically locate a specific device from a group of similar devices. Activating the command causes a selected number of port LEDs to alternately flash green then amber (if that device has amber LEDs) at a rate of 1 Hz:

```
findme [interface <port-list>] [timeout <duration>]
```

Use the **no** variant of this command to deactivate the FindMe feature prior to the timeout expiring.

Examples

To activate the FindMe feature for the default duration (60 seconds) on all ports, use the following command:

```
awplus# findme
```

To activate the Find Me feature for 120 seconds on all ports, use the following command:

```
awplus# findme timeout 120
```

Clean up unused wireless settings when pulling them from the AWC plugin

Applies to TQR Series

Previously, when configurations were managed via the AWC plugin, the wireless TQR device could detect a mismatch in the configuration hash and create a new instance using an available ID. Frequent changes made through the plugin could result in large configuration files, which could trigger a "Failed to start Wireless Firmware Loader" error during reboot. This error could cause the TQR device to enter a reboot loop.

From version 5.5.5-1.2 onwards, you can avoid this issue by using the new **clean-up** parameter when fetching the current running wireless configuration from the AWC plugin:

```
awplus# wireless ap-configuration pull ap local clean-up
```

This new optional parameter removes any unused wireless configurations in the following areas: Network, Security, RADIUS Server Group, and wireless MAC Filters.

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

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 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 25 and "Details for x930 Series" on page 26 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.

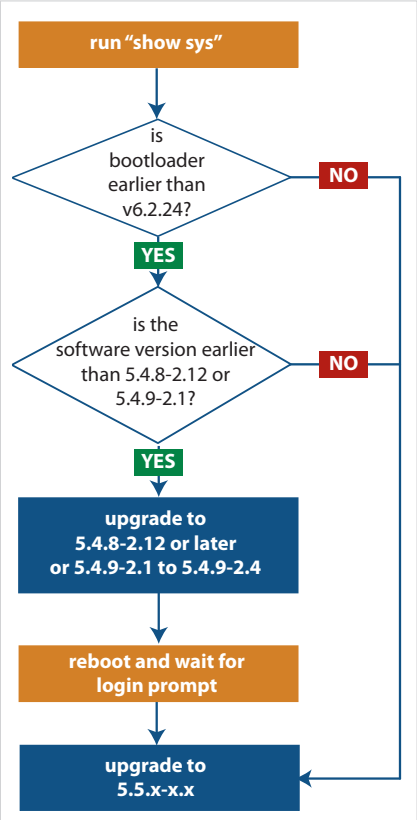
Instead, before upgrading from one of those versions to the current version, make sure your switch is running one of these specified versions:

- 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:

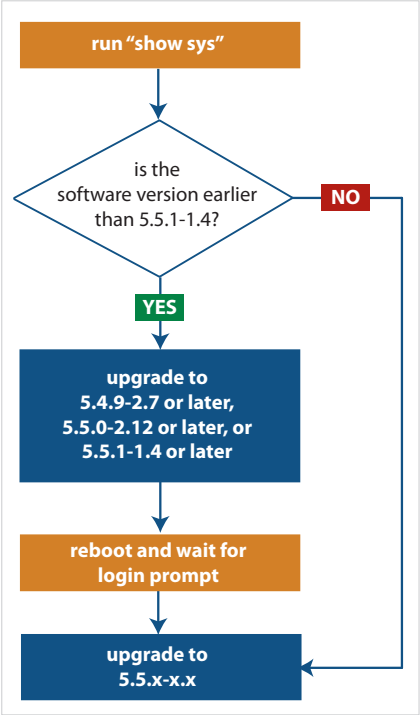
```
awplus# show system
```



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 33 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 35.

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. However, if this is not possible, then nodes running this version are fully compatible with nodes running 5.4.5-0.1 onwards.

From version 5.5.5-1.2 onwards, the type of host keys used by AMF Plus have changed. You do not have to change your AMF Plus network because of this, but devices running releases **earlier than 5.4.5-0.1** will no longer be able to:

- Use the command **atmf remote-login <node>** to connect to a device running the new software
- Use a number of commands in a single-node working set to a device running the new software. A single-node working set is created using the command **atmf working-set <node>**. The affected commands are:
  - 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:

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

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

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

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

In summary, the process for upgrading firmware on an AMF 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.

Obtaining User Documentation

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

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

Verifying the Release File

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 5.5.5-1.3 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 5.5.5-1.3

Product family	Software File	Hash
AMF Plus Cloud	vaa-5.5.5-1.3.rel	360bfa34d9cc0e326c64046b61597ec47705196628eff35260c40810f7ad1d
SBx8100	SBx81CFC960-5.5.5-1.3.rel	564c98ae8afa7a6e195fe55c85ff48fa61ed292784f8bab920696c
SBx908 GEN2	SBx908NG-5.5.5-1.3.rel	4069fed4b8868f6aeb7d71bb38163012ff86bf3b4625b1e765c2f16a8
x950	x950-5.5.5-1.3.rel	4069fed4b8868f6aeb7d71bb38163012ff86bf3b4625b1e765c2f16a8e90f
x930	x930-5.5.5-1.3.rel	10d56a7985546e5b71b7baeabc0938d26ceee7b39b72efcb4137dc2bd15bb
x550	x550-5.5.5-1.3.rel	3ae18e06e69fea70bdce46f29798c96123dc9a0b89c9bfc86acb0a689e7a0
x540L	x540-5.5.5-1.3.rel	66aec0bc924da61a4f052fc40567640d4a9e3fb4c7810b24f28f3c3be0248
x530 & x530L	x530-5.5.5-1.3.rel	14b3b9d40f143b74541e71b3e2be229b78c76fa52bbc70487e5daad9ff1a5

Table: Hash values for 5.5.5-1.3

Product family	Software File	Hash
x330	x330-5.5.5-1.3.rel	7942bea8b453c9d6f993d5400491194fd609aa2ad84aea74121c64a007b53
x320	x320-5.5.5-1.3.rel	14b3b9d40f143b74541e71b3e2be229b78c76fa52bbc70487e5daad9ff1a5
x250	x250-5.5.5-1.3.rel	dc5f3f4175406507bf9a8859971d216aa70e22a6e2a54a32b8514508c2766
x240	x240-5.5.5-1.3.rel	9dfdf2b28410b43c144bf7b6207a5b1ffbabe3260e3c7b659b77315f43d9d
x230 & x230L	x230-5.5.5-1.3.rel	cd5733a9180071e54dae38aaab9634656adcdfb7bbf5682c8982b7b9130e7
x220	x220-5.5.5-1.3.rel	ee99592ce0c6786d4364b9a6ba505315b1359cdf803e0ec1670f6701d2818
IE360	IE360-5.5.5-1.3.rel	ba39708c9986a2d1dae425e227104c5c7ff4ea55c24a49c6a8f6c69394e6
IE340 & IE340L	IE340-5.5.5-1.3.rel	52b3afd9e4d98b21f4f39b9a63c305be9270b5bec858f1d4fd18a7498945
IE220	IE220-5.5.5-1.3.rel	3bef41e5efe9ef1f0c260c89e0d080e9dd8e4fca9ee421346348d7b45dfb
IE210L	IE210-5.5.5-1.3.rel	cd5733a9180071e54dae38aaab9634656adcdfb7bbf5682c8982b7b9130e
SE540L	SE540-5.5.5-1.3.rel	66aec0bc924da61a4f052fc40567640d4a9e3fb4c7810b24f28f3c3be024
SE250	SE250-5.5.5-1.3.rel	dc5f3f4175406507bf9a8859971d216aa70e22a6e2a54a32b8514508c276
SE240	SE240-5.5.5-1.3.rel	9dfdf2b28410b43c144bf7b6207a5b1ffbabe3260e3c7b659b77315f43d9
XS900MX	XS900-5.5.5-1.3.rel	aa945ea79f35d562f05d03f7971b4cd7ed30fc180b5e69a48b377349c92b
GS980MX	GS980MX-5.5.5-1.3.rel	14b3b9d40f143b74541e71b3e2be229b78c76fa52bbc70487e5daad9ff
GS980EM	GS980EM-5.5.5-1.3.rel	14b3b9d40f143b74541e71b3e2be229b78c76fa52bbc70487e5daad9ff
GS980M	GS980M-5.5.5-1.3.rel	ee99592ce0c6786d4364b9a6ba505315b1359cdf803e0ec1670f6701d28
GS970EMX	GS970EMX-5.5.5-1.3.rel	7942bea8b453c9d6f993d5400491194fd609aa2ad84aea74121c64a00
GS970M	GS970-5.5.5-1.3.rel	cd5733a9180071e54dae38aaab9634656adcdfb7bbf5682c8982b7b9130e
ARX200S	ARX200S-5.5.5-1.3.rel	b83ba99eaa40d446a9bfb46fffae3961fe42578750f217f32ef3104753
AR4050S-5G	AR4050S-5.5.5-1.3.rel	6373f28379197d7fef4fe0acb8cea4d8905455e014672770d690458113
AR4050S	AR4050S-5.5.5-1.3.rel	6373f28379197d7fef4fe0acb8cea4d8905455e014672770d690458113
AR3050S	AR3050S-5.5.5-1.3.rel	6373f28379197d7fef4fe0acb8cea4d8905455e014672770d690458113
AR1050V	AR1050V-5.5.5-1.3.rel	cd41281d5f662e5e963477587ffaf4ca6907826cecce581f71c2e6f232
TQ6702 GEN2-R	TQ6702GEN2R-5.5.5-1.3.rel	a3b5d306263b58d62f7706d6a670c997ce5bef3661e81a209c1986
TQ6702e GEN2-R	TQ6702eGEN2R-5.5.5-1.3.rel	c95d3c3f4f4e62c75db8733115c6e82a51442d37a55fcb60c4b94
TQ7403-R	TQ7403R-5.5.5-1.3.rel	b060c7c1a0e4e65e7391ad4fb56e12b01a1c484f3a750869aee0ecba11

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 33 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 35.

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 SBx8100-5.5.5-1.3.rel`
SBx908 GEN2	`awplus(config)# boot system ARX200S-5.5.5-1.3.rel`
x950 series	`awplus(config)# boot system x950-5.5.5-1.3.rel`
x930 series	`awplus(config)# boot system x930-5.5.5-1.3.rel`
x550 series	`awplus(config)# boot system x550-5.5.5-1.3.rel`
x540L series	`awplus(config)# boot system x540-5.5.5-1.3.rel`
x530 series	`awplus(config)# boot system x530-5.5.5-1.3.rel`

Product	Command
x330 series	awplus(config)# boot system x330-5.5.5-1.3.rel
x320 series	awplus(config)# boot system x320-5.5.5-1.3.rel
x250 series	awplus(config)# boot system x250-5.5.5-1.3.rel
x240 series	awplus(config)# boot system x240-5.5.5-1.3.rel
x230 series	awplus(config)# boot system x230-5.5.5-1.3.rel
x220 series	awplus(config)# boot system x220-5.5.5-1.3.rel
IE360 series	awplus(config)# boot system IE360-5.5.5-1.3.rel
IE340 series	awplus(config)# boot system IE340-5.5.5-1.3.rel
IE220 series	awplus(config)# boot system IE220-5.5.5-1.3.rel
IE210L series	awplus(config)# boot system IE210-5.5.5-1.3.rel
SE540L series	awplus(config)# boot system SE540-5.5.5-1.3.rel
SE250 series	awplus(config)# boot system SE250-5.5.5-1.3.rel
SE240 series	awplus(config)# boot system SE240-5.5.5-1.3.rel
XS900MX series	awplus(config)# boot system XS900-5.5.5-1.3.rel
GS980M series	awplus(config)# boot system GS980M-5.5.5-1.3.rel
GS980EM series	awplus(config)# boot system GS980EM-5.5.5-1.3.rel
GS980MX series	awplus(config)# boot system GS980MX-5.5.5-1.3.rel
GS970EMX series	awplus(config)# boot system GS970EMX-5.5.5-1.3.rel
GS970M series	awplus(config)# boot system GS970-5.5.5-1.3.rel
AR4050S-5G	awplus(config)# boot system AR4050S-5.5.5-1.3.rel
AR4050S	awplus(config)# boot system AR4050S-5.5.5-1.3.rel
AR3050S	awplus(config)# boot system AR3050S-5.5.5-1.3.rel
AR1050V	awplus(config)# boot system AR1050V-5.5.5-1.3.rel
ARX200S series	awplus(config)# boot system ARX200S-5.5.5-1.3.rel
TQ6702 GEN2-R	awplus(config)# boot system TQ6702GEN2R-5.5.5-1.3.rel
TQ6702e GEN2-R	awplus(config)# boot system TQ6702eGEN2R-5.5.5-1.3.rel
TQ7403-R	awplus(config)# boot system TQ7403R-5.5.5-1.3.rel

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

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

5. Reboot using the new software version.

```
awplus# reload
```

Accessing and Updating the Web-based GUI

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

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

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

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

Browse to the GUI

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

Perform the following steps to browse to the GUI.

1. If you haven't already, add an IP address to an interface. For example:

   ```
   awplus> enable
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)# ip address 192.168.1.1/24
   ```

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

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

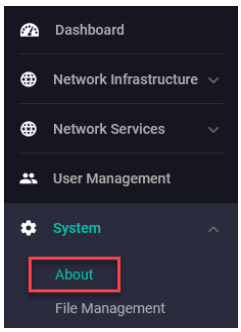
2. Open a web browser and browse to the IP address from step 1.

3. The GUI starts up and displays a login screen. Log in with your username and password. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the **System** > **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.5-1.x is **2.21.0**.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 40 or "Update the GUI on AR-Series devices" on page 41.



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 v5.5.5-1.x is awplus-gui_555_39.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:

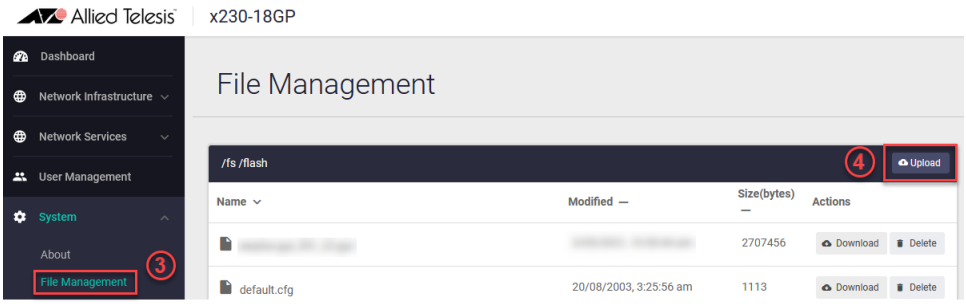
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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 AR-Series devices

Prerequisite: On AR-Series devices, if the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

Perform the following steps if you have been running an earlier version of the GUI and need to update it.

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

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

3. Browse to the GUI and check that you have the latest version now, on the **System** > **About** page. You should have v2.21.0 or later.