Allied Telesis™

Release Note for AlliedWare Plus Software Version 5.5.2-2.x

AlliedWare Plus
OPERATING SYSTEM

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

x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series

XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series

AR4000S-Cloud
10GbE UTM Firewall
AR4050S-5G
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

» 5.5.2-2.1 » 5.5.2-2.2 » 5.5.2-2.3 » 5.5.2-2.4 » 5.5.2-2.5 » 5.5.2-2.6 » 5.5.2-2.7

Acknowledgments

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

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

All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see **www.openssl.org/**
Copyright (c) 1998-2019 The OpenSSL Project
Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson
All rights reserved.

This product includes software licensed under the GNU General Public License available from: **www.gnu.org/licenses/gpl2.html**

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

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

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

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

Getting the most from this Release Note

To get the best from this release note, we recommend using Adobe Acrobat Reader version 8 or later. You can download Acrobat free from **www.adobe.com/**

Contents

What's New in Version 5.5.2-2.7 1

Introduction 1

Issues Resolved in Version 5.5.2-2.7 5

What's New in Version 5.5.2-2.6 9

Introduction 9

New Features and Enhancements 13

Issues Resolved in Version 5.5.2-2.6 14

What's New in Version 5.5.2-2.5 21

Introduction 21

Issues Resolved in Version 5.5.2-2.5 25

What's New in Version 5.5.2-2.4 33

Introduction 33

Issues Resolved in Version 5.5.2-2.4 37

What's New in Version 5.5.2-2.3 38

Introduction 38

New Features and Enhancements 41

What's New in Version 5.5.2-2.2 42

Introduction 42

New Features and Enhancements 45

Issues Resolved in Version 5.5.2-2.2 46

What's New in Version 5.5.2-2.1 49

Introduction 49

New Features and Enhancements 53

Important Considerations Before Upgrading 62

Obtaining User Documentation 69

Verifying the Release File 69

Licensing this Version on an SBx908 GEN2 Switch 70

Licensing this Version on an SBx8100 Series CFC960 Control Card 72

Installing this Software Version 74

Accessing and Updating the Web-based GUI 76

What’s New in Version 5.5.2-2.7

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
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-2.7.

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 74.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 76. 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 Cloud		08/2023	vaa-5.5.2-2.7.iso (VAA OS) vaa-5.5.2-2.7.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-2.7.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2023	SBx81CFC960-5.5.2-2.7.rel
SBx908 GEN2	SBx908 GEN2	08/2023	SBx908NG-5.5.2-2.7.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	08/2023	x950-5.5.2-2.7.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	08/2023	x930-5.5.2-2.7.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2023	x550-5.5.2-2.7.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	08/2023	x530-5.5.2-2.7.rel
x330-10GTX x330-20GTX x330-28GTX	x330	08/2023	x330-5.5.2-2.7.rel
x320-10GH x320-11GPT	x320	08/2023	x320-5.5.2-2.7.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2023	x230-5.5.2-2.7.rel
x220-28GS x220-52GT x220-52GP	x220	08/2023	x220-5.5.2-2.7.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	08/2023	IE340-5.5.2-2.7.rel
IE210L-10GP IE210L-18GP	IE210L	08/2023	IE210-5.5.2-2.7.rel
XS916MXT XS916MXS	XS900MX	08/2023	XS900-5.5.2-2.7.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	08/2023	GS980MX-5.5.2-2.7.rel
GS980EM/10H GS980EM/11PT	GS980EM	08/2023	GS980EM-5.5.2-2.7.rel
GS980M/52 GS980M/52PS	GS980M	08/2023	GS980M-5.5.2-2.7.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	08/2023	GS970EMX-5.5.2-2.7.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2023	GS970-5.5.2-2.7.rel
AR4000S-Cloud		08/2023	AR4000S-Cloud-5.5.2-2.7.iso AR4000S-Cloud-5.5.2-2.7.vhd and upload_vhd.py (for AWS)
10GbE UTM Firewall		08/2023	ATVSTAPL-1.7.2.iso and vfw-x86_64-5.5.2-2.7.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	08/2023	AR4050S-5.5.2-2.7.rel AR3050S-5.5.2-2.7.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	08/2023	AR2050V-5.5.2-2.7.rel AR2010V-5.5.2-2.7.rel AR1050V-5.5.2-2.7.rel

⚠ **Caution:** Software version 5.5.2-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-2.x. Such switches do 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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

Unsupported devices

Version 5.5.2-2.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-2.7 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.2-2.7

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

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79709	**AMF**	Previously, it was possible for an AMF network to become unstable due to too many entries in the AMF database. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	–	–	–	Y	–	–
CR-79525	**ARP** **Neighbor Discovery**	Previously, ARP learning was causing memory exhaustion. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-79624	**Configuration Replay, Loop Protection**	Previously, when some VLANs were configured with names, creating an MST instance with one or more VLANs could fail. 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	–
CR-79447	**Device Security, File System, AMF**	Previously, when the command **`strict-user-process-control`** was executed on a working-set, it was only successfully executed on the local node. This issue has been resolved. With this software update, the command **`strict-user-process-control`** can only be executed on local nodes. To make the behaviour more apparent to users, now the command can only be executed either on a console of a node, or a working-set containing only the local node. 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	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79420	**DNS**	This software update addresses a DNS vulnerability issue as specified in CVE-2022-4904 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	–
CR-79421	**DNS**	This software update addresses a DNS vulnerability issue as specified in CVE-2023-28450. 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	–
CR-79935	**DPI, Web Control**	Previously, when Digital Arts Web Categorization for either Web Control or DPI was enabled, it could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–
CR-79763	**Firewall**	Previously, a firewall rule was still getting hit even after removing zone/subnet/host from the rule. Configuration changes would only take effect after a device restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–
CR-79948	**Firewall**	Previously, when entities had hosts or networks removed, the firewall rules that used these entities would continue to act on the removed entities. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–
CR-79415	**HTTP Service**	This software update addresses a HTTP Service vulnerability as specified in CVE-2023-25725 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	–
CR-79665	**MLD**	Previously, static MLD groups were not correctly added to interfaces on startup or when interface state changed. 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	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-73124	**Port Configuration** **VCStack**	Previously, the **`medium-type copper`** or **`medium-type fiber`** configuration would not apply correctly to a member joining a running stack and the configuration would be removed from the running-configuration. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-79410	**RADIUS**	This software update addresses RADIUS vulnerabilities as specified in CVE-2022-41860 and CVE-2022-41861. 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	–
CR-79417	**System**	This software update addresses a vulnerability as specified in CVE-2023-1095. 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	–
CR-79433	**System**	This software update addresses a vulnerability as specified in CVE-2023-1077. 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	–
CR-79435	**System**	This software update addresses a vulnerability as specified in CVE-2023-0179. 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	–
CR-79781	**System**	Previously, repeated entries of 'CTRL + C' keys on the CLI for copying, could cause an unexpected device restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-79395	**Tunnelling**	Previously, under some circumstances, IPSec tunnels could be unreachable over other IPSec tunnels. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79116	**Unicast Routing**	Previously, if QoS egress queue drop/transmit counters overflowed in hardware, the counters in **`show mls qos interface INTERFACE queue-counters`** would show correct values, but become busy and exhaust CPU resource. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	Y	–	Y	–	–	–	Y	–	Y	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–
CR-79504	**VCStack**	Previously, IP addresses learned by DHCP would not be properly learned by a backup member that joined an existing stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-79428	**VRF-lite**	Previously, the **`show run vrf`** output did not include BGP configuration. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–

What’s New in Version 5.5.2-2.6

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
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-2.6.

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 74.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 76. 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 Cloud		07/2023	vaa-5.5.2-2.6.iso (VAA OS) vaa-5.5.2-2.6.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-2.6.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	07/2023	SBx81CFC960-5.5.2-2.6.rel
SBx908 GEN2	SBx908 GEN2	07/2023	SBx908NG-5.5.2-2.6.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	07/2023	x950-5.5.2-2.6.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	07/2023	x930-5.5.2-2.6.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2023	x550-5.5.2-2.6.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	07/2023	x530-5.5.2-2.6.rel
x330-10GTX x330-20GTX x330-28GTX	x330	07/2023	x330-5.5.2-2.6.rel
x320-10GH x320-11GPT	x320	07/2023	x320-5.5.2-2.6.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2023	x230-5.5.2-2.6.rel
x220-28GS x220-52GT x220-52GP	x220	07/2023	x220-5.5.2-2.6.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	07/2023	IE340-5.5.2-2.6.rel
IE210L-10GP IE210L-18GP	IE210L	07/2023	IE210-5.5.2-2.6.rel
XS916MXT XS916MXS	XS900MX	07/2023	XS900-5.5.2-2.6.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	07/2023	GS980MX-5.5.2-2.6.rel
GS980EM/10H GS980EM/11PT	GS980EM	07/2023	GS980EM-5.5.2-2.6.rel
GS980M/52 GS980M/52PS	GS980M	07/2023	GS980M-5.5.2-2.6.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	07/2023	GS970EMX-5.5.2-2.6.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2023	GS970-5.5.2-2.6.rel
AR4000S-Cloud		07/2023	AR4000S-Cloud-5.5.2-2.6.iso AR4000S-Cloud-5.5.2-2.6.vhd and upload_vhd.py (for AWS)
10GbE UTM Firewall		07/2023	ATVSTAPL-1.7.2.iso and vfw-x86_64-5.5.2-2.6.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	07/2023	AR4050S-5.5.2-2.6.rel AR3050S-5.5.2-2.6.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	07/2023	AR2050V-5.5.2-2.6.rel AR2010V-5.5.2-2.6.rel AR1050V-5.5.2-2.6.rel

⚠ **Caution:** Software version 5.5.2-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-2.x. Such switches do 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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

Unsupported devices

Version 5.5.2-2.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-2.6 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the enhancements in software version 5.5.2-2.6.

Applies to all AlliedWare Plus products

ER-5399 With this software update, the 802.1X retransmission mechanism is now supported and if the Supplicant does not respond on an EAP Request, the Authenticator resends the EAP Request.

If a timeout occurs and the maximum number of retransmissions is reached, the authentication process will fail.

This change is ISSU compatible with conditions. As long as 'dot1x max-req' is not configured on the new release during upgrade, the upgrade process is safe because without configuring 'dot1x max-req' there is no difference in authd in old and new releases. It does not require to boot LIFs with new release as the change exists in authd only.

To configure the maximum number of retransmissions, a new command is available:

```
dot1x max-req <1-10>
no dot1x max-req
```

Example To configure the maximum number of EAP Request retransmission attempts for interface port1.0.1 to 3, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dot1x max-req 3
```

ISSU: Effective when CFCs upgraded

Issues Resolved in Version 5.5.2-2.6

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

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-75284	**ACL**	Previously, on x230 Series, when ACL lists were over subscribed, no error would be logged. This issue has been resolved.	Y	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-79282	**ACL**	Previously, modifying a named IPv4 ACL group, configured using the **`acl-group ip address`** command, by adding or deleting an IP address entry, could lead to incorrect application of hardware access-lists on an interface when there were multiple hardware access-lists configured. Similar behaviour could occur for the named port ACL group commands, **`acl-group ip port`** and **`acl-group ipv6 address`**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-79459	**ACL**	Previously, the system did not output any error when an ACL list on a port was oversubscribed. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-78746	**AMF**	Previously, a non-existent AMF node was displayed on the AMF security list and it could not be removed manually. 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	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79119	**AMF**	Previously, under certain unusual circumstances, TQ guest nodes backup could fail with the error message: "*Unable to open rsync log file*" 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	–
CR-79084	**AMF**	Previously, executing a "delete" after performing certain AMF provisioning actions, such as configuring a provisioned node's configuration file, backup configuration file, firmware release, or backup firmware release, could result in leaving AMF provisioning without a valid working directory. This meant that subsequent AMF provisioning actions could fail. 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	–	–
CR-77444	**AMF**	Previously on very rare occasions, application proxy was placed under extreme load, and it was possible for the AMF process to fail. This could also result in the failure of an AMF node to join an AMF network. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-79082	**AMF**	With this software update, only secure connection using TLS version 1.2 or later will be accepted in order to improve the security and integrity of connections between Vista Manager and AMF nodes via AMF Controllers or Masters. SSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
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 VCS stack 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-79525	**ARP** **Neighbor Discovery**	Previously, ARP learning was causing memory exhaustion. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-78714	**DNS**	Previously, there could be issues loading web pages due to a DNS error. 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	–
CR-79163	**DNS**	Previously, the DNS relay process could fail when upstream DNS servers were unreachable and deadtime was exceeded. 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	–	–
CR-79328	**EPSR, VCStack**	Previously, if an EPSR ring was broken, a stack member in the EPSR ring could fail to rejoin the stack when the EPSR ring recovered. This issue has been resolved.	Y	Y	–	–	–	–	Y	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-78551	**File System**	Previously, when the "strict-user-process-control" feature was enabled, certain system only files could still be accessed via the **mail** facility. 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	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-78553	**File System**	Previously, when the "strict-user-process-control" feature was enabled, certain system only files could still be accessed via **SCP** or **SFTP**. 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	–	–
CR-79493	**IPv6**	With this software update, adding or removing an IPv6 address from a VLAN now notifies eventwatch on Vista Manager. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-76763	**IPv6, Tunnelling**	Previously, if one of the transactions to the map rule server failed, it could result in the softwire configuration being deleted and cause the IPv4 tunnel connectivity to be removed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-76785	**LACP**	Previously, executing the **`show diagnostic channel-group`** command could result in a gradual accumulation of memory usage per channel-group. Unfortunately, this memory was not released or freed after each run of the 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	–	–
CR-79251	**Loop Detection**	Previously, after a system boot up, the first time a packet loop was detected by the loop protection feature, the specified action to break the loop did not operate correctly. LDF did operate correctly for any subsequently detected loops. This issue has been resolved.	Y	Y	–	–	–	Y	Y	–	Y	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-78748	**MAC Authentication**	Previously, when executing the **`clear mac address-table`** command, it did not clear the MAC addresses that were added by port-security when the MACs were learned on backup members of a stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-72577	**Pluggable Transceivers**	Previously, under some circumstances, the x220, x320, x530, x530L, and GS980MX series could log a large amount of "Port Manager queue has grown to XXX (250)" messages, if the stacking DAC cable was inserted in the SFP+ port. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	Y	–	–	Y	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-79612	**Pluggable Transceivers**	Previously, on x330 series, some SFPs might not be able to correctly link up with other link partners. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-78755	**Port Authentication** **VCStack**	Previously, when Port Authentication was configured on an aggregator, sometimes adding switchports of late-join stack members to the aggregator failed. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	–	Y	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-79057	**Port Configuration**	Previously, the ports on the x330 Series could occasionally flap when executing the **`show platform port`** command. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-79107	**Static Link Aggregation**	Previously, on x930-28GSTX variant, a combo port which was shut down in the startup config may link up on the copper port even though it still shows as link down. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-77361	**Switching**	Previously, on x530, x530L and GS980MX Series, when changing to a lower port speed of 1G or 100M, the 10 or 18 port models might take a long time to link up, or might fail to link. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-78481	**System**	This software update addresses a Linux Kernel vulnerability as addressed in CVE-2022-4129. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79364	**Upstream Forwarding**	Previously when moving hosts from an upstream to a downstream port, the device could undergo an unexpected re-start. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	–	–	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–	–
CR-78570	**VCStack**	Previously, if a stack was under heavy CPU load, there was a small chance that a rejoining stack member may not rejoin the stack correctly, triggering a duplicate master reboot. A message similar to the following would appear in the log when this issue occurred: 'daemon.err awplus corosync[2842]: [TOTEM] totemsrp.c:3797 FAILED TO RECEIVE.' This issue has been resolved.	Y	Y	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-78619	**VCStack**	Previously, on x950 Series stacks, under rare occasions, the stacking VLAN traffic would not be processed timely, resulting in TIPC time-outs and resiliency link healthcheck failures. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79090	**VRF-lite**	Previously, VRF routing was not processing traffic correctly, resulting in performance degradation. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	Y	Y	Y	–	–
CR-79100	**VRRP**	Previously, when multiple instances of VRRP were running on different subnets with varying subnet masks, there was a problem where some of the VRRP virtual router addresses became unreachable. This occurred due to miscalculations in assigning the masks to the virtual router addresses. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–

What’s New in Version 5.5.2-2.5

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
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-2.5.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the 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 74.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 76. 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 Cloud		04/2023	vaa-5.5.2-2.5.iso (VAA OS) vaa-5.5.2-2.5.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-2.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	04/2023	SBx81CFC960-5.5.2-2.5.rel
SBx908 GEN2	SBx908 GEN2	04/2023	SBx908NG-5.5.2-2.5.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	04/2023	x950-5.5.2-2.5.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	04/2023	x930-5.5.2-2.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2023	x550-5.5.2-2.5.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	04/2023	x530-5.5.2-2.5.rel
x330-10GTX x330-20GTX x330-28GTX	x330	04/2023	x330-5.5.2-2.5.rel
x320-10GH x320-11GPT	x320	04/2023	x320-5.5.2-2.5.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2023	x230-5.5.2-2.5.rel
x220-28GS x220-52GT x220-52GP	x220	04/2023	x220-5.5.2-2.5.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	04/2023	IE340-5.5.2-2.5.rel
IE210L-10GP IE210L-18GP	IE210L	04/2023	IE210-5.5.2-2.5.rel
XS916MXT XS916MXS	XS900MX	04/2023	XS900-5.5.2-2.5.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	04/2023	GS980MX-5.5.2-2.5.rel
GS980EM/10H GS980EM/11PT	GS980EM	04/2023	GS980EM-5.5.2-2.5.rel
GS980M/52 GS980M/52PS	GS980M	04/2023	GS980M-5.5.2-2.5.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	04/2023	GS970EMX-5.5.2-2.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2023	GS970-5.5.2-2.5.rel
AR4000S-Cloud		04/2023	AR4000S-Cloud-5.5.2-2.5.iso AR4000S-Cloud-5.5.2-2.5.vhd and upload_vhd.py (for AWS)
10GbE UTM Firewall		04/2023	ATVSTAPL-1.7.2.iso and vfw-x86_64-5.5.2-2.5.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	04/2023	AR4050S-5.5.2-2.5.rel AR3050S-5.5.2-2.5.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	04/2023	AR2050V-5.5.2-2.5.rel AR2010V-5.5.2-2.5.rel AR1050V-5.5.2-2.5.rel

Caution: Software version 5.5.2-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-2.x. Such switches do 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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

Unsupported devices

Version 5.5.2-2.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-2.5 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.2-2.5

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

CR	Module	Description	GS970M\EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-76217	**ACL**	On SBx81GS24a and SBx81XS6 LIFs, it was possible for certain combinations of ACLs to result in incorrect behaviour. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-78841	**ACL**	Previously, the ACL Hit Counters weren't operating correctly on the x320 Series. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-78869	**ACL**	Previously, when editing an ACL attached to a VLAN access-map after it had already been applied, the changed entries may not have been correctly applied. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	Y	Y	Y	–	–	Y	–	Y	Y	Y	–	–	–	Y	–	–	–	–	–	–	–
CR-78359	**AMF**	Previously, on occasion, excessive error log messages of: "*Input suspended. Re-queuing event*" were generated when an AMF remote login session was disconnected. 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	–
CR-78518	**AMF**	Previously, when a redundant virtual-link was configured and in a blocking state, it was possible for the interface to still forward traffic while in a blocking state, causing a loop. This issue is now resolved and the redundant virtual link is now correctly set to Down when in a blocking state. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-78544	**AMF**	Previously it was possible for an AMF network to become unstable (nodes continuously leaving and joining) when a node was evicted due to an overrun of licensed nodes. 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	–

CR	Module	Description	GS970M\EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-77489	**ARP, Neighbor Discovery, VCStack**	Previously, in specific VCS configurations utilizing static aggregators and VCS resiliency links, ARP entries might not get flushed correctly when a VCS master failover occured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-78836	**AWC-lite, SESC**	Previously, AlliedWare Plus software versions earlier than 5.5.2-2.x were unable to communicate with AMF-SEC version 2.4.0 or later, due to the disabling of TLS v1.0 and 1.1. This issue has now been resolved, and the cypher suites for AWC-lite have been updated.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	–
CR-78732	**Boot**	Previously on releases 5.5.2-1 and 5.5.2-2, the x930-28GSTX could lockup during boot, eventually restarting. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-78767	**Cellular Modem**	Previously, the AR4050S-5G device GUI was not displaying the Modem state slot ID correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-78769	**Cellular Modem**	Previously, the AR4050S-5G device GUI was not displaying the 5G carriers on the Wireless WAN page due to a missing API. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-78798	**Cellular Modem**	Previously, the AR4050S-5G device GUI was not displaying the build ID for each slot of modem firmware due to a missing API. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-78208	**Cellular Modem**	Previously LTE B40 and 5g Sub band n40 were enabled but not certified. These bands have now been disabled.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-76753	**Cellular Modem**	Previously, the slot information was listed as "Empty" for active status in the **`show 5g carrier`** command output. The command output now provides more descriptive information This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-78340	**DHCP Server**	Previously, a system reboot could occur in DHCP. 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	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-78654	**DHCP Server**	Previously the DHCP lease list was not in sorted order as required by the **`show`** command. This issue has now been resolved and a sorted list of DHCP leases is now output correctly in the **`show dhcp binding`** command output. 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	–
CR-78768	**DHCP Snooping**	Previously, when DHCP snooping was enabled with DHCP relay on the network, DHCP reply packets were forwarded with a vlan tag to untagged switch ports. This issue has been resolved. Now, the 802.1Q vlan tag is properly set to DHCP reply packets when transmitted to tagged switch ports. ISSU: Effective when ISSU complete.	Y	–	Y	–	Y	–	–	Y	–	Y	Y	Y	–	–	–	Y	–	–	–	–	–	–	–
CR-78222	**DNS** **Security**	This software update addresses security vulnerability issues as specified in: CVE-2022-0934 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-78466	**Environmental Monitoring**	Previously on very rare occasions, spurious PSU alarm logs could be generated for AT-PWR600 PSUs. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-78569	**FDB**	Previously, static MAC entries could result in hash collisions in the FDB due to a suboptimal hashing algorithm being used by default. This has been resolved by using a superior hashing algorithm by default, resulting in a much lower chance of hash collisions occurring.	–	–	–	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-78673	**IDS/IPS**	Previously the commands **`show ips categories`** and **`show ips categories details`** would not always generate the correct output. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–

CR	Module	Description	GS970M\EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-76232	**IPv6**	Previously, IPv6 auto-configured addresses via ND proxy may not have had their valid and preferred lifetimes topped up by RAs with the same valid and preferred lifetimes as the original RA that assigned the address prefix. 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
CR-78819	**Linkmon, SNMP**	Previously, the Linkmon MIB could not be read or written to via SNMP. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–
CR-78070	**Loop Protection** **VCStack**	Previously, invalid loop protection interface configuration could appear after a stack member bootup. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-76100	**PoE**	■ Previously, LLDP would report a 0mW allocation when 71,300 mW was requested. This issue has been resolved. ■ Previously, LLDP power allocation requests for dual signature devices class 1-3 were being unintentionally ignored in some scenarios. This issue has been resolved. ■ Previously, on the x530DP-28GHXm and x530DP-52GHXm, LLDP requests for power from powered devices could request more than what was allowed for a PoE+ (60W) port. The incorrectly configured power limit was shown in the CLI command **`show power-inline`** and in LLDP packets (however, powered devices still could not draw more than 60W from a PoE+ port). This issue has been resolved. ■ Previously, on x530DP-28GHXm and x530DP-52GHXm products, on PoE+ (60W) ports when a powered device (PD) requested PoE++ (90W) power (single signature classes 7 and 8 and dual signature class 5) the class shown in the **`show power-inline`** and **`show power-inline interface detail`** commands reflected the powered device requested class. This has been changed and now the class shown is the class assigned by the power sourcing equipment (PSE - x530DP), and an asterisk * is shown to indicate the class has been demoted (or "(demoted)" in the detailed version of the command). For example, if a PD requests class 8 now class 6* is shown. This is in line with the x530DP ports being PoE+ (60W), not PoE++ (90W). ISSU: Effective when ISSU complete.	–	–	–	–	Y	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-77529	**Port Authentication**	Previously, it was possible for stale IP information for a MAC authenticated supplicant to incorrectly cause an authenticating web-auth supplicant to report it was authenticated before authentication had completed. 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	–

CR	Module	Description	GS970M\EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-77605	**Port Authentication, VCStack**	Previously, port authentication supplicant MAC addresses were not being deleted from the FDB when the supplicant audit had failed and the supplicant was unauthorized. This issue was only present on VCStacks, and has been resolved.	–	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-78930	**PPPoE-AC**	Previously, since AlliedWare Plus software version 5.5.1, L2TPv2 could fail to establish a connection to the LNS. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–
CR-78068	**QoS, VCStack**	Previously, if a policy-map was configured to set new-DSCP, this could fail on VCStack members that were rebooted and rejoined the VCStack. This issue has been resolved. ISSU: Effective when ISSU complete.	–	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-78188	**Security**	This software update addresses security vulnerability issues as specified in: CVE-2022-29154. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-78189	**Security**	This software update addresses security vulnerability issues as specified in: CVE-2022-37434 ISSU: ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-78498	**SNMP**	Previously, it was possible for SNMP to fail when the system was busy. 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	–
CR-78382	**SNMP** **Security**	This software update addresses security vulnerability issues as specified in: CVE-2022-44792 and CVE-2022-44793 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	–
CR-78434	**SNMP** **Security**	Previously, an SNMP MIB browser might fail to get the mib object value of freeMemory: (1.3.6.1.4.1.207.8.4.4.3.7.1). 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	–
CR-78634	**Tech-support**	Previously, ports on the XEM2-12XSv2, XEM2-8XSTm, and x550-18XSQ, could go down when generating a **`show tech support`** file. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-78646	**Tech-support**	Previously, in some instances a system reboot could occur when performing a **`show tech support`** on x950 or x908Gen2 platforms. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–
CR-76523	**Unicast Routing**	In certain unusual routing scenarios a system reboot could occur when evaluating routes as a result of a link going down. One mitigation for this is to not use the default route to resolve recursive next hops. A new command is introduced to enable/disable the use of a default route to resolve next hops in IP routing: ■ To enable the use of a default route, use the command: `ip resolve-via-default` ■ To disable the use of a default route, use the command: `no ip resolve-via-default`	–	–	–	Y	–	–	Y	–	–	–	–	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	–
CR-73422	**Unicast Routing**	Previously, in certain complex routing situations, rebooting one device could cause another device to reboot as part of transient routing changes. This issue has been resolved. With this software update, the routing calculation has been improved to prevent this from happening. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-73081	**VCStack**	Previously, there was a delay between a member leaving the stack and its ports being logically removed. If an auth audit was being executed during this time, the audit could fail. This issue has been resolved.	–	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-73699	**VCStack ARP**	Previously, it was possible to exhaust memory with a particular combination of ARP traffic. This issue has been resolved.	–	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	GS970M\EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-73842	**VXLAN**	Previously, if an MLD report was received on a VLAN that had MLD snooping disabled, it could cause a multicast loop between VXLAN tunnel endpoints. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	Y	–	–	–	–	–	–

What’s New in Version 5.5.2-2.4

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
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-2.4.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the 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 74.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 76. 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 Cloud		02/2023	vaa-5.5.2-2.4.iso (VAA OS) vaa-5.5.2-2.4.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-2.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	02/2023	SBx81CFC960-5.5.2-2.4.rel
SBx908 GEN2	SBx908 GEN2	02/2023	SBx908NG-5.5.2-2.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	02/2023	x950-5.5.2-2.4.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	02/2023	x930-5.5.2-2.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	02/2023	x550-5.5.2-2.4.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	02/2023	x530-5.5.2-2.4.rel
x330-10GTX x330-20GTX x330-28GTX	x330	02/2023	x330-5.5.2-2.4.rel
x320-10GH x320-11GPT	x320	02/2023	x320-5.5.2-2.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	02/2023	x230-5.5.2-2.4.rel
x220-28GS x220-52GT x220-52GP	x220	02/2023	x220-5.5.2-2.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	02/2023	IE340-5.5.2-2.4.rel
IE210L-10GP IE210L-18GP	IE210L	02/2023	IE210-5.5.2-2.4.rel
XS916MXT XS916MXS	XS900MX	02/2023	XS900-5.5.2-2.4.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	02/2023	GS980MX-5.5.2-2.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	02/2023	GS980EM-5.5.2-2.4.rel
GS980M/52 GS980M/52PS	GS980M	02/2023	GS980M-5.5.2-2.4.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	02/2023	GS970EMX-5.5.2-2.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	02/2023	GS970-5.5.2-2.4.rel
AR4000S-Cloud		02/2023	AR4000S-Cloud-5.5.2-2.4.iso AR4000S-Cloud-5.5.2-2.4.vhd and upload_vhd.py (for AWS)
10GbE UTM Firewall		02/2023	ATVSTAPL-1.7.2.iso and vfw-x86_64-5.5.2-2.4.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	02/2023	AR4050S-5.5.2-2.4.rel AR3050S-5.5.2-2.4.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	02/2023	AR2050V-5.5.2-2.4.rel AR2010V-5.5.2-2.4.rel AR1050V-5.5.2-2.4.rel

⚠ **Caution:** Software version 5.5.2-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-2.x. Such switches do 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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

Unsupported devices

Version 5.5.2-2.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-2.4 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.2-2.4

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-78732	**Boot**	This software change applies to x930-28GSTX only. Previously, x930-28GSTX running 5.5.2-1 and 5.5.2-2 could hang during bootup, eventually causing the switch to restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–

What’s New in Version 5.5.2-2.3

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
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-2.3.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the 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 74.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 76. 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 Cloud		01/2023	vaa-5.5.2-2.3.iso (VAA OS) vaa-5.5.2-2.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-2.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	01/2023	SBx81CFC960-5.5.2-2.3.rel
SBx908 GEN2	SBx908 GEN2	01/2023	SBx908NG-5.5.2-2.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	01/2023	x950-5.5.2-2.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	01/2023	x930-5.5.2-2.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2023	x550-5.5.2-2.3.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	01/2023	x530-5.5.2-2.3.rel
x330-10GTX x330-20GTX x330-28GTX	x330	01/2023	x330-5.5.2-2.3.rel
x320-10GH x320-11GPT	x320	01/2023	x320-5.5.2-2.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2023	x230-5.5.2-2.3.rel
x220-28GS x220-52GT x220-52GP	x220	01/2023	x220-5.5.2-2.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	01/2023	IE340-5.5.2-2.3.rel
IE210L-10GP IE210L-18GP	IE210L	01/2023	IE210-5.5.2-2.3.rel
XS916MXT XS916MXS	XS900MX	01/2023	XS900-5.5.2-2.3.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	01/2023	GS980MX-5.5.2-2.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	01/2023	GS980EM-5.5.2-2.3.rel
GS980M/52 GS980M/52PS	GS980M	01/2023	GS980M-5.5.2-2.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	01/2023	GS970EMX-5.5.2-2.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2023	GS970-5.5.2-2.3.rel
AR4000S-Cloud		02/2023	AR4000S-Cloud-5.5.2-2.3.iso AR4000S-Cloud-5.5.2-2.3.vhd and upload_vhd.py (for AWS)
10GbE UTM Firewall		01/2023	ATVSTAPL-1.7.2.iso and vfw-x86_64-5.5.2-2.3.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	01/2023	AR4050S-5.5.2-2.3.rel AR3050S-5.5.2-2.3.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	01/2023	AR2050V-5.5.2-2.3.rel AR2010V-5.5.2-2.3.rel AR1050V-5.5.2-2.3.rel

⚠ **Caution:** Software version 5.5.2-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-2.x. Such switches do 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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

Unsupported devices

Version 5.5.2-2.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-2.3 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the enhancements in 5.5.2-2.3.

Support for AMF Plus

Applies to all AlliedWare Plus products

This software update supports the new AMF Plus menu in Vista Manager EX 3.10.1. For details, see https://www.alliedtelesis.com/documents/vista-manager-ex-release-note.

Support for AR4000S-Cloud Virtual UTM Firewall

This software update supports the newly-released AR4000S-Cloud. This high-performance virtual firewall includes inter-office SD-WAN connectivity, remote worker VPNs, and easy access to cloud-based applications. For details, see our website.

What’s New in Version 5.5.2-2.2

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
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-2.2.

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 74.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 76. 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 Cloud		01/2023	vaa-5.5.2-2.2.iso (VAA OS) vaa-5.5.2-2.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-2.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	01/2023	SBx81CFC960-5.5.2-2.2.rel
SBx908 GEN2	SBx908 GEN2	01/2023	SBx908NG-5.5.2-2.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	01/2023	x950-5.5.2-2.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	01/2023	x930-5.5.2-2.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2023	x550-5.5.2-2.2.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	01/2023	x530-5.5.2-2.2.rel
x330-10GTX x330-20GTX x330-28GTX	x330	01/2023	x330-5.5.2-2.2.rel
x320-10GH x320-11GPT	x320	01/2023	x320-5.5.2-2.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2023	x230-5.5.2-2.2.rel
x220-28GS x220-52GT x220-52GP	x220	01/2023	x220-5.5.2-2.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	01/2023	IE340-5.5.2-2.2.rel
IE210L-10GP IE210L-18GP	IE210L	01/2023	IE210-5.5.2-2.2.rel
XS916MXT XS916MXS	XS900MX	01/2023	XS900-5.5.2-2.2.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	01/2023	GS980MX-5.5.2-2.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	01/2023	GS980EM-5.5.2-2.2.rel
GS980M/52 GS980M/52PS	GS980M	01/2023	GS980M-5.5.2-2.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	01/2023	GS970EMX-5.5.2-2.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2023	GS970-5.5.2-2.2.rel
10GbE UTM Firewall		01/2023	ATVSTAPL-1.7.2.iso and vfw-x86_64-5.5.2-2.2.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	01/2023	AR4050S-5.5.2-2.2.rel AR3050S-5.5.2-2.2.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	01/2023	AR2050V-5.5.2-2.2.rel AR2010V-5.5.2-2.2.rel AR1050V-5.5.2-2.2.rel

⚠ **Caution**: Software version 5.5.2-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-2.x. Such switches do 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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

Unsupported devices

Version 5.5.2-2.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-2.2 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the enhancements in 5.5.2-2.2

TLS authentication on mail client

ER-5174: Available on GS970EMX, GS970M, GS980EM, GS980M, GS980MX, XS900MX, IE340, IE210L, x220, x230/x230L, x320, x330, x530 / x530L, x550, x930, x950, SBx908Gen2, SBx81CFC960, AR1050V, AR4050S, AR2050V/AR2010V, AR4050S-5G, AR3050S Series.

With this software update, TLS authentication is supported on the AlliedWare Plus mail client.

Unicast forwarding

ER-5196: Available on x330 Series.

With this software update, ECMP routing is now enabled on the x330 Series.

Issues Resolved in Version 5.5.2-2.2

This AlliedWare Plus maintenance version includes the following resolved issues:

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-77887	**ACL**	Previously, adding a list of hardware ACLs on a switch could sometimes cause the switch to restart unexpectedly. This issue has been resolved.	Y	Y	Y	–	–	Y	Y	–	Y	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-77962	**ACL, VLAN**	This software update fixes a number of issues related to configuring VLAN filters and ACL groups. These issues have been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-76935	**AMF**	Previously, it was possible for AMF automatic node recovery to occasionally fail. 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	–
CR-77916	**AWC-lite, Device GUI**	Previously, executing a wireless task on a CWM capable switch could sometimes cause the switch to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	–
CR-78193	**BGP**	Previously, BGP was not compatible with extended attributes as stated under RFC4271. With this software update, AlliedWare Plus BGP implementation now conforms with RFC 4271. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–
CR-76833	**Environmental Monitoring**	With this software update, the PWR1200 v2 is now supported on the x930 series.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-77777	**Multicast Forwarding HW**	With this software upate, an issue impacting the CPU performance around sending multicast packets has been resolved.	Y	Y	–	–	–	Y	Y	–	Y	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-77739	**Pluggable Transceivers**	Previously, under rare circumstances, a fiber SFP in the combo port of a x930-GSTX would not come up at startup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-78157	**Pluggable Transceivers**	Previously, on insertion of a DAC cable, the link could flap before settling into the correct 'up' state. This issue has been resolved.	Y	Y	–	–	–	–	–	–	Y	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-77782	**sFlow, VCStack**	Previously, a stack failover could make sFlow stop sending samples to the sFlow collector. This issue has been resolved.	Y	Y	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-78227	**SNMP**	With this software update, MIB will no longer report usage values for shared and cached memory, (OIDs 1.3.6.1.2.1.25.2.3.1.6.7 and .8) since they previously created a false positive alert that could be safely ignored. Popular SNMP management tools that monitor the Host Resource MIB such as SolarWinds, will no longer create critical alerts for the cached and shared memory resources. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77793	**SSH**	Previously, known SSH hosts were not saved properly, which meant typing in "yes" for accepting connection to hosts that were already connected. 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	–
CR-78392	**Static Aggregation, QoS HW, VCStack**	Previously, using the **`static-channel-group member-filters`** command on a switchport would fail during VCStack bootup if there was a service-policy configured on the same switchport. This issue has been resolved.	Y	Y	–	Y	Y	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-78090	**VCStack, QoS HW**	Previously, the **`wrr-queue weight`** commands might not be synchronised across to the VCStack backup member. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE210L	IE340	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR3040S-5G	AMF Cloud
CR-78339	**VCStack, QoS HW**	Previously, the QoS configuration command **`wrr-queue egress-rate-limit`** could fail to execute on a late joining stack member. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	Y	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-78066	**VCStack, VRRP**	Previously, VRRP advertisement packets could occasionally be dropped as a result of a buffer overflow. This triggered a VRRP transition message to be logged. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–

What’s New in Version 5.5.2-2.1

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
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-2.1.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the 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 74.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 76. 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 Cloud		11/2022	vaa-5.5.2-2.1.iso (VAA OS) vaa-5.5.2-2.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-2.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2022	SBx81CFC960-5.5.2-2.1.rel
SBx908 GEN2	SBx908 GEN2	11/2022	SBx908NG-5.5.2-2.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	11/2022	x950-5.5.2-2.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	11/2022	x930-5.5.2-2.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2022	x550-5.5.2-2.1.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	11/2022	x530-5.5.2-2.1.rel
x330-10GTX x330-20GTX x330-28GTX	x330	11/2022	x330-5.5.2-2.1.rel
x320-10GH x320-11GPT	x320	11/2022	x320-5.5.2-2.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2022	x230-5.5.2-2.1.rel
x220-28GS x220-52GT x220-52GP	x220	11/2022	x220-5.5.2-2.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	11/2022	IE340-5.5.2-2.1.rel
IE210L-10GP IE210L-18GP	IE210L	11/2022	IE210-5.5.2-2.1.rel
XS916MXT XS916MXS	XS900MX	11/2022	XS900-5.5.2-2.1.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	11/2022	GS980MX-5.5.2-2.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2022	GS980EM-5.5.2-2.1.rel
GS980M/52 GS980M/52PS	GS980M	11/2022	GS980M-5.5.2-2.1.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	11/2022	GS970EMX-5.5.2-2.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2022	GS970-5.5.2-2.1.rel
10GbE UTM Firewall		11/2022	ATVSTAPL-1.7.2.iso and vfw-x86_64-5.5.2-2.1.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	11/2022	AR4050S-5.5.2-2.1.rel AR3050S-5.5.2-2.1.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	11/2022	AR2050V-5.5.2-2.1.rel AR2010V-5.5.2-2.1.rel AR1050V-5.5.2-2.1.rel

Caution: Software version 5.5.2-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-2.x. Such switches do 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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

Unsupported devices

Version 5.5.2-2.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-2.1 software version is not ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.2-2.1:

- "Alternative and additional security options" on page 53
- "Ability to specify a VRF for NTP, SNMP, sFlow and SSH features" on page 55
- "VRRP support on 10GbE UTM firewall" on page 56
- "WAN load balancing weighted lottery mode on 10GbE UTM firewall" on page 56
- "Support for TQ6602 GEN2 and TQm6602 GEN2 APs as AMF guest nodes" on page 57
- "Prevention of flooding of multicast packets to CPU when IGMP or MLD snooping are disabled" on page 57
- "Increase in supported number of link aggregation groups on SBx908 GEN2" on page 57
- "QoS enhancements" on page 57
- "Environment sensor readings hidden for missing PSUs on x930 and x530DP Series switches" on page 58
- "Display the whole interface description" on page 58
- "Change to clearing of access list counters" on page 58
- "Reduction in acceptable input voltage level on IE340 Series" on page 59
- "More frequent polling of voltage level on IE340 Series" on page 59
- "Force Power Save Disabled setting for Channel Blanket" on page 59
- "Support for Channel Blanket on TQ6702 GEN2 and AT-TQ6602 GEN2" on page 60
- "Strict User Process Control" on page 60
- "Increase to default VTY limit" on page 61
- "Increase to maximum RSA key length" on page 61

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 69.

Alternative and additional security options

Advanced IPS

Available on: AR4050S, AR4050S-5G, and 10GbE UTM Firewall

From version 5.5.2-2.1 onwards, AlliedWare Plus provides Advanced IPS (Intrusion Prevention System) functionality.

This is made possible by the addition of the third-party vendor Proofpoint's ET Pro Ruleset. The Proofpoint ET Pro Ruleset detects and blocks advanced threats. Updated daily, it covers Malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing. It also detects and blocks distributed denial-of-service attacks (DDoS), protocol and application anomalies, exploit kits and supervisory control and data acquisition (SCADA) attacks.

Advanced IPS requires a license, which is available in the bundle pack: AT-AR4-UTM-02-1/3/5YR. Contact your authorized Allied Telesis support center to obtain a license.

Webroot

Available on: AR3050S, AR4050S, AR4050S-5G, and 10GbE UTM Firewall

Also available from version 5.5.2-2.1, support for provider Webroot has be added to Web Categorization and Web Control. Webroot delivers multi-vector protection for endpoints and networks and threat intelligence.

Web control requires a license, which is available in the bundle packs: AT-AR3-UTM-01-1/3/5YR and AT-AR4-UTM-01-1/3/5YR. Contact your authorized Allied Telesis support center to obtain a license.

New URL Filtering solution

Available on: AR3050S, AR4050S, AR4050S-5G, and 10GbE UTM Firewall

Additionally, an alternative solution for Kaspersky URL Filtering based on a combination of DPI Web Categorization (provider Webroot) and firewall rules has been added.

Support for existing features/capabilities via Digital Arts and Kaspersky remain.

New and updated commands

There a number of new and updated commands in support of IPS and DPI functionality with this software release, they are as follows:

New commands

- dpi categorize

```
awplus(config)# dpi categorize <url-list>
```

- provider (IPS)

```
awplus(config-ips)# provider proofpoint
```

- sid

```
awplus(config-ips)# sid <1-2147483647> action [alert|deny|
disable]
```

- update-interval (IPS)

```
awplus(config-ips)# update-interval {minutes <10-525600>|hours
<1-8760>|days <1-365>|weeks <1-52>|never}
```

- show ips categories detail

```
awplus# show ips categories detail [<category-name>]
```

```
awplus#show ips categories detail activex
  Category (* = invalid) Action  Rules Description
--------------------------------------------------------------------------------
  activex                alert   242   Signatures for protection against
                                         attacks on Microsoft ActiveX controls
                                         and exploits targeting vulnerabilities
                                         in ActiveX controls
```

Updated commands

The categorization provider - Webroot is added to and displayed in the following commands:

- provider (web-control)

```
awplus(config-web-control)# provider [digitalarts|webroot]
```

- web-categorization

```
awplus(config-dpi)# web-categorization [digital-arts|webroot]
```

- show dpi

```
awplus#show dpi
Status:       running
Provider:     built-in
Mode:         assured
Counters:     global only
Providing application database: disabled
Web Categorization:          enabled
Web Categorization Provider: webroot
```

For more information about advanced network security features on the AlliedWare Plus UTM firewalls, see the Advanced Network Protection Feature Overview and Configuration Guide.

Ability to specify a VRF for NTP, SNMP, sFlow and SSH features

Available on all AlliedWare Plus devices that support VRF-lite

From version 5.5.2-2.1 onwards, AlliedWare Plus provides VRF support for NTP, SNMP, sFlow and SSH features.

NTP You can now specify a VRF instance for the NTP server to run in.

Note: This command does not work when a hostname is used. It only works if an IP address is specified.

A VRF parameter has been added to the **ntp server** command:

```
ntp server {<serveraddress>} [vrf <vrf-name>] [prefer] [key
<key>] [version <version>]
```

A VRF parameter has been added to the **ntp peer** command:

```
ntp peer {<peeraddress>} [vrf <vrf-name>] [prefer] [key <key>]
[version <version>]
```

SNMP You can use this new command **snmp-server vrf** to isolate the SNMP Agent to operate within a previously configured non-global named VRF. This means the SNMP Agent can only respond to requests from SNMP Managers operating within the same VRF.

```
snmp-server vrf [<vrf-name>]
```

```
no snmp-server vrf
```

Use the **no** variant of this command to revert the SNMP Agent to operating within the default global VRF.

sFlow A VRF parameter has been added to the **sflow collector id** command:

```
sflow collector id <1-5> ip <ip-address> [vrf <vrf-name>]
[port <1-65535>|max-datagram-size <200-1500>]
```

SSH You can use this new command to modify the configured VRF of the SSH client. Use this configuration for any SSH client on the device to connect to remote SSH servers.

This change affects all new user shell sessions. Existing sessions will not be affected.

A user may override this on a per-session basis using the **exec mode** variant of this command.

```
ssh client vrf [<vrf-name>]
no client vrf
```

Use the **no** variant of this command to restore the configured VRF to the default global VRF.

For more information about VRF features on AlliedWare Plus switches and firewalls, see the VRF-lite Feature Overview and Configuration Guide.

VRRP support on 10GbE UTM firewall

From 5.5.2-2.1 onwards, the 10GbE UTM firewall supports VRRP on ethernet interfaces and 802.1q sub-interfaces. This means you can configure VRRP on interfaces such as eth1 and eth1.1.

The 10GbE UTM firewall is an application that you can install on the Allied Telesis network appliance.

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

WAN load balancing weighted lottery mode on 10GbE UTM firewall

From version 5.5.2-2.1 onwards, you can use weighted lottery mode for distributing traffic between static routes.

Weighted lottery mode can be used when you have two or more static routes with the same destination. Using the **ip route** command with the **weight** parameter, you can set a weight for each static route. AlliedWare Plus distributes the traffic based on the number of sessions that are connected through the interfaces. It uses the weight that you assign to each interface to calculate a percentage of the total sessions that are allowed to connect through each interface. It then distributes the number of sessions between the interfaces accordingly.

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

The 10GbE UTM firewall is an application that you can install on the Allied Telesis network appliance.

Support for TQ6602 GEN2 and TQm6602 GEN2 APs as AMF guest nodes

Available on all AlliedWare Plus devices

From version 5.5.2-2.1 onwards, AlliedWare Plus supports TQ6602 GEN2 and TQm6602 GEN2 APs as AMF guest nodes. You can configure these APs as static guest nodes, or configure AMF to discover them through DHCP snooping or LLDP.

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

Prevention of flooding of multicast packets to CPU when IGMP or MLD snooping are disabled

Available on all AlliedWare Plus switches

From version 5.5.2-2.1 onwards, if you disable IGMP or MLD snooping, the switch no longer floods unknown multicast packets to its CPU. This means you can disable IGMP and MLD snooping if necessary, without risking packet loss from high CPU usage.

For more information about IGMP and MLD Snooping, see the IGMP/MLD Feature Overview and Configuration Guide.

Increase in supported number of link aggregation groups on SBx908 GEN2

From version 5.5.2-2.1 onwards, 168 link aggregation groups (LAGs) are supported on SBx908 GEN2 switches.

For more information about link aggregation, see the Link Aggregation: LACP and Static Channel Groups Feature Overview and Configuration Guide.

QoS enhancements

Available on all AlliedWare Plus switches

From version 5.5.2-2.1 onwards, QoS has the following enhancements:

Clear queue pass/drop counters

You can now reset the queue pass/drop counters on a switchport, by using the command:

```
awplus#clear mls qos interface <port> queue-counters
```

Give a queue a description

You can now give a queue a description, by using the optional **description** parameter in the command:

```
awplus(config)#mls qos queue <0-7> name <name> description
<description>
```

The description can be a word or a phrase.

Display queue pass/drop counters

You can now display the queue pass/drop counters for a switchport, by using the command:

```
awplus#show mls qos interface <port> queue-counters
```

Environment sensor readings hidden for missing PSUs on x930 and x530DP Series switches

From version 5.5.2-2.1 onwards, the environment sensor readings for removable PSUs on x930 and x530DP Series switches are hidden unless the PSU is physically present. Previously, when there was no PSU, these sensors read 0 for fan sensors and -128 for temperature sensors.

You can see sensor readings in the output of the command **show system environment** and through SNMP.

Display the whole interface description

Available on all AlliedWare Plus devices

From version 5.5.2-2.1 onwards, the **show interface status** command displays the whole interface description in its 'Name' column. Previously, only the first 18 characters of the name displayed.

Some other small changes were made to the command output too, including displaying a dash (-) in empty columns and changing 'err-disabled' to 'err-disable'.

Change to clearing of access list counters

Available on all AlliedWare Plus switches

From version 5.5.2-2.1 onwards, entering the **show access-list counters** command no longer clears the ACL hit counters. Instead, you can clear the counters whenever you want to by entering the new command:

```
awplus#clear access-list counters [<acl>]
```

where the optional <*acl*> parameter is the name or number of an ACL whose counters you want to clear.

This change means that output of the **show access-list counters** command now displays the count of hits for each ACL since the last time the counters were cleared with the **clear access-list counters** command.

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

Reduction in acceptable input voltage level on IE340 Series

From version 5.5.2-2.1 onwards, when PoE is disabled on IE340 Series switches, the lower voltage limit has been reduced. The new minimum voltages are:

- Without PoE: 18V (reduced from 52.5V)
- With PoE: 46V (reduced from 52.5V)

If the voltage is less than these minimums, the switch generates an alarm.

This improvement means that if you are not using PoE++, you do not need a PoE++ capable power supply.

More frequent polling of voltage level on IE340 Series

From version 5.5.2-2.1 onwards, the power supply voltage is now checked more frequently on IE340 Series switches. It is now checked every 10 seconds instead of every 30 seconds. This change lets you respond more quickly to a potential power issue. It also makes it more likely for the switch to alert you to a short-duration problem in the power supply.

Force Power Save Disabled setting for Channel Blanket

Available on all devices that support Channel Blanket in Vista Manager mini for wireless control.

Some models of wireless client may unintentionally change to power saving mode, even if the connection between the AP and client is alive. From version 5.5.2-2.1 onwards, you can enable the Force Power Save Disabled setting to avoid this. This will prevent clients from changing to power saving mode.

To enable this, use the following commands (this example uses profile 10):

```
awplus(config)#wireless
awplus(config-wireless)#ap-profile 10
awplus(config-wireless-ap-prof)#channel-blanket
awplus(config-wireless-ap-prof-cb)#force-power-save-disable
```

Support for Channel Blanket on TQ6702 GEN2 and AT-TQ6602 GEN2

Available on all devices that support Vista Manager mini for wireless control. The APs must be running firmware version 8.0.2-1.1 or later.

From version 5.5.2-2.1 onwards, you can use selected AlliedWare Plus devices to configure and manage Channel Blanket on your TQ6702 GEN2 and TQ6602 GEN2 access points. Channel Blanket offers true seamless roaming.

You can also configure and manage Channel Blanket on these APs using Device GUI version 2.13.0 or later on the AlliedWare Plus device.

For more information, see the Autonomous Wave Control chapter of your device's Command Reference and the Wireless Management (AWC) with Vista Manager Mini User Guide.

Strict User Process Control

Available on all AlliedWare Plus devices

From 5.5.2-2.1 onwards, Strict User Process Control protects sensitive system files from unnecessary user access. The affected commands are file and directory manipulation commands and trigger scripting. To enable Strict User Process Control, use the new command:

```
awplus(config)# strict-user-process-control
```

In order to maintain backward compatibility, Strict User Process Control is disabled by default. When you enter the **strict-user-process-control** command, it prompts you for a password. Make the password different from any existing privileged management passwords. Store the password carefully and securely, because you will need it if you want to disable the feature using the **no** form of the command.

The command must be entered from a physical console; entering it from a remote login session is not allowed for extra security.

You can use the show running-config command to confirm whether Strict User Process Control is on or off. If the feature is running the output will contain the command **strict-user-process-control**.

The commands affected by Strict User Process Control are:

- activate <*script-name*>
- copy [force] <*source-name*> <*destination-name*>
- copy <*file-name*> zmodem
- copy <*file-name*> startup-config
- copy current-software <*file-name*>
- copy running-config <*file-name*>

- copy startup-config <*file-name*>
- copy buffered-log <*file-name*>
- copy permanent-log <*file-name*>
- delete <*file-name*>
- edit [<*file-name*>]
- move <*source-name*> <*destination-name*>
- mkdir <*file-name*>
- rmdir <*file-name*>
- show file <*file-name*>
- show commands with output redirection

Increase to default VTY limit

Available on all AlliedWare Plus devices

From 5.5.2-2.1 onwards, the default VTY limit has been raised to 8 (from 5). This makes sure that it is possible to access the device via SSH if the GUI is in heavy use.

Increase to maximum RSA key length

Available on all AlliedWare Plus devices

From 5.5.2-2.1 onwards, the maximum RSA key length has been extended to16384 bits for all commands that enable you to generate RSA keys.

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.2-2.x and 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 5.5.1-1.x version, please check the 5.5.1-2.x and 5.5.2-0.x release note. Release notes are available from our website, including:

- 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 63 and “Details for x930 Series” on page 64 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, **versions 5.5.0-0.1** and later are affected, on switches where the bootloader is older than 6.2.24. If your bootloader is older than 6.2.24, you **cannot** upgrade to versions 5.5.0-0.1 and later directly from:

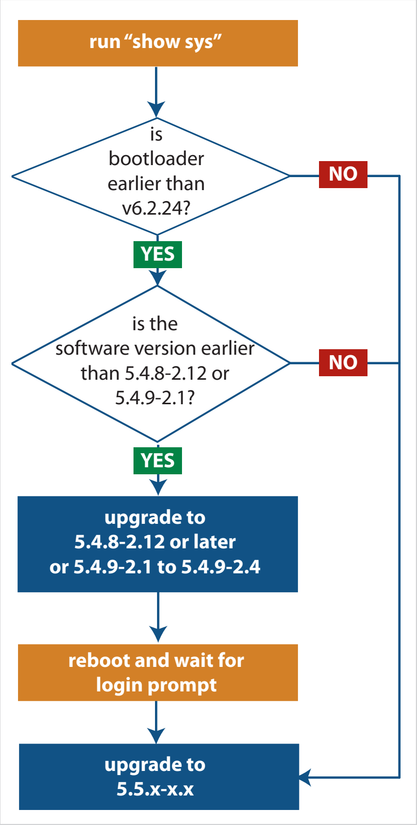
- 5.4.9-1.x
- 5.4.9-0.x
- any version before 5.4.8-2.12.

Instead, before upgrading from one of those versions to 5.5.0-0.1 or later, 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 desired 5.5.x-x.x version.

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


run “show sys”
is bootloader earlier than v6.2.24?
NO
YES
is the software version earlier than 5.4.8-2.12 or 5.4.9-2.1?
NO
YES
upgrade to 5.4.8-2.12 or later or 5.4.9-2.1 to 5.4.9-2.4
reboot and wait for login prompt
upgrade to 5.5.x-x.x

```
awplus# show system
```

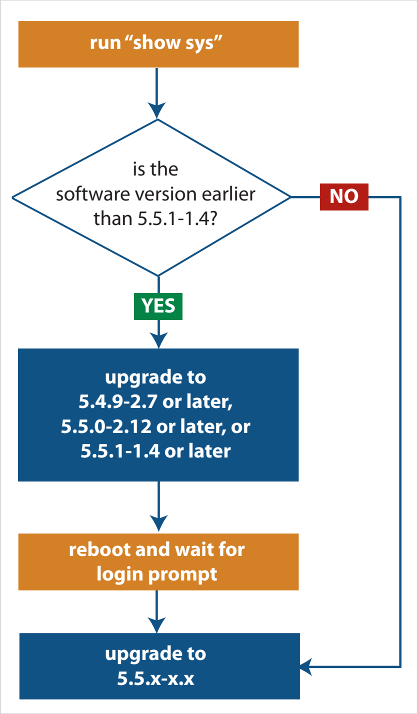
Details for x930 Series

For these switches, **versions 5.5.1-2.1** and later are affected, on switches with all bootloaders. You **cannot** upgrade to versions 5.5.1-2.1 and later 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 5.5.1-2.1 or later, 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.


run "show sys"
is the software version earlier than 5.5.1-1.4?
NO
YES
upgrade to 5.4.9-2.7 or later, 5.5.0-2.12 or later, or 5.5.1-1.4 or later
reboot and wait for login prompt
upgrade to 5.5.x-x.x

If it is not, upgrade to one of these versions before upgrading to version 5.5.1-2.1 or later.

To see your current software 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
switchport access vlan <vid> command no longer accepted in trunk mode	All AlliedWare Plus devices that support VLANs	In 5.5.2-0.x and 5.5.2-1.x, it was possible to use the **switchport access vlan <vid>** command in trunk mode. From 5.5.2-2.1 onwards, this is not possible. To set a native VLAN on a trunk port, use the **switchport trunk native vlan <vid>** command instead.
MRP debugging available in privileged exec mode	All AlliedWare Plus devices that support MRP	From 5.5.2-2.1 onwards, debugging commands for MRP are only available for privilege level 15 users in privileged exec mode. Previously, they were available in exec mode.
Enable or disable TCP port forwarding on the SSH server	All AlliedWare Plus devices that support SSH server	From 5.5.2-1.1 onwards, SSH TCP port forwarding is disabled by default to enhance security. A new command allows you to enable it: `awplus(config)# ssh server tcpforwarding`
AMF Cloud no longer supported on Citrix Hypervisor	AMF Cloud	From 5.5.2-2.1 onwards, Allied Telesis no longer supports the deployment of AMF Cloud on Citrix HyperVisor (which used to be known as Citrix XenServer).
Very old browsers may not be able to access the Device GUI.	All AlliedWare Plus devices	From 5.5.2-2.1 onwards, to improve the security of the communication for the Device GUI, ciphersuites which use RSA or CBC based algorithms have been disabled, as they are no longer considered secure. Note that the removal of ciphersuites using those algorithms may prevent some old versions of browsers from communicating with the device using HTTPS.

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.2 license on your switch if you are upgrading to 5.5.2-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 70 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 72.

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 lefthand 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 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

Product family	Software File	Hash
AMF Cloud	vaa-5.5.2-2.7.rel	b06024601a8a291750e4d3cb402bf9f1153d243e24060a55c38b8bc61b197036
SBx8100	SBx81CFC960-5.5.2-2.7.rel	0086b9b01ba83c96d94a16094579355bf0c29a3958fadc59d7598c46579bd522
SBx908 GEN2	SBx908NG-5.5.2-2.7.rel	17e40cfe96fea00e9fa31deaa01bf56f7f9230012ac7143a6bb0e1720ee7d2fc
x950	x950-5.5.2-2.7.rel	17e40cfe96fea00e9fa31deaa01bf56f7f9230012ac7143a6bb0e1720ee7d2fc
x930	x930-5.5.2-2.7.rel	d919dc8b700f8dc7ed16a29703f001ffc9a67ad57d4bbea54ef51ddcd642d94b
x550	x550-5.5.2-2.7.rel	503f75659a98dd7698b6e9bce6ae36d814b415b5a4b7526c22cb48c747b04af0
x530 & x530L	x530-5.5.2-2.7.rel	ec8be25e1d29b3f806312b594fca93c3b80f98b0e5a7de2151de5bac57da1c5c
x330	x330-5.5.2-2.7.rel	dfa15336681727f54c47a0beb054904311614cb7071ce0c95f302c0ba5264635

Table: Hash values

Product family	Software File	Hash
x320	x320-5.5.2-2.7.rel	ec8be25e1d29b3f806312b594fca93c3b80f98b0e5a7de2151de5bac57da1c5c
x230 & x230L	x230-5.5.2-2.7.rel	cd20ef479aebc3be8d0d6be4afa0eb49f4e043ed88cd495cc1560608b1af5fac
x220	x220-5.5.2-2.7.rel	01247ff247781013ed5456c72317229226e8f1b7ba77738498f6b2628c87619b
IE340 & IE340L	IE340-5.5.2-2.7.rel	d93a30e2c51affa3020872728dc0eebc7090e942237322134aecb08db7b66501
IE210L	IE210-5.5.2-2.7.rel	cd20ef479aebc3be8d0d6be4afa0eb49f4e043ed88cd495cc1560608b1af5fac
XS900MX	XS900-5.5.2-2.7.rel	fce58132b8f03cdade4d439e4ae53581803ad9f9e0abced731c76724e02fa800
GS980MX	GS980MX-5.5.2-2.7.rel	ec8be25e1d29b3f806312b594fca93c3b80f98b0e5a7de2151de5bac57da1c5c
GS980EM	GS980EM-5.5.2-2.7.rel	ec8be25e1d29b3f806312b594fca93c3b80f98b0e5a7de2151de5bac57da1c5c
GS980M	GS980M-5.5.2-2.7.rel	01247ff247781013ed5456c72317229226e8f1b7ba77738498f6b2628c87619b
GS970EMX	GS970EMX-5.5.2-2.7.rel	dfa15336681727f54c47a0beb054904311614cb7071ce0c95f302c0ba5264635
GS970M	GS970-5.5.2-2.7.rel	cd20ef479aebc3be8d0d6be4afa0eb49f4e043ed88cd495cc1560608b1af5fac
AR4050S-5G	AR4050S-5.5.2-2.7.rel	d105fec945b79953d643f73b53699b4b53cb578876e0309d6d113d7ad8e10523
AR4050S	AR4050S-5.5.2-2.7.rel	d105fec945b79953d643f73b53699b4b53cb578876e0309d6d113d7ad8e10523
AR3050S	AR3050S-5.5.2-2.7.rel	d105fec945b79953d643f73b53699b4b53cb578876e0309d6d113d7ad8e10523
AR2050V	AR2050V-5.5.2-2.7.rel	d105fec945b79953d643f73b53699b4b53cb578876e0309d6d113d7ad8e10523
AR2010V	AR2010V-5.5.2-2.7.rel	d105fec945b79953d643f73b53699b4b53cb578876e0309d6d113d7ad8e10523
AR1050V	AR1050V-5.5.2-2.7.rel	3d51f6f484f3013abfde0cac611cb90d6bf0f1a6f3f91b566af6e4f962458cb2

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-2021
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                  : 5.5.2
Customer name                 : ABC Consulting
Quantity of licenses          : 1
Type of license               : Full
License issue date            : 20-Aug-2021
License expiry date           : N/A
Release                       : 5.5.2
```

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-2021
License expiry date           : N/A
Features included             : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                Virtual-MAC, VRRP

Index                         : 2
License name                  : 5.5.2
Customer name                 : ABC Consulting
Quantity of licenses          : -
Type of license               : Full
License issue date            : 20-Aug-2021
License expiry date           : N/A
Release                       : 5.5.2
```

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

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 SBx8100-5.5.2-2.7.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.2-2.7.rel`
x950 series	`awplus(config)# boot system x950-5.5.2-2.7.rel`
x930 series	`awplus(config)# boot system x930-5.5.2-2.7.rel`
x550 series	`awplus(config)# boot system x550-5.5.2-2.7.rel`
x530 series	`awplus(config)# boot system x530-5.5.2-2.7.rel`
x330-10GTX	`awplus(config)# boot system x330-5.5.2-2.7.rel`
x320 series	`awplus(config)# boot system x320-5.5.2-2.7.rel`
x230 series	`awplus(config)# boot system x230-5.5.2-2.7.rel`
x220 series	`awplus(config)# boot system x220-5.5.2-2.7.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.2-2.7.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.2-2.7.rel`

Product	Command
XS900MX series	`awplus(config)# boot system XS900-5.5.2-2.7.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.2-2.7.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.2-2.7.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.2-2.7.rel`
GS970EMX/10	`awplus(config)# boot system GS970EMX-5.5.2-2.7.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.2-2.7.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.2-2.7.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.2-2.7.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.2-2.7.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.5.2-2.7.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.2-2.7.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.2-2.7.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

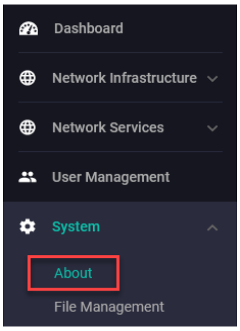
2. Open a web browser and browse to the IP address from step 1.

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 5.5.2-2.7 is **2.14**.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 77 or "Update the GUI on AR-Series devices" on page 78.



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 v5.5.2-2.x is awplus-**gui_552_29**.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. 552) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

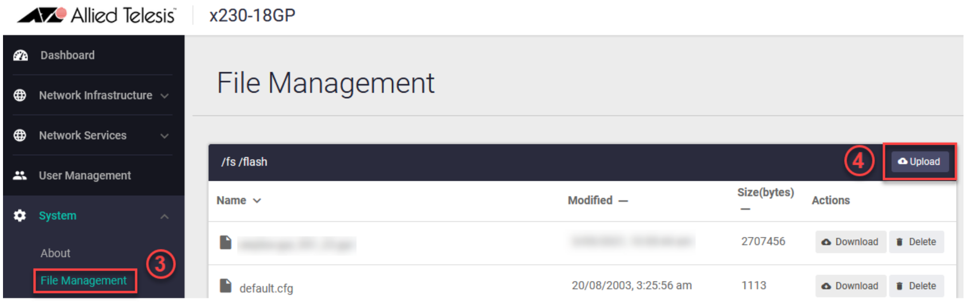
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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**.



Name	Modified	Size(bytes)	Actions
[redacted]	[redacted]	2707456	Download Delete
default.cfg	20/08/2003, 3:25:56 am	1113	Download Delete

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

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

6. Reboot the switch. Or alternatively, use **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.

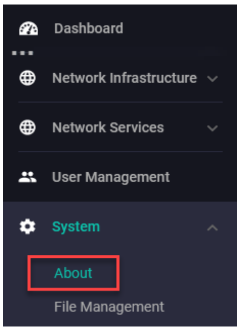
Perform the following steps if you have been running an earlier version of the GUI and need to update it.

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 v2.14.0 or later.


Dashboard
Network Infrastructure
Network Services
User Management
System
About
File Management