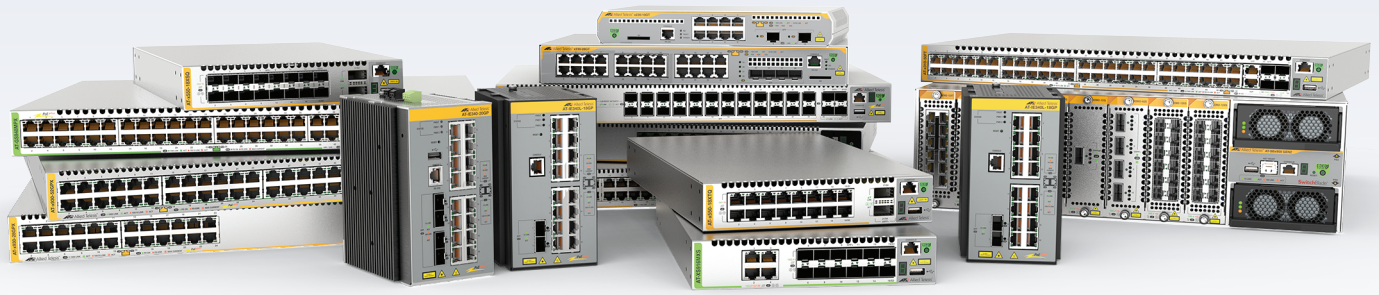
Release Note for AlliedWare Plus Software Version 5.5.4-0.x



AlliedWare Plus OPERATING SYSTEM

AMF Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x240 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE240 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S-5G
AR4050S
AR3050S
AR1050V
TQ6702 GEN2-R

» 5.5.4-0.1 » 5.5.4-0.3 » 5.5.4-0.5

Acknowledgments

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 5.5.4-0.5

Product families supported by this version:

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

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-0.5.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the Software Download area of the Allied Telesis website. 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 49.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 51. 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		08/2024	vaa-5.5.4-0.5.iso (VAA OS) vaa-5.5.4-0.5.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-0.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2024	SBx81CFC960-5.5.4-0.5.rel
SBx908 GEN2	SBx908 GEN2	08/2024	SBx908NG-5.5.4-0.5.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	08/2024	x950-5.5.4-0.5.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	08/2024	x930-5.5.4-0.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2024	x550-5.5.4-0.5.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	08/2024	x530-5.5.4-0.5.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	08/2024	x330-5.5.4-0.5.rel
x320-10GH x320-11GPT	x320	08/2024	x320-5.5.4-0.5.rel
x240-10GTXm x240-10GHXm	x240	08/2024	x240-5.5.4-0.5.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2024	x230-5.5.4-0.5.rel
x220-28GS x220-52GT x220-52GP	x220	08/2024	x220-5.5.4-0.5.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	08/2024	IE340-5.5.4-0.5.rel
IE220-6GHX IE220-10GHX	IE220	08/2024	IE220-5.5.4-0.5.rel

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

Models	Family	Date	Software File
IE210L-10GP IE210L-18GP	IE210L	08/2024	IE210-5.5.4-0.5.rel
SE240-10GTXm SE240-10GHXm	SE240	08/2024	SE240-5.5.4-0.5.rel
XS916MXT XS916MXS	XS900MX	08/2024	XS900-5.5.4-0.5.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	08/2024	GS980MX-5.5.4-0.5.rel
GS980EM/10H GS980EM/11PT	GS980EM	08/2024	GS980EM-5.5.4-0.5.rel
GS980M/52 GS980M/52PS	GS980M	08/2024	GS980M-5.5.4-0.5.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	08/2024	GS970EMX-5.5.4-0.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2024	GS970-5.5.4-0.5.rel
AR4000S-Cloud		08/2024	AR-4000S-Cloud-5.5.4-0.5.iso
10GbE UTM Firewall		08/2024	ATVSTAPL-1.9.2.iso and vfw-x86_64-5.5.4-0.5.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	08/2024	AR4050S-5.5.4-0.5.rel AR3050S-5.5.4-0.5.rel
AR1050V	AR-series VPN routers	08/2024	AR1050V-5.5.4-0.5.rel
TQ6702 GEN2-R	Wireless AP Router	08/2024	TQ6702GEN2R-5.5.4-0.5.rel

Caution: Software version 5.5.4-0.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 5.5.4 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.4 license installed, that license also covers all later 5.5.4 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 45 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 47.

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

The 5.5.4-0.5 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.4-0.5:

ER-6288 *Available on: GS980M, x230/x230L, x220, and IE210 Series switches.*

This enhancement adds DoS protection support to a number of switch platforms.

Issues Resolved in Version 5.5.4-0.5

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

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82915	**Aggregation, LACP, Static, Private VLAN**	Previously, QoS (ACLs, Policy-maps), VLAN classifiers, VLAN translation, and UFO features and protocols, could sometimes have an incorrect interaction between particular trunk and port configurations. This issue has been resolved.	–	–	–	Y	Y	Y	–	–	–	Y	–	Y	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-83780	**AMF, API**	Previously, an administrative change in time-zone was not being registered by the AMF backup software. This issue has been resolved. The AMF backup API has also been changed to add the backup time in UTC as well as local time. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	Y	–	–	–
CR-77632	**ARP / Neighbor Discovery, EPSR, MAC Thrashing, VCStack**	Previously, it was possible for EPSR blocking to be defeated for ARP packets (request and reply) ingressing a port on a VCStack if the ingress port was on the backup member. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	–	–	–	–	Y	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-82861	**BFD**	Previously, a BFD session down event following a port link down was deleting the BFD session, which could result in incorrect OSPF/BGP neighbour states when the port linked up again. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-81850	**Bootup**	Previously, when a SBx8100C960 was starting up, some LIF cards might take a while to join, resulting in the CFC resetting the LIF cards. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-81744	**Cellular Modem**	Previously, on the AR4050s-5G, the AT$QCPDPP command did not support authentication, so if the 5G carrier required authentication, the router was unable to connect. This issue has been resolved, and the AT$QCPDPP command now supports authentication parameters.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–
CR-83259	**DHCP Relay**	Previously, DHCP relay could miss some VLAN interface up/down events, resulting in DHCP relay not operating on a VLAN. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y
CR-83420	**EPSR**	Previously, on a port under EPSR (Ethernet Protection Switching Ring) control, FDB entries were not removed when they should have been. This issue has been resolved.	Y	Y	Y	–	–	–	–	–	Y	–	Y	–	–	Y	–	–	Y	Y	–	Y	–	–	–	–	–	–
CR-81763	**HTTP**	This software update addresses the vulnerability specified in CVE-2023-38545 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-83116	**IDS/IPS**	Previously, Suricata operation could become unstable during scanning. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82127	**IPsec**	Previously, if both ends of an IPsec tunnel were set with '*oper-status-control ipsec'* and IKEv1 was used, the tunnel could be unstable and result in an increasing number of IPsec SAs. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y
CR-83417	**ISSU upgrade**	This maintenance release resolves an issue with ISSU compatibility. Previously, traffic failed to recover after ISSU upgrade from software version 5.5.4-0.2 to 5.5.4-0.3. As a result, traffic flow did not recover, including after rebooting the line-cards. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-83691	**OpenSSH**	This software update addresses an OpenSSH vulnerability issue listed in CVE-2024-6387.	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-83837	**OpenSSH**	This software update addresses a OpenSSH vulnerability issue listed in CVE-2024-6409.	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-83958	**OSPFv2**	Previously, during bootup, the software could reject the **`passive-interface tunnel`** command and fail to set a tunnel interface as an OSPF or OSPFv2 passive-interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-81827	**OSPFv2, Web API**	Previously, certain multicast reserve range packets were not correctly being trapped to the CPU. This issue has been resolved.	Y	Y	Y	–	–	–	–	–	Y	–	Y	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-82935	**PIM-SM**	Previously, multicast packets could be lost during multicast route updates. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	Y	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-83874	**PTP**	Previously, on switches supporting PTP, PTPv1, traffic could be dropped if it ingressed a port configured as a 'clock-port'. This issue has been resolved.	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	Y	Y	–	–	Y	–	–	–	–	–	–
CR-84018	**RIP, RIPng**	Previously, during bootup, the command parameter '*passive-interface*' was rejected, resulting in the corresponding tunnel interface failing to be configured as a RIP or RIPng passive-interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–
CR-83343	**SNMP**	Previously, SNMP walk on pluggable diagnostic tables did not show all pluggable interfaces. This issue has been resolved.	Y	–	–	Y	Y	–	–	–	–	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–	–
CR-83715	**System**	Previously, in rare situations, log messages generated by NSM might be incorrectly dropped by rate-limiting. 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	–	–	–
CR-83564	**System**	Previously, there was a small amount of memory leakage. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-83229	**UTM Offload**	Previously, when UTM offload was configured after URL filtering was enabled, the offload device could take a long time to startup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-83354	**VCStack**	Previously, some multicast streams could fail to recover after a stack master failover. This issue has been resolved.	–	Y	Y	–	–	–	–	–	Y	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-82678	**VRRP**	Previously, an overlap in the settings for trapping reserve multicast packets to the CPU, could result in short periods of packet loss during a rolling reboot, if the stack was the VRRP master. This issue has been resolved.	–	Y	Y	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82778	**VRRP, VCStack**	Previously, a prolonged traffic interruption could occur during rolling reboot when the stack was configured as a VRRP master. This issue has been resolved.	–	Y	Y	–	–	–	–	–	Y	–	–	–	–	Y	Y	Y	Y	–	Y	–	–	–	–	–	–	–

What's New in Version 5.5.4-0.3

Product families supported by this version:

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

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-0.3.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the Software Download area of the Allied Telesis website. 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 49.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 51. 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		07/2024	vaa-5.5.4-0.3.iso (VAA OS) vaa-5.5.4-0.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-0.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	07/2024	SBx81CFC960-5.5.4-0.3.rel
SBx908 GEN2	SBx908 GEN2	07/2024	SBx908NG-5.5.4-0.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	07/2024	x950-5.5.4-0.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	07/2024	x930-5.5.4-0.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2024	x550-5.5.4-0.3.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	07/2024	x530-5.5.4-0.3.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	07/2024	x330-5.5.4-0.3.rel
x320-10GH x320-11GPT	x320	07/2024	x320-5.5.4-0.3.rel
x240-10GTXm x240-10GHXm	x240	07/2024	x240-5.5.4-0.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2024	x230-5.5.4-0.3.rel
x220-28GS x220-52GT x220-52GP	x220	07/2024	x220-5.5.4-0.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	07/2024	IE340-5.5.4-0.3.rel
IE220-6GHX IE220-10GHX	IE220	07/2024	IE220-5.5.4-0.3.rel

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

Models	Family	Date	Software File
IE210L-10GP IE210L-18GP	IE210L	07/2024	IE210-5.5.4-0.3.rel
SE240-10GTXm SE240-10GHXm	SE240	07/2024	SE240-5.5.4-0.3.rel
XS916MXT XS916MXS	XS900MX	07/2024	XS900-5.5.4-0.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	07/2024	GS980MX-5.5.4-0.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	07/2024	GS980EM-5.5.4-0.3.rel
GS980M/52 GS980M/52PS	GS980M	07/2024	GS980M-5.5.4-0.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	07/2024	GS970EMX-5.5.4-0.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2024	GS970-5.5.4-0.3.rel
AR4000S-Cloud		07/2024	AR-4000S-Cloud-5.5.4-0.3.iso
10GbE UTM Firewall		07/2024	ATVSTAPL-1.9.2.iso and vfw-x86_64-5.5.4-0.3.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	07/2024	AR4050S-5.5.4-0.3.rel AR3050S-5.5.4-0.3.rel
AR1050V	AR-series VPN routers	07/2024	AR1050V-5.5.4-0.3.rel
TQ6702 GEN2-R	Wireless AP Router	07/2024	TQ6702GEN2R-5.5.4-0.3.rel

Caution: Software version 5.5.4-0.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 5.5.4 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.4 license installed, that license also covers all later 5.5.4 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 45 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 47.

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

The 5.5.4-0.3 software version is **not** ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.4-0.3:

ER-6110 *Available on: GS980MX, x220, x230/x230L, x240, x250, x530 / x530L Series switches.*

Previously, on some switches, a short delay (500ms) was implemented when a port linked up before traffic was forwarded. This was in order to guarantee that the link was stable before traffic was forwarded. This delay could result in a small number of dropped packets that arrived before forwarding was enabled.

A new command has been added to disable this delay. Note: This should only be configured in circumstances where the small number of lost packets are causing a network issue.

The new command is: (no) **linkflap enable-stable-time**

ER-6109 *Available on: GS980EM, GS980M, GS980MX, x220, x230/x230L, x320, x530L Series switches*

This enhancement enables the command **`platform port-tx-recovery`** by default, where previously it was disabled, unless explicitly configured.

This command prevents an issue where traffic passing over a port configured with a duplex-mismatch could result in traffic to the CPU failing and causing a VCStack failover.

This command can be manually disabled with the **`no platform port-tx-recovery`** command, however it is recommended that this command is left enabled.

ER-6093 *Available on: x230 Series switches*

Secure mode is now supported on the x230 Series switches.

ER-6021 *Available on: TQ6702 GEN2-R*

This enhancement adds support for edge security on the TQ6702GEN2-R. Edge security performs the following:

- Allows and denies specific clients to connect to the Wireless AP.
- Records all the clients which attempt to connect to the Wireless AP.

There are new commands available, configured in 'wireless-network' mode, as follows:

```
(no)unassociated-client-list acquire
(no)mac-auth radius send service-type
mac-auth radius dynamic-authorization-client <ip-address> key
<password> [encrypted]
no mac-auth radius dynamic-authorization-client
```

ER-5890 *Available on: GS970EMX, GS980MX, XS900MX, x330, x530 / x530L, x550, x930, x950 Series switches, and the SBx908Gen2 and SBx81CFC960*

This enhancement provides improvements to the rolling reboot. Namely, allowing the stack master to retain routes from dynamic routing protocols such as OSPF, BGP, and RIP throughout the reboot process. This helps minimize network disruption caused by the rolling reboot process.

ER-5997 *Available on: All AlliedWare Plus devices*

Previously, it was not possible to enforce max-fail account lockout to only remote logins. With this enhancement, this option is now supported on the following command:

```
(no)aaa local authentication attempts max-fail remote-login-
only
```

When the command is enabled, physical console logins are not subject to blocking from failed login attempts.

ER-5368 *Available on: AR4000S-Cloud, AR1050V, AR3050S, AR4050S, and TQ6702 GEN2-R*

This enhancement provides support for AES-GCM encryption/integrity for IPSec tunnels.

The AES-GCM option is added to the list of options for negotiating the IPSEC connection after the current SHA256/SHA512/AES options to maintain existing behavior but before the SHA1/3DES options as SHA1 and 3DES are less secure.

Issues Resolved in Version 5.5.4-0.3

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

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-80477	**AMF**	Previously, it was possible for a provisioned AMF node to include a copy of a UUID, if the **copy** or **clone** commands were used during the provisioning process. This could result in problems identifying the device after recovery when Vista Manager was in use. 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
CR-82753	**AMF**	Previously, when attempting to use an AMF backup command on a router that did not support backups, the error message provided suggested that the problem was incorrect configuration. The error message has been changed so that it is clear the hardware platform does not support AMF backup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	Y
CR-82730	**AMF**	Previously, the Vista Manager firmware distribution feature could fail to upload releases to the selected distribution point. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	Y	–	–	–
CR-82833	**AMF**	Previously, it was possible for an AMF network member to become unstable if the last virtual link on the device was destroyed and subsequently replaced with a non-virtual link. 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	–
CR-82454	**AMF, VCStack**	Previously, on rare occasions, it was possible for a system reboot to occur during a master failover while gathering counter information. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-81061	**API, AMF**	Previously, on AMF networks containing an AMF controller and one or more AMF masters, it was possible for Vista Manager to reach the devices HTTP server connection limit. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	Y	–	Y	–
CR-82856	**BFD**	Previously, **`echo mode`** configured on BFD peers did not work if VRF-lite was configured. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	–	–	–	–	–
CR-83227	**Cellular Modem**	For the AR4050S-5G, Product Bulletin 41114653 advises the EM9191 modem could suffer hardware damage when using n41 bandwidth firmware before 03.10.07.00. With this change, the n41 band is now blocked if EM9191 firmware is older than 03.10.07.00.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–
CR-82069	**CLI, VLAN**	Previously, running the **`show interface switchport vlan transport interface`** command on an interface with a default VLAN translation of outer-vlan, could incorrectly display the VLAN ID in middle field. This has been resolved, and the VLAN ID now correctly displays in the correct right hand column of the show output.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–
CR-82972	**DDNS, IPSec**	Previously, when an IPsec tunnel connected to a peer using a hostname instead of an IP address, there was a potential issue. If the remote peer's IP address changed, such as in a dynamic DNS (DDNS) scenario, the device might fail to update the new IP address. As a result, it would continue attempting to connect using the old IP address associated with the hostname. This issue has now been resolved. The device will now regularly resolve the hostname to an IP address to keep up with any address changes.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	Y

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82926	**Device GUI, PKI**	Previously, the PKI certificate generated by the device GUI did not contain the configured lifetime value. 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
CR-82498	**Device Security**	Previously, on platforms with **`crypto secure-mode`** enabled, on-demand algorithm self-tests may not have worked. This issue has been resolved.	–	–	Y	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-82014	**Device Security, HTTP service, Logging**	CBC and CCM based TLS ciphers have been removed, because they are now considered less secure and are not allowed by some security certifications. In addition, more TLS ciphers are also supported for TLSv1.2 and TLSv1.3 for web GUI HTTPS connections.	Y	Y	Y	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-82798	**DHCP Snooping**	Previously, the DHCP snooping module could restart when handling a bootp packet. 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
CR-82954	**DPI, NAT**	Previously, when NAT and DPI were used together, a conflict between two threads could cause the DPI module to lock up, resulting in no packets being processed or forwarded. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	Y
CR-81181	**EPSR, G.8032**	Previously, EPSR and G.8023 failover performance could be slower than expected in some circumstances. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-81196	**File System**	Previously, the **`show file`** command output could fail to display the first line of the selected file. This issue has been resolved.	–	Y	–	–	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-81787	**Firewall**	Previously, if a firewall rule was added to permit ICMP packets generated by the router (e.g., TTL exceeded) in response to received packets, the ICMP packet would not be sent even though the rule was correctly matched. This issue specifically occurred with user-defined applications where the protocol was specified as 'icmp'. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-82739	**Firewall**	Previously, with a large number of firewall rules the command **`show firewall rules`** could take a very long time to complete. This resulted in a health-check failure and system reboot of the router. This issue has been resolved by improving the way the firewall rule hit-counts are retrieved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	Y
CR-82514	**IGMP**	Previously, if a dynamically learned IGMP group record changed to a static group record, multicast traffic for that group might not be forwarded correctly. 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
CR-81093	**IPSec**	Previously, IPSec tunnels were not being established when using the AES-GCM IPSec profile on AR Routers. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–
CR-82787	**IPv6, VRRP**	Previously, the device could undergo a system reboot if the **`vrrp ipv6`** configuration was entered. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–	–
CR-82788	**IPv6, VRRP**	Previously, an internal process called ‘alfred’ could cause a system reboot during configuration. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-81618	**MAP-E**	Previously, under certain conditions, traffic being transmitted in a softwire tunnel would not be masqueraded correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	–
CR-82740	**MAP-E**	Previously, in certain circumstances, executing the **show `softwire-config`** command could result in a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	Y
CR-77098	**Multicast**	Previously, a memory leak could occur if a switch received packet fragments from unregistered multicast streams and was configured with the command: **`ip multicast allow-register-fragments`**. 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	–	–	–	–	–	–
CR-81015	**NAT**	Previously, if a NAT port forwarding rule for FTP including a port translation was configured, the first connection to the FTP server from a client would work but subsequent connections could fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	–
CR-81827	**OSPFv2, Web API**	Previously, certain multicast reserve range packets were not correctly being trapped to the CPU. This issue has been resolved.	Y	Y	Y	–	–	–	–	–	Y	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-82993	**PIM-DM**	Previously, when using PIM dense mode, some memory was not being freed when multicast groups joined and left. Over time, this resulted in free memory depletion. This issue has been resolved.	–	Y	Y	–	Y	Y	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–
CR-82679	**Pluggable Transceivers**	Previously, 1G SFPs (e.g. AT-SPSX) installed in the x530-28GSX could fail to link up when configured for 100M-BASE-FX mode. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-77391	**PoE**	Previously, in rare circumstances, it was possible for an x930-28GPX and x930-52GPX to fail to detect that a PoE device had been connected. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-81749	**PoE**	Previously, ports on the x230-28GP could temporarily stop providing power. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-82259	**QoS**	Previously, it was possible for the software to attempt to execute a QSP (QoS Storm Protection) action on a port that was link down, resulting in an error log. 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	–	–	–	–	–	–
CR-82980	**QoS**	Previously, when an ACL was configured as a match in a class-map, the ACL name could be truncated in the class-map's running configuration. 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	–	–	–	–	–	–
CR-82821	**Security, User Management**	Previously, there was an issue with the command **`show hash bootrom`**. This issue has been resolved.	–	–	Y	–	–	–	Y	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-82780	**SSH**	Previously, SSH known hosts which used non-standard port numbers could fail to be removed. 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
CR-82030	**Switching**	Previously, switch ports on XLEM/XT4 extension modules might not link up following a reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-82166	**VCStack**	Previously, when removing a stack link and connecting it to a different new stack member, the new stack member might not have joined the stack. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82920	**VCStack, ARP, Neighbor Discovery**	Previously, if a VCStack member was restarted in a network containing Windows NLB Servers, it was sometimes possible for a stack member to restart while it was configuring. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-82163	**VCStack, Loop Protection**	Previously, if Loop Detection Frame (LDF) packets from a neighbor device caused a storm, it could cause a stack separation on the x330 platform. This issue has been resolved by setting the storm control level of LDF broadcast to 50% of port speed by default.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-83115	**VLAN Stacking (Q-in-Q)**	Previously, on the x330-52GTX and GS970EMX-52, VLAN stacking (Q-in-Q) configuration would fail to be applied to ports connected to the second switch chip. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-82678	**VRRP**	Previously, an overlap in the settings for trapping reserve multicast packets to the CPU, could result in short periods of packet loss during a rolling reboot, if the stack was the VRRP master. This issue has been resolved.	–	Y	Y	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–

What's New in Version 5.5.4-0.1

Product families supported by this version:

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

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-0.1.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the Software Download area of the Allied Telesis website. 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 49.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 51. 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		03/2024	vaa-5.5.4-0.1.iso (VAA OS) vaa-5.5.4-0.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-0.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2024	SBx81CFC960-5.5.4-0.1.rel
SBx908 GEN2	SBx908 GEN2	03/2024	SBx908NG-5.5.4-0.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	03/2024	x950-5.5.4-0.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	03/2024	x930-5.5.4-0.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2024	x550-5.5.4-0.1.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2024	x530-5.5.4-0.1.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	03/2024	x330-5.5.4-0.1.rel
x320-10GH x320-11GPT	x320	03/2024	x320-5.5.4-0.1.rel
x240-10GTXm x240-10GHXm	x240	03/2024	x240-5.5.4-0.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2024	x230-5.5.4-0.1.rel
x220-28GS x220-52GT x220-52GP	x220	03/2024	x220-5.5.4-0.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2024	IE340-5.5.4-0.1.rel
IE220-6GHX IE220-10GHX	IE220	03/2024	IE220-5.5.4-0.1.rel

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

Models	Family	Date	Software File
IE210L-10GP IE210L-18GP	IE210L	03/2024	IE210-5.5.4-0.1.rel
SE240-10GTXm SE240-10GHXm	SE240	03/2024	SE240-5.5.4-0.1.rel
XS916MXT XS916MXS	XS900MX	03/2024	XS900-5.5.4-0.1.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	03/2024	GS980MX-5.5.4-0.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2024	GS980EM-5.5.4-0.1.rel
GS980M/52 GS980M/52PS	GS980M	03/2024	GS980M-5.5.4-0.1.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	03/2024	GS970EMX-5.5.4-0.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2024	GS970-5.5.4-0.1.rel
AR4000S-Cloud		03/2024	AR-4000S-Cloud-5.5.4-0.1.iso
10GbE UTM Firewall		03/2024	ATVSTAPL-1.9.2.iso and vfw-x86_64-5.5.4-0.1.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	03/2024	AR4050S-5.5.4-0.1.rel AR3050S-5.5.4-0.1.rel
AR1050V	AR-series VPN routers	03/2024	AR1050V-5.5.4-0.1.rel
TQ6702 GEN2-R	Wireless AP Router	03/2024	TQ6702GEN2R-5.5.4-0.1.rel

Caution:

Software version 5.5.4-0.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 5.5.4 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.4 license installed, that license also covers all later 5.5.4 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 45 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 47.

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

The 5.5.4-0.1 software version is **not** ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.4-0.1:

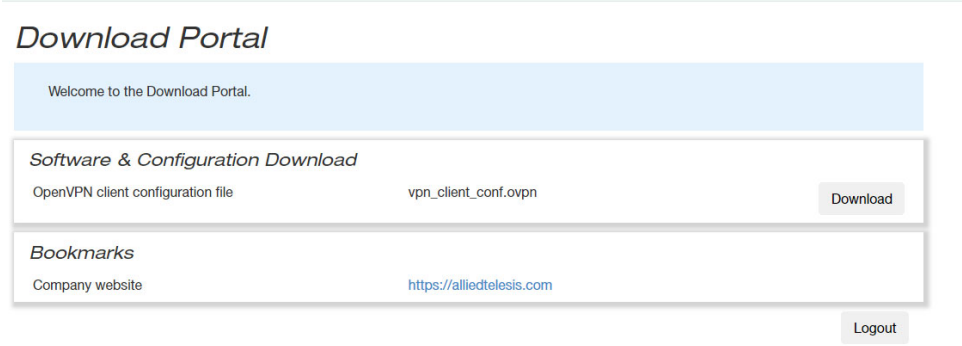
To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 44.

Support for Download Portal

Applies to AR-Series UTM firewalls and VPN routers, AR4000-Cloud, the 10GbE UTM firewall, and TQ6702 GEN2-R

From AlliedWare Plus version 5.5.4-0.1 and Device GUI version 2.17.0 onwards, there is a new feature called **Download Portal**.

The Download Portal lets administrators offer resources to network users, protected by authentication. The resources could include software installers and setup guidelines, for example a remote access client along with setup instructions, like this:



The Download Portal has two user types, administrators and users.

Administrators:

- define the files and links they wish to display on the Download Portal page.
- set up an authentication mechanism that controls access to the Download Portal through usernames and passwords.
- provide users with a URL to subsequently navigate to the Download Portal and retrieve the necessary files and links that they need.

Users:

- navigate to the Download Portal (using a link provided by Admin)
- login to the Download Portal page
- download resources from the Download Portal page

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

Push entity routes to OpenVPN clients

Applies to AR-Series UTM firewalls and VPN routers, AR4000-Cloud, the 10GbE UTM firewall, and TQ6702 GEN2-R

From AlliedWare Plus version 5.5.4-0.1 onwards, a device configured as an OpenVPN server can push route information based on specific entities. When an OpenVPN client establishes a connection, the IPv4 and IPv6 host addresses along with network subnets for that entity are pushed to the client. The client then routes matching traffic through the OpenVPN tunnel to the AlliedWare Plus device, using a configured IP as the gateway. Host addresses are sent as either a /32 IPv4 route or a /128 IPv6 route.

Note that if there are changes in the network subnets or host IPs on the entity, the client connections will not be automatically updated. In such cases, clients will need to reconnect to obtain any new routes.

New command `tunnel openvpn route <entity-name>`

To configure an entity with subnets and addresses that will be pushed to the OpenVPN client that will be routed to the device, use the following commands:

```
awplus# configure terminal
awplus(config)# zone openvpn_routes
awplus(config-zone)# network internet
awplus(config-network)# host example
awplus(config-host)# ip address dynamic fqdn example.com
awplus(config-host)# exit
awplus(config-network)# exit
awplus(config-zone)# network local
awplus(config-network)# ip subnet 172.16.0.0/16
awplus(config-network)# host example
awplus(config-host)# ip address 10.255.0.1
awplus(config-host)# exit
awplus(config-network)# exit
awplus(config-zone)# exit
awplus(config)# interface tunnel1
awplus(config-if)#tunnel openvpn route openvpn_routes
```

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

Improved formatting of new OpenText categories

Available on AR-Series UTM firewalls and VPN routers, AR4000-Cloud, and the 10GbE UTM firewall

OpenText is one of the providers that AlliedWare Plus can use to categorize websites and applications for deep packet inspection (DPI) and web control. OpenText has recently released four new categories, which are already visible in DPI and web categorization. From 5.5.4-0.1 onwards, AlliedWare Plus formats and displays these new categories in the same way as OpenText's already-existing categories. The new categories are:

- Self Harm
- DNS Over HTTPS
- Low-THC Cannabis Products
- Generative AI

For more information about using web categorization for DPI, see the Application Awareness Feature Overview and Configuration Guide.

For more information about web control, see the Web Control section of the Advanced Network Protection Feature Overview and Configuration Guide.

TQ6702 GEN2-R enhancements

From version 5.5.4-0.1 onwards, the following features have been added to the TQ6702 GEN2-R wireless router.

AMF Plus links over Ethernet ports

From version 5.5.4-0.1 onwards, it is possible to create AMF Plus links over Ethernet ports on TQ6702 GEN2-R wireless routers. This means you can provision, back up, and recover nodes connected to the wireless router's Ethernet ports.

Only up/down links are supported.

For example, use the following commands to configure an up/down link over the eth1 interface:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# atmf-link
```

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

Device Discovery of wireless clients

From version 5.5.4-0.1 and Vista Manager 3.12.0 onwards, Vista Manager EX's Device Discovery can discover wireless clients that are attached to TQ6702 GEN2-R wireless routers. This means that these clients will display on the network map in Vista Manager EX.

To enable this, use the following command on the wireless router when setting up Device Discovery using STOAT:

```
awplus(config)# stoat discovery wireless
```

For more information about Device Discovery, see the Device Discovery using STOAT Feature Overview and Configuration Guide.

Enhancements to wireless authentication features

From version 5.5.4-0.1 and device GUI 2.17.0 onwards, wireless authentication on TQ6702 GEN-2 wireless routers allows you to use:

- a wildcard when you specify the IP address, network, or domain name of a walled garden in Captive Portal. A walled garden allows users to access certain web pages without first needing to authenticate with captive portal.
- a MAC address list at the same time as an external RADIUS server for MAC authentication
- AMF application proxy for MAC authentication.

We recommend you use the Device GUI to configure these new features. You can find these new features in the Device GUI by selecting **Wireless** in the left hand menu, then selecting the tab for Radio1 or Radio2, then the **Edit** button for the desired VAP, then the **Advanced Settings** button, then the **Security** tab.

Standardization of maximum bridge ID

Applies to AR-Series UTM firewalls and VPN routers, AR4000-Cloud, the 10GbE UTM firewall, and TQ6702 GEN2-R

From version 5.5.4-0.1 and Device GUI 2.17.0 onwards, the maximum ID number you can give a bridge entity is 300 on all devices that support bridging. This means that when you create a bridge entity using the commands:

```
awplus# configure terminal
awplus(config)# bridge <bridge-id>
```

then <bridge-id> can be any number from 1 to 300.

Note that the number of supported bridge entities for each firewall or router model has not changed.

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

Support for more NETCONF and RESTCONF data models

Applies to All AlliedWare Plus devices

From AlliedWare Plus version 5.5.4-0.1 onwards, NETCONF and RESTCONF protocols have ***xpath*** capability and support the ***openconfig-interfaces*** and ***ietf-interfaces*** data models.

Note that an xpath query may have a greater impact on performance than a subtree filter. This is for two reasons:

- having to retrieve more data than is strictly needed
- the extra processing required to apply the query to that data.

We recommend you use subtree filters with NETCONF.

Data models are the foundation for both NETCONF and RESTCONF, as they define the structure and semantics of the data exchanged between network management systems and network devices. These models make it possible to manage network configurations and gather operational data in a consistent, standardized, and vendor-agnostic way, facilitating efficient network management and automation.

For more information about NETCONF and RESTCONF on AlliedWare Plus devices, see the NETCONF and RESTCONF Feature Overview and Configuration Guide.

Fast failover for Free Range Routing Bidirectional Forwarding Detection (FRR BFD) in VCStacks

Applies to SBx8100, SBx908 GEN2, x950, x930, and x530 series switches

BFD is a network protocol that provides low-overhead, short-duration detection of failures in the path between two endpoints. Routing protocols such as BGP can use BFD to receive faster notification of failing links than would be possible using the protocol's own keepalive mechanism.

From version 5.5.4-0.1 onwards, FRR BFD restores routing more quickly when a stack failover occurs in a VCStack. When BFD sessions are created via routing protocols such as BGP, they are now synced across the stack. During a stack failover the new VCStack master device continues using the same session, so it can recover routing quickly.

For this fast failover to work, you need to create a BFD profile on the stack and make **detect-multiplier** x **transmit-interval** be at least 6 seconds. One possible configuration is:

detect-multiplier = 20
transmit-interval = 300 milliseconds (the default)
detect-multiplier x **transmit-interval** = 6000 milliseconds = 6 seconds

An example of this configuration is:

```
bfd profile BGP_EXAMPLE
 detect-multiplier 20
!
router bgp 2
 neighbor 10.10.10.1 remote-as 1
 neighbor 10.10.10.1 fall-over bfd profile BGP_EXAMPLE
```

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

Features that no longer require a license on IE220 and IE340 Series devices

From version 5.5.4-0.1 onwards, the following features no longer require a feature license on IE220 or IE340 Series devices[1].

On IE220 Series switches

- VLAN double tagging (also called nested VLANs or Q-in-Q)
- EPSR master functionality
- VLAN translation (full functionality)
- G.8032 (Ethernet ring protection switching)
- Connectivity Fault Management (CFM)
- OpenFlow

On IE340 Series switches

- Virtual Router Redundancy Protocol (VRRP)
- VLAN double tagging (also called nested VLANs or Q-in-Q)
- EPSR master functionality
- VLAN translation (full functionality)
- G.8032 (Ethernet ring protection switching)
- Connectivity Fault Management (CFM)
- OpenFlow
- MODBUS
- Media Redundancy Protocol (MRP)
- PROFINET
- Continuous PoE

1. These features still require a license in Japan.

Support for Precision Time Protocol (PTP) on stacked x930 Series switches

From version 5.5.4-0.1 onwards, AlliedWare Plus supports PTP Transparent Clock on x930 Series switches in a VCStack (except when stacking over the 1G ports).

PTP is used for applications that require very high precision timing - at the nanosecond level - using Ethernet or Ethernet/IP. This includes, for example, Telco applications such as cellular, where not only frequency, but also phase precision, is needed in order to control hand-off of mobile phones from one cell tower to the next.

The Transparent Clock feature is used by bridges or routers to assist clocks in measuring and adjusting for packet delay. The transparent clock computes the variable delay as the PTP packets pass through the switch.

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

Increasing the maximum lifetime of X.509 certificates

Applies to all AlliedWare Plus devices

From version 5.5.4-0 onwards, the maximum lifetime of self-signed X.509 certificates has increased to 10 years. The certificate lifetime is an optional setting when creating a trustpoint, with a default of 5 years. You can specify a non-default lifetime in days (1-3650), months (1-120) or years (1-10).

To do this, use the following command in Trustpoint Configuration mode for a trustpoint:

```
awplus(ca-trustpoint)# lifetime {days <1-3650>|months <1-120>|
years <1-10>}
```

For more information about trustpoints, see the PKI Feature Overview and Configuration Guide.

Support for sFlow on x240 Series switches

From version 5.5.4-0.1 onwards, sFlow is supported on x240 Series switches. For details about sFlow, see the sFlow Feature Overview and Configuration Guide.

Note that while sFlow sampling can be enabled on all ports, you can only configure 7 different sample rates. If you attempt to add an 8th sample rate, the following error message appears:

"Unable to set sample rate <rate> on interface <interface> because HW resource is exhausted"

Support for OpenFlow™ protocol on x240 Series

From version 5.5.4-0.1 onwards, the OpenFlow protocol is supported on x240 Series switches.

x240 Series switches have:

- maximum number of flow table entries: 2560
- maximum number of end-user devices: 1280.

For details about the OpenFlow protocol, see the OpenFlow Feature Overview and Configuration Guide.

Passwords are now displayed in encrypted form in running configuration

Applies to all AlliedWare Plus devices

From version 5.5.4-0.1 onwards, a number of features will now have their passwords displayed in running configuration in encrypted form, instead of in plain text.

This change was made for a number of features in 5.5.3-2.1. In 5.5.4-0.1 onwards, it has been made to the remaining features that displayed passwords in plain text.

For example, if you enter the following CLI command:

```
ppp password <cleartext>
```

It will be displayed in running configuration as:

```
ppp password <ciphertext> encrypted
```

The **encrypted** parameter shows that the password is encrypted. Do not use this parameter when you enter a password in the CLI.

If you need to display the passwords in unencrypted form, use the new command:

```
awplus# show running-config unencrypted
```

This command can only be entered by users with privilege level 15.

VLAN translation enhancement

Applies to SBx908 GEN2 and x950 series switches

From 5.5.4-0.1 onwards, you can apply a new action to packets that do not match one of your explicit VLAN translation rules. Previously, you could choose whether the switch would drop such packets or pass them through without any translation. Now the switch can add a default outer VLAN tag to these packets instead.

This enhancement is helpful if you need to apply the same outer VLAN tag to incoming packets that have many different VLAN tags, or if you do not know the tags of the incoming packets. For example, if you need to add an outer tag of VLAN3 to incoming packets, no matter what VLAN tag they have, you can use this feature to do that.

To get the switch to add an outer tag to such packets, specify the desired outer VLAN ID for the appropriate switch ports (on port1.0.1 in this example):

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport vlan translation default
outer-vlan <vlan-id>
```

For details about VLAN translation, see the VLANs Feature Overview and Configuration Guide.

Display transceiver power values in dBm

Applies to all devices that support transceivers (also named pluggables)

From 5.5.4-0 onwards, a new **show** command option lets you display power values for transceivers in dBm (decibel-milliwatts) instead of mW (milliwatts). To do this, use the command:

```
awplus# show system pluggable [<port-list>] diagnostics dbm
```

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

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

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

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

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

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

- 5.5.3-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 38 and "Details for x930 Series" on page 39 for details.

Affected Products

The following models could be affected:

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

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

Recovering from upgrading from an incompatible version

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

Details for SBx908 GEN2 and x950 Series

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

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

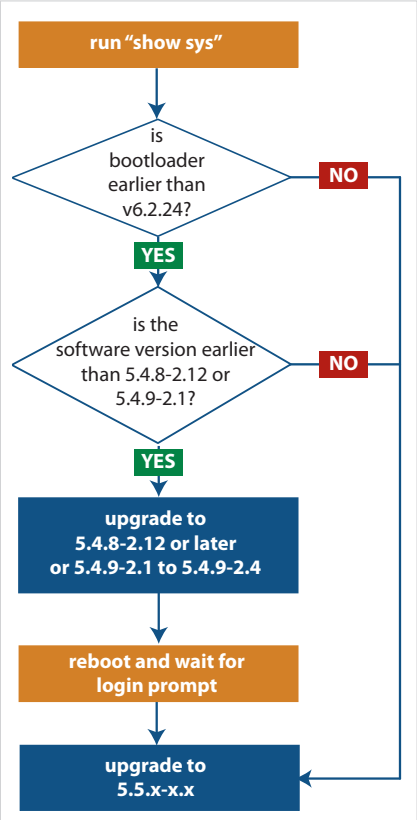
Instead, before upgrading from one of those versions to the current version, make sure your switch is running one of these specified versions:

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

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

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

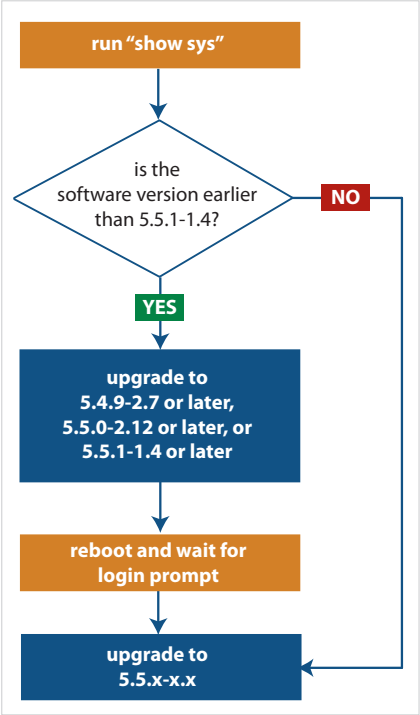
```
awplus# show system
```



Details for x930 Series

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

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



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

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

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

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

```
awplus# show system
```

Changes that may affect device or network configuration

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

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

Summary	Affected devices	Detail

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

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 45 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 47.

Upgrading a VCStack with rolling reboot

Applies to all stackable AlliedWare Plus switches, except SBx8100

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

For SBx908 GEN2, x950 and x550 Series switches

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

- All versions from 5.5.0-x.x onwards

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

For x530 Series switches using DAC to stack

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

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

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

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

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

To use rolling reboot

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

Forming or extending a VCStack with auto-synchronization

Applies to all stackable AlliedWare Plus switches

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

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

For SBx908 GEN2, x950 and x550 Series switches

Auto-synchronization is supported between this version and:

- All versions from 5.5.0-x.x onwards

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

For CFC960 cards in an SBx8100 system

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

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

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

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

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

For x530 Series switches using DAC to stack

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

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

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

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

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

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

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

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

Upgrading all devices in an AMF network

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).

2. Decide which AMF upgrade method is most suitable.

3. Initiate the AMF network upgrade using the selected method. To do this:
   a. create a working-set of the nodes you want to upgrade
   b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
   c. Check the console messages to make sure that all nodes are “release ready”. If they are, follow the prompts to perform the upgrade.

Obtaining User Documentation

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

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

Verifying the Release File

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

```
awplus(config)# crypto verify <filename> <hash-value>
```

where <*hash-value*> is the known correct hash of the file.

This command compares the SHA256 hash of the release file with the correct hash for the file. The correct hash is listed in the table of Hash values for 5.5.4-0.5 below or in the release's sha256sum file, which is available from the Allied Telesis Download Center.

Caution

If the verification fails, the following error message will be generated:
"% Verification Failed"
In the case of verification failure, please delete the release file and contact Allied Telesis support.

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

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

Table: Hash values for 5.5.4-0.5

Product family	Software File	Hash
AMF Cloud	vaa-5.5.4-0.5.rel	f0e2612d6fbede4fedcf3a3e6d26da8a1fe2ececb1b12b7b4df2c82d42bf79fa
SBx8100	SBx81CFC960-5.5.4-0.5.rel	265512d51004ca1e7604f997d2c69b1c54c0732c4cc5e94ded3cfea39657fd10
SBx908 GEN2	SBx908NG-5.5.4-0.5.rel	f0420b35343731c1afeda1847fc1f5bbb0d44ef38d55f147f838224494b8843c
x950	x950-5.5.4-0.5.rel	f0420b35343731c1afeda1847fc1f5bbb0d44ef38d55f147f838224494b8843c
x930	x930-5.5.4-0.5.rel	7b44e0cf4f646d8f7874aa504abb5e1a06529b49dc4a385d7490b0e0d78b2c67
x550	x550-5.5.4-0.5.rel	b2cea1566b619737138d740fe828cb22f3f7d770ec1c36e9b90dcc48d884a842
x530 & x530L	x530-5.5.4-0.5.rel	927a502152b25102860b49941c6874b72b0c7cc2fea6f9f920ab4e62972f15a9
x330	x330-5.5.4-0.5.rel	09bf22b073e7129253f83f5364ab99b53692258b1db7dc9168de08caaf651881

Table: Hash values for 5.5.4-0.5

Product family	Software File	Hash
x320	x320-5.5.4-0.5.rel	927a502152b25102860b49941c6874b72b0c7cc2fea6f9f920ab4e62972f15a9
x230 & x230L	x230-5.5.4-0.5.rel	2204a0351adf59d1e22cb0e163750206ca432deec60260af8899de69479fd31c
x220	x220-5.5.4-0.5.rel	ce04aa6bb2e685312a916f7d223b1b93fd3a2c05bb6d0f791f374f1703d73d19
IE340 & IE340L	IE340-5.5.4-0.5.rel	777696a6800e228ccf1ff53569f0684db1c3d89817f52167e92c7300fe8e13e4
IE220	IE220-5.5.4-0.5.rel	0ec46542ca51315f7b55b2644fe92c3b936bda5f24add4f5e76a7e31a34cfa94
IE210L	IE210-5.5.4-0.5.rel	2204a0351adf59d1e22cb0e163750206ca432deec60260af8899de69479fd31c
XS900MX	XS900-5.5.4-0.5.rel	6ced3a1c8b75bb20d342bca260f33bd8dc816cc46fa43210980cea208de3ef01
GS980MX	GS980MX-5.5.4-0.5.rel	927a502152b25102860b49941c6874b72b0c7cc2fea6f9f920ab4e62972f15a9
GS980EM	GS980EM-5.5.4-0.5.rel	08fad4ca8e8fa4d878328a8cc377f5e732693874c2938e5fb4bb437a87f5a36a
GS980M	GS980M-5.5.4-0.5.rel	ce04aa6bb2e685312a916f7d223b1b93fd3a2c05bb6d0f791f374f1703d73d19
GS970EMX	GS970EMX-5.5.4-0.5.rel	09bf22b073e7129253f83f5364ab99b53692258b1db7dc9168de08caaf651881
GS970M	GS970-5.5.4-0.5.rel	2204a0351adf59d1e22cb0e163750206ca432deec60260af8899de69479fd31c
AR4050S-5G	AR4050S-5.5.4-0.5.rel	1f309d9b44629fad453b12720a218f37c7021d5003a5c0558934171f170329bd
AR4050S	AR4050S-5.5.4-0.5.rel	1f309d9b44629fad453b12720a218f37c7021d5003a5c0558934171f170329bd
AR3050S	AR3050S-5.5.4-0.5.rel	1f309d9b44629fad453b12720a218f37c7021d5003a5c0558934171f170329bd
AR1050V	AR1050V-5.5.4-0.5.rel	c2f25f035ebe544eeaed2524d00bf3127153b5a0f2ddb7db675687bf577d4f9c
TQ6702 GEN2-R	TQ6702GEN2R-5.5.4-0.5.rel	cb891728959a5d623f7e2024d69d6f73b59cc3edc473d23d91faacb53f0eea46

Licensing this Version on an SBx908 GEN2 Switch

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

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

1. Obtain the MAC address for a switch

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

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

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

2. Obtain a release license for a switch

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

3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

```
awplus#show license

Board region: Global

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

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

Licensing this Version on an SBx8100 Series CFC960 Control Card

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

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

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

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

1. Obtain the MAC address for a control card

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

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

```
awplus#show system mac license

MAC address for licensing:


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

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

2. Obtain a release license for a control card

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

3. Apply a release license on a control card

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

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

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

Installing this Software Version

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 45 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 47.

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

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

2. If necessary, delete or move files to create space in the switch's Flash memory for the new file. To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

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

Product	Command
SBx8100 with CFC960	`awplus(config)# boot system SBx8100-5.5.4-0.5.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.4-0.5.rel`
x950 series	`awplus(config)# boot system x950-5.5.4-0.5.rel`
x930 series	`awplus(config)# boot system x930-5.5.4-0.5.rel`
x550 series	`awplus(config)# boot system x550-5.5.4-0.5.rel`
x530 series	`awplus(config)# boot system x530-5.5.4-0.5.rel`
x330 series	`awplus(config)# boot system x330-5.5.4-0.5.rel`
x320 series	`awplus(config)# boot system x320-5.5.4-0.5.rel`
x240 series	`awplus(config)# boot system x240-5.5.4-0.5.rel`
x230 series	`awplus(config)# boot system x230-5.5.4-0.5.rel`
x220 series	`awplus(config)# boot system x220-5.5.4-0.5.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.4-0.5.rel`
IE220 series	`awplus(config)# boot system IE220-5.5.4-0.5.rel`

Product	Command
IE210L series	`awplus(config)# boot system IE210-5.5.4-0.5.rel`
SE240 series	`awplus(config)# boot system SE240-5.5.4-0.5.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.4-0.5.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.4-0.5.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.4-0.5.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.4-0.5.rel`
GS970EMX series	`awplus(config)# boot system GS970EMX-5.5.4-0.5.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.4-0.5.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.4-0.5.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.4-0.5.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.4-0.5.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.4-0.5.rel`
TQ6702 GEN2-R	`awplus(config)# boot system TQ6702GEN2R-5.5.4-0.5.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 AR4050S and AR3050S firewalls, you can use the GUI to create an advanced application-aware firewall with features such as Application control and Web control. Alternatively, you can configure real-time threat protection with URL filtering, Intrusion Prevention and Malware protection.

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

Browse to the GUI

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

Perform the following steps to browse to the GUI.

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

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

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

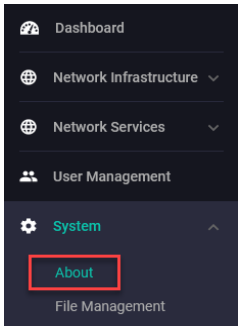
   - on switches: 169.254.42.42
   - on AR-Series: 192.168.1.1

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

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

Check the GUI version

To see which version you have, open the **System** > **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.4-0.x is 2.17.0.



If you have an earlier version, update it as described in "Update the GUI on switches" on page 52 or "Update the GUI on AR-Series devices" on page 53.

Update the GUI on switches

Perform the following steps through the Device GUI and command-line interface if you have been running an earlier version of the GUI and need to update it.

1. Obtain the GUI file from our Software Download center. The GUI filename to use with AlliedWare Plus v5.5.4-0.x is awplus-gui_554_32.gui.

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

2. Log into the GUI:

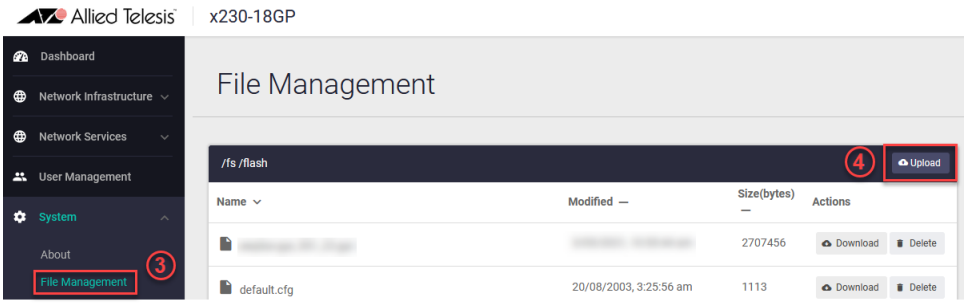
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   The GUI starts up and displays a login screen. Log in with your username and password.

   The default username is *manager* and the default password is *friend*.

3. Go to **System** > **File Management**

4. Click **Upload**.



5. Locate and select the GUI file you downloaded from our Software Download center. The new GUI file is added to the **File Management** window.

   You can delete older GUI files, but you do not have to.

6. Reboot the switch. Or alternatively, use **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 v2.17.0 or later.