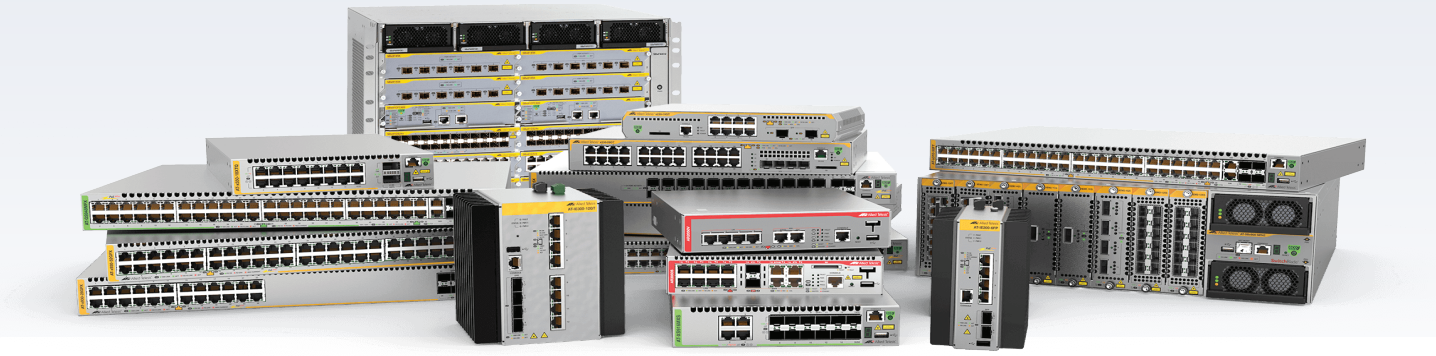
Release Note for AlliedWare Plus Software Version 5.5.1-2.x



AlliedWare Plus OPERATING SYSTEM

AMF Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10GbE UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

» 5.5.1-2.1 » 5.5.1-2.2 » 5.5.1-2.3 » 5.5.1-2.4 » 5.5.1-2.6 » 5.5.1-2.7 » 5.5.1-2.8 » 5.5.1-2.9
» 5.5.1-2.12 » 5.5.1-2.14 » 5.5.1-2.17

Acknowledgments

Getting the most from this Release Note

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

Contents

What's New in Version 5.5.1-2.17

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G GbE UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.17.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. The GUI offers easy visual monitoring and configuration of your device.

New licensing system: Feature String Licenses (FSL)

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

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

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

Please contact your local sales office for more information.

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

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

The following table lists model names and software files for this version:

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		10/2025	vaa-5.5.1-2.17.iso (VAA OS) vaa-5.5.1-2.17. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.17.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2025	SBx81CFC960-5.5.1-2.17.rel
SBx908 GEN2	SBx908 GEN2	10/2025	SBx908NG-5.5.1-2.17.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	10/2025	x950-5.5.1-2.17.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	10/2025	x930-5.5.1-2.17.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2025	x550-5.5.1-2.17.rel

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

Models	Family	Date	Software File
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	10/2025	x530-5.5.1-2.17.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	10/2025	x510-5.5.1-2.17.rel
IX5-28GPX	IX5	10/2025	IX5-5.5.1-2.17.rel
x330-10GTX	x330	10/2025	x330-5.5.1-2.17.rel
x320-10GH x320-11GPT	x320	10/2025	x320-5.5.1-2.17.rel
x310-26FT x310-26FP x310-50FT x310-50FP	x310	10/2025	x310-5.5.1-2.17.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2025	x230-5.5.1-2.17.rel
x220-28GS x220-52GT x220-52GP	x220	10/2025	x220-5.5.1-2.17.rel
IE510-28GSX	IE510-28GSX	10/2025	IE510-5.5.1-2.17.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	10/2025	IE340-5.5.1-2.17.rel
IE300-12GT IE300-12GP	IE300	10/2025	IE300-5.5.1-2.17.rel
IE210L-10GP IE210L-18GP	IE210L	10/2025	IE210-5.5.1-2.17.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	10/2025	IE200-5.5.1-2.17.rel
XS916MXT XS916MXS	XS900MX	10/2025	XS900-5.5.1-2.17.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	10/2025	GS980MX-5.5.1-2.17.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2025	GS980EM-5.5.1-2.17.rel
GS980M/52 GS980M/52PS	GS980M	10/2025	GS980M-5.5.1-2.17.rel
GS970EMX/10	GS970EMX	10/2025	GS970EMX-5.5.1-2.17.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2025	GS970-5.5.1-2.17.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	10/2025	GS900-5.5.1-2.17.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	10/2025	FS980-5.5.1-2.17.rel
10Gbe UTM Firewall		10/2025	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.17.app
AR4050S AR3050S	AR-series UTM firewalls	10/2025	AR4050S-5.5.1-2.17.rel AR3050S-5.5.1-2.17.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	10/2025	AR2050V-5.5.1-2.17.rel AR2010V-5.5.1-2.17.rel AR1050V-5.5.1-2.17.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.17 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.17

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

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall
CR-84412	**CLI**	Previously, under rare circumstances, it was possible for the command prompt to terminate abnormally. This issue has been resolved	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-82923	**EPSR**	Previously, when an EPSR ring transitioned to a 'complete' state after a failure, transit nodes could start receiving traffic on the alternate EPSR port. In some cases, host entries were not correctly updated to reflect the old port, causing traffic to be forwarded through the wrong interface This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-86567	**Port Authentication**	Previously, on affected stacked platforms with port authentication configured, it was possible for switch lockup to occur if many supplicants joined in a short period of time. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-85399	**Port Authentication, VCStack**	Previously, it was possible for an IP connection to cease when a MAC entry aged out for a supplicant connected to a port of a VCStack member. This issue has been resolved.	–	Y	Y	Y	–	–	–	–	–	Y	Y	Y	–	–	Y	–	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall
CR-85793	**Security**	This software update addresses the following vulnerabilities: CVE-2024-12084 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087 CVE-2024-12088 CVE-2024-12747	–	Y	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-86197	**Software Licensing**	The **`license update online`** command has been removed as this functionality is no longer available.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-85760	**SSH**	Previously, if a space was accidentally appended to a legitimate username when logging in via SSH, this could result in the legitimate user being deleted from the user database preventing subsequent logins using the affected username. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-86049	**SSH**	This software update addresses SSH vulnerabilities stated in: CVE-2025-26465.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-84092	**System**	Previously, in rare circumstances, the IE200 Series switch could stop transmitting packets. This issue has been resolved. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-86133	**System**	With this software update, the CPU load and stability for the IE300 series switch has been improved.	–	–	–	–	–	–	–	–	–	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	Y	Y

Enhancements

This section summarizes the enhancements in AlliedWare Plus version 5.5.4-2.17.

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

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

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

ISSU: Effective when CFCs upgraded.

ER-6863 *Applies to all AlliedWare Plus devices*

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

ISSU: Effective when ISSU completed.

What's New in Version 5.5.1-2.14

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G GbE UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.14.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		03/2025	vaa-5.5.1-2.14.iso (VAA OS) vaa-5.5.1-2.14. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.14.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2025	SBx81CFC960-5.5.1-2.14.rel
SBx908 GEN2	SBx908 GEN2	03/2025	SBx908NG-5.5.1-2.14.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	03/2025	x950-5.5.1-2.14.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	03/2025	x930-5.5.1-2.14.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2025	x550-5.5.1-2.14.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2025	x530-5.5.1-2.14.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	03/2025	x510-5.5.1-2.14.rel
IX5-28GPX	IX5	03/2025	IX5-5.5.1-2.14.rel
x330-10GTX	x330	03/2025	x330-5.5.1-2.14.rel
x320-10GH x320-11GPT	x320	03/2025	x320-5.5.1-2.14.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	03/2025	x310-5.5.1-2.14.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2025	x230-5.5.1-2.14.rel
x220-28GS x220-52GT x220-52GP	x220	03/2025	x220-5.5.1-2.14.rel
IE510-28GSX	IE510-28GSX	03/2025	IE510-5.5.1-2.14.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2025	IE340-5.5.1-2.14.rel
IE300-12GT IE300-12GP	IE300	03/2025	IE300-5.5.1-2.14.rel
IE210L-10GP IE210L-18GP	IE210L	03/2025	IE210-5.5.1-2.14.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2025	IE200-5.5.1-2.14.rel
XS916MXT XS916MXS	XS900MX	03/2025	XS900-5.5.1-2.14.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	03/2025	GS980MX-5.5.1-2.14.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2025	GS980EM-5.5.1-2.14.rel
GS980M/52 GS980M/52PS	GS980M	03/2025	GS980M-5.5.1-2.14.rel
GS970EMX/10	GS970EMX	03/2025	GS970EMX-5.5.1-2.14.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2025	GS970-5.5.1-2.14.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2025	GS900-5.5.1-2.14.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	03/2025	FS980-5.5.1-2.14.rel
10Gbe UTM Firewall		03/2025	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.14.app
AR4050S AR3050S	AR-series UTM firewalls	03/2025	AR4050S-5.5.1-2.14.rel AR3050S-5.5.1-2.14.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	03/2025	AR2050V-5.5.1-2.14.rel AR2010V-5.5.1-2.14.rel AR1050V-5.5.1-2.14.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.14 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.14

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

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-84412	**CLI**	Previously, under rare circumstances, it was possible for the command prompt to terminate abnormally. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-82923	**EPSR**	Previously, it was possible for a transit node in an ESPR ring to not forward the traffic correctly after the transit node was shutdown and then brought back up again. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-75199	**PoE**	Previously, under rare circumstances, the PoE ports on the IE200 Series would not be initialized after a reboot. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-85399	**Port Authentication**	Previously, it was possible for an IP connection to cease when a MAC entry aged out for a supplicant connected to a port of a VCStack member. This issue has been resolved.	–	Y	Y	Y	–	–	–	–	–	Y	Y	Y	–	–	Y	–	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-79428	**VRF-Lite**	With this software update, the **show run vrf** output now includes the BGP configuration. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–

What's New in Version 5.5.1-2.12

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G GbE UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.12.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		12/2024	vaa-5.5.1-2.12.iso (VAA OS) vaa-5.5.1-2.12. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.12.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	12/2024	SBx81CFC960-5.5.1-2.12.rel
SBx908 GEN2	SBx908 GEN2	12/2024	SBx908NG-5.5.1-2.12.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	12/2024	x950-5.5.1-2.12.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	12/2024	x930-5.5.1-2.12.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	12/2024	x550-5.5.1-2.12.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	12/2024	x530-5.5.1-2.12.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	12/2024	x510-5.5.1-2.12.rel
IX5-28GPX	IX5	12/2024	IX5-5.5.1-2.12.rel
x330-10GTX	x330	12/2024	x330-5.5.1-2.12.rel
x320-10GH x320-11GPT	x320	12/2024	x320-5.5.1-2.12.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	12/2024	x310-5.5.1-2.12.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	12/2024	x230-5.5.1-2.12.rel
x220-28GS x220-52GT x220-52GP	x220	12/2024	x220-5.5.1-2.12.rel
IE510-28GSX	IE510-28GSX	12/2024	IE510-5.5.1-2.12.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	12/2024	IE340-5.5.1-2.12.rel
IE300-12GT IE300-12GP	IE300	12/2024	IE300-5.5.1-2.12.rel
IE210L-10GP IE210L-18GP	IE210L	12/2024	IE210-5.5.1-2.12.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	12/2024	IE200-5.5.1-2.12.rel
XS916MXT XS916MXS	XS900MX	12/2024	XS900-5.5.1-2.12.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	12/2024	GS980MX-5.5.1-2.12.rel
GS980EM/10H GS980EM/11PT	GS980EM	12/2024	GS980EM-5.5.1-2.12.rel
GS980M/52 GS980M/52PS	GS980M	12/2024	GS980M-5.5.1-2.12.rel
GS970EMX/10	GS970EMX	12/2024	GS970EMX-5.5.1-2.12.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	12/2024	GS970-5.5.1-2.12.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	12/2024	GS900-5.5.1-2.12.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	12/2024	FS980-5.5.1-2.12.rel
10Gbe UTM Firewall		12/2024	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.12.app
AR4050S AR3050S	AR-series UTM firewalls	12/2024	AR4050S-5.5.1-2.12.rel AR3050S-5.5.1-2.12.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	12/2024	AR2050V-5.5.1-2.12.rel AR2010V-5.5.1-2.12.rel AR1050V-5.5.1-2.12.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.12 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.12

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

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-82915	**Aggregation, LACP, Static, Private VLAN**	Previously, QoS (ACLs, Policy-maps), VLAN classifiers, VLAN translation, and UFO features and protocols, could sometimes have an incorrect interaction between particular trunk and port configurations. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–
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	Y	–	–	–	–	Y	–	–
CR-80477	**AMF**	Previously, it was possible for a provisioned AMF node to include a copy of a UUID, if the 'copy' or 'clone' commands were used during the provisioning process. This could result in problems identifying the device after recovery when Vista Manager EX was in use. 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-82753	**AMF**	Previously, when attempting to use an AMF backup command on a router that did not support backups, the error message provided suggested that the problem was incorrect configuration. The error message has been changed so that it is clear the hardware platform does not support AMF backup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-64010	**AMF**	Previously, there was an issue with how numerical data (specifically the length of the DBE, or Data Block Element) was encoded and transmitted over the network. The issue could generate periodic error logs. 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	–	–	–	–	–	–	–	–	–	–	–
CR-63789	**AMF, Application Proxy Whitelist**	Previously, RADIUS proxy information was expiring after 60 minutes, which was causing proxy settings to be deleted and breaking whitelist functionality. This issue has now been resolved and Application Proxy Whitelist NASs now retain the RADIUS proxy information indefinitely.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	Y	–	–
CR-79757	**API, IPv6**	Previously, configurations involving softwire (MAP-E or LW4o6) may have occasionally experienced benign core-file generation related to a process called 'lua'. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-77632	**ARP / Neighbor Discovery, EPSR, MAC Thrashing, VCStack**	Previously, it was possible for EPSR blocking to be defeated for ARP packets (request and reply) ingressing a port on a VCStack if the ingress port was on the backup member. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-79525	**ARP Neighbor Discovery**	Previously, ARP learning could cause 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	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-80964	**AWC-lite**	Previously, there was no validation for WEP security, making it difficult for users to determine whether the WEP configuration was invalid. This issue has been resolved. The following validations for security WEP have been added: ■ Check if WEP is assigned to radio with "b/g" mode (for 2.4GHz) or "a" mode (for 5GHz) ■ Check if WEP is assigned to VAP0 network.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–
CR-81462	**AWC-lite**	Previously, TQ APs with the new MAC OUI (00:C2:8F) were not recognised by AWC-Lite. This prevented devices with this MAC OUI from being detected by the easy setup auto config feature. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-81247	**CLI**	Previously, after enabling 802.1q encapsulation on an Ethernet/tunnel/bridge/WAN interface, the default MTU of this newly created sub-interface was displayed in the running-config. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	Y	Y	–
CR-81342	**CLI**	Previously, If multiple commands were entered rapidly (e.g. using a script) into the command line interface, it was possible for the mode of the CLI session to change to EXEC mode unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	Y	Y	Y	Y	Y	–	Y	–	Y	Y	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-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	Y	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-79324	**DHCP Snooping, Private VLAN**	Previously, when DHCP-snooping was in use in conjunction with private VLANs, DHCP responses arriving on a promiscuous port would not be received by a DHCP client attached via an isolated private VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	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	Y	Y	Y	Y	Y	Y	Y	Y
CR-83420	**EPSR**	Previously, on a port under EPSR (Ethernet Protection Switching Ring) control, FDB entries were not removed when they should have been. This issue has been resolved.	–	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-82923	**EPSR**	Previously, when an EPSR ring transitioned to a 'complete' state after a failure, transit nodes could start receiving traffic on the alternate EPSR port. In some cases, host entries were not correctly updated to reflect the old port, causing traffic to be forwarded through the wrong interface This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–	–
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	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
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	–	–
CR-81787	**Firewall**	Previously, if a firewall rule was added to permit ICMP packets generated by the router (e.g., TTL exceeded) in response to received packets, the ICMP packet would not be sent even though the rule was correctly matched. This issue specifically occurred with user-defined applications where the protocol was specified as 'ICMP'. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-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	Y	Y	Y	Y	Y	Y	Y	Y
CR-82514	**IGMP**	Previously, if a dynamically learned IGMP group record changed to a static group record, multicast traffic for that group might not be forwarded correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-79751	**IPv6, VRF-lite**	Previously, in certain situations, router-advertisements from connected routers could be lost following IPv6 being re-enabled (i.e. disabled then enabled). This was due to the "RA-received" flag not being reset correctly when DAD was initiated on an interface. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-79697	**IPv6 CLI**	Previously, the command **`no ipv6 forwarding`** did not stop the device from routing IPv6 traffic. 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-62976	**Logging**	Previously, in rare circumstances, the syslog-ng process could fail due to a timing issue. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y
CR-58712	**Logging**	Previously, the syslog-ng process could fail if the console or TTY connection timed out while the terminal monitor was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–
CR-81577	**Memory Management**	Previously, on virtual firewall and AMF containers, debug-low-memory files weren't being generated when crossing the critical low memory threshold. This issue has been resolved. Now, if free memory becomes very low a debug-low-memory file will be generated, and if free memory is below the critical level, the container will reboot automatically.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-77098	**Multicast**	Previously, a memory leak could occur if a switch received packet fragments from unregistered multicast streams and was configured with the command: **`ip multicast allow-register-fragments`**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-81797	**Pluggable Transceivers**	Previously, the **`limited-reach-mode`** command could fail to be executed on the x550 platform. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-78924	**PoE, LLDP**	Previously, on platforms that support PoE: If LLDP was enabled and the Power Via MDI TLV included **`lldp tlv-select all`** or **`lldp tlv-select power-management`**, then in rare cases the PSE allocated power value in the LLDP packet transmitted was not calculated from the PD requested power value included in the same packet, and sometimes the PSE allocated power field contained an old value. This functionality was not conforming to the IEEE 802.3 specification (specifically, "33.6.2 Data Link Layer classification timing requirements"). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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-80881	**Port Configuration**	Previously, specifying an invalid port range in global configuration mode with the command **`interface portx.x.x-y.y.y`** could result in an unexpected system reboot.This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	Y	Y	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	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-80698	**PPP**	Previously, if a remote PPP server required CHAP authentication but the final 'outcome' message from the server was lost, the PPP connection could hang. It wouldn't fail and wouldn't fully establish This issue has been resolved. Now, if the 'outcome' message is not received after 60 seconds, the PPP will behave as though the outcome was 'Failure'. The PPP will be brought down and restarted.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-82259	**QoS**	Previously, it was possible for the software to attempt to execute a QSP (QoS Storm Protection) action on a port that was link down, resulting in an error log. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
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	Y	Y	Y	Y	Y	Y	Y	Y
CR-78845	**Security, SSL**	This software update upgrades OpenSSL to 1.1.1u to address the security vulnerabilities specified in: CVE-2023-0286, CVE-2023-0215, CVE-2022-4450 and CVE-2022-4304.	Y	Y	Y	Y	Y	Y	Y	Y	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	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-78955	**SNMP**	Previously, in SNMP traps for MAC thrashing, the VLAN ID was set to 0. This is now resolved and the VLAN ID is set to the VLAN the thrashing was detected on. 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-80830	**SNMP**	Previously, if SNMP service was disabled using the command **`no snmp-server`** and then re-enabled 10 minutes or longer later with the command **`snmp-server`**, some MIB objects in System Group (MIB-2, 1), such as System Contact, System Name, etc, would become unavailable. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-83343	**SNMP**	Previously, SNMP walk on pluggable diagnostic tables did not show all pluggable interfaces. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	Y	–	–	–	Y	–	Y	–	–	–	–	–	–	–
CR-81948	**SSH**	This software update addresses the SSH vulnerabilities specified in CVE-2023-48795.	Y	Y	Y	Y	Y	Y	Y	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-77128	**SW Bridging**	Previously, the user configured MTU value for tunnel dot1q sub interfaces could sometimes change to a lower value, causing packets to be dropped. This issue has been resolved, and the user configured value will always be respected.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-79290	**Syslog, Bootup**	Previously, there was an internal issue with syslog, resulting in slow initialisation. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-77080	**System**	This software update addresses the Linux kernel vulnerabilities specified in the following: CVE-2022-22576, CVE-2022-27774, CVE-2022-27776, CVE-2022-27782, CVE-2022-27781, CVE-2022-27775, CVE-2022-27780, CVE-2022-27779, CVE-2022-30115. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-77100	**System**	This software update addresses the Linux kernel vulnerability specified in CVE-2022-32250. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-77469	**System**	This software update addresses a file system vulnerability as specified in CVE-2019-5188. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-78367	**System**	Although the DoS vulnerability was not observed on AlliedWare Plus, a patch for CVE-2022-3435 has been implemented upstream as a precautionary measure. This patch effectively addresses the potential vulnerability. 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	–	–
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	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	–	–
CR-76097	**System**	This software update addresses a memory vulnerability as specified in CVE-2022-23218 and CVE-2022-23219. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y
CR-76586	**System**	This software update addresses a memory vulnerability as specified in CVE-2022-23308. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-76739	**System**	This software update addresses a memory vulnerability as specified in CVE-2018-25032. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y
CR-77156	**System**	This software update addresses a file system vulnerability as specified in CVE-2022-1998. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y
CR-78181	**System**	This software update addresses a file system vulnerability as specified in CVE-2022-36946. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y
CR-78788	**System**	This software update addresses the HTTP vulnerabilities stated in CVE-2022-43551	Y	Y	Y	Y	Y	Y	Y	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-81148	**System**	This software update addresses the HTTP vulnerabilities stated in CVE-2023-38039. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-83869	**System**	Previously, an unexpected system reboot could occur on the IE510 if fan speed, temperature, or voltage measurements exceeded their bounds. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-81012	**Triggers**	Previously, it was possible for Log Triggers to get into a state where further activations of the trigger would not occur. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79359	**Tunneling**	Previously, when the MTU for a dot1q interface was left unset, the automatically calculated value was incorrect and often far lower than the MTU of the parent tunnel interface. This issue has now been resolved and the dot1q interface MTU will always be 4 bytes less than the parent tunnel MTU, to account for the encapsulation header size. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
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	Y	Y	–	–	–	–	–	–	–
CR-80241	**VCStack**	Previously, a polling request from Vista Manager EX 3.10 or later could cause a system reboot on a VCStack master if the polling request arrived immediately after a VCStack failover, while the old master was in the process of rejoining the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–
CR-80760	**VCStack**	Previously, when SBx8100 line cards were rebooted via the **`reboot card`** command, in rare cases a VCStack Plus separation could occur. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-81609	**VCStack**	Previously, when VCStack traps were enabled, a VCStack would send a VCS resiliency link trap if the link status changed from shutdown to up, or from up to shutdown. This behaviour is now changed. A resiliency link trap can be generated only if both VCStack traps and VCStack resiliency link traps are enabled. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–	–
CR-83354	**VCStack**	Previously, some multicast streams could fail to recover after a stack master failover. This issue has been resolved.	Y	–	Y	Y	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
CR-80751	**VCStacking**	Previously, it was possible for the IE510 to become stuck in the INIT state after rejoining the stack. This could occur if pluggable ports were not initialised due to spurious interrupts. This issue has now been resolved by preventing the spurious interrupts so pluggable ports are correctly initialized on boot up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-81610	**Web API**	Previously, when an API Json response for the non-version API was an exact multiple of 4096 bytes, some additional characters could be returned at the end of the response. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	–	Y	Y	–	Y	–	–	–	–	Y	–	Y	Y	–	Y	Y	Y	–	–	Y	–	–	–	–	–	–	–	–

What's New in Version 5.5.1-2.9

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G GbE UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.9.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		06/2023	vaa-5.5.1-2.9.iso (VAA OS) vaa-5.5.1-2.9. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.9.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	06/2023	SBx81CFC960-5.5.1-2.9.rel
SBx908 GEN2	SBx908 GEN2	06/2023	SBx908NG-5.5.1-2.9.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	06/2023	x950-5.5.1-2.9.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	06/2023	x930-5.5.1-2.9.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2023	x550-5.5.1-2.9.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	06/2023	x530-5.5.1-2.9.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	06/2023	x510-5.5.1-2.9.rel
IX5-28GPX	IX5	06/2023	IX5-5.5.1-2.9.rel
x330-10GTX	x330	06/2023	x330-5.5.1-2.9.rel
x320-10GH x320-11GPT	x320	06/2023	x320-5.5.1-2.9.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	06/2023	x310-5.5.1-2.9.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	06/2023	x230-5.5.1-2.9.rel
x220-28GS x220-52GT x220-52GP	x220	06/2023	x220-5.5.1-2.9.rel
IE510-28GSX	IE510-28GSX	06/2023	IE510-5.5.1-2.9.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	06/2023	IE340-5.5.1-2.9.rel
IE300-12GT IE300-12GP	IE300	06/2023	IE300-5.5.1-2.9.rel
IE210L-10GP IE210L-18GP	IE210L	06/2023	IE210-5.5.1-2.9.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2023	IE200-5.5.1-2.9.rel
XS916MXT XS916MXS	XS900MX	06/2023	XS900-5.5.1-2.9.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	06/2023	GS980MX-5.5.1-2.9.rel
GS980EM/10H GS980EM/11PT	GS980EM	06/2023	GS980EM-5.5.1-2.9.rel
GS980M/52 GS980M/52PS	GS980M	06/2023	GS980M-5.5.1-2.9.rel
GS970EMX/10	GS970EMX	06/2023	GS970EMX-5.5.1-2.9.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2023	GS970-5.5.1-2.9.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2023	GS900-5.5.1-2.9.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	06/2023	FS980-5.5.1-2.9.rel
10Gbe UTM Firewall		06/2023	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.9.app
AR4050S AR3050S	AR-series UTM firewalls	06/2023	AR4050S-5.5.1-2.9.rel AR3050S-5.5.1-2.9.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	06/2023	AR2050V-5.5.1-2.9.rel AR2010V-5.5.1-2.9.rel AR1050V-5.5.1-2.9.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.9 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.9

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S	10GbE UTM Firewall	AMF Cloud
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	–	–
CR-72577	**Pluggable Tranceivers**	Previously, under some circumstancwes, 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-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	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–

Enhancements

The following enhancement is available with this software update:

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	10GbE UTM Firewall	AMF Cloud
ER-5359	**Environmental Monitoring**	With this software update, support for Delta system fans has been added to the x530L-10GHXm and GS980MX/10HSm devices.	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–

What's New in Version 5.5.1-2.8

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G GbE UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.8.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		06/2023	vaa-5.5.1-2.8.iso (VAA OS) vaa-5.5.1-2.8. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.8.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	06/2023	SBx81CFC960-5.5.1-2.8.rel
SBx908 GEN2	SBx908 GEN2	06/2023	SBx908NG-5.5.1-2.8.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	06/2023	x950-5.5.1-2.8.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	06/2023	x930-5.5.1-2.8.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2023	x550-5.5.1-2.8.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	06/2023	x530-5.5.1-2.8.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	06/2023	x510-5.5.1-2.8.rel
IX5-28GPX	IX5	06/2023	IX5-5.5.1-2.8.rel
x330-10GTX	x330	06/2023	x330-5.5.1-2.8.rel
x320-10GH x320-11GPT	x320	06/2023	x320-5.5.1-2.8.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	06/2023	x310-5.5.1-2.8.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	06/2023	x230-5.5.1-2.8.rel
x220-28GS x220-52GT x220-52GP	x220	06/2023	x220-5.5.1-2.8.rel
IE510-28GSX	IE510-28GSX	06/2023	IE510-5.5.1-2.8.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	06/2023	IE340-5.5.1-2.8.rel
IE300-12GT IE300-12GP	IE300	06/2023	IE300-5.5.1-2.8.rel
IE210L-10GP IE210L-18GP	IE210L	06/2023	IE210-5.5.1-2.8.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2023	IE200-5.5.1-2.8.rel
XS916MXT XS916MXS	XS900MX	06/2023	XS900-5.5.1-2.8.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	06/2023	GS980MX-5.5.1-2.8.rel
GS980EM/10H GS980EM/11PT	GS980EM	06/2023	GS980EM-5.5.1-2.8.rel
GS980M/52 GS980M/52PS	GS980M	06/2023	GS980M-5.5.1-2.8.rel
GS970EMX/10	GS970EMX	06/2023	GS970EMX-5.5.1-2.8.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2023	GS970-5.5.1-2.8.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2023	GS900-5.5.1-2.8.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	06/2023	FS980-5.5.1-2.8.rel
10Gbe UTM Firewall		06/2023	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.8.app
AR4050S AR3050S	AR-series UTM firewalls	06/2023	AR4050S-5.5.1-2.8.rel AR3050S-5.5.1-2.8.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	06/2023	AR2050V-5.5.1-2.8.rel AR2010V-5.5.1-2.8.rel AR1050V-5.5.1-2.8.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.8 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.8

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

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76217	**ACL**	Previously, 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-78869	**ACL**	Previously, when editing an ACL attached to a VLAN access-map after it has 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-75284	**ACL**	Previously, on x230 and GS970M Series, when ACL lists were over subscribed, no error was 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	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-78746	**AMF**	Previously, a non-existant 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	Y	Y	Y	Y	Y	Y	–
CR-79119	**AMF**	Previously, under certain unusual circumstances, TQ guestnodes 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	Y	Y	Y	Y	Y	Y	Y	–
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. 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-77424	**DHCP Server VRF-lite**	Previously, the **`show ip dhcp binding vrf`** <*`vrf-name`*> command output would show the global VRF static entries in addition to dynamic entries for the specified VRF. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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	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-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	–	Y	Y	Y	–	Y	–	–	–	–	–
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	Y	Y	Y
CR-78748	**MAC Authentication**	Previously, executing the **`clear mac address-table`** command didn't 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	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-77445	**Multicast Routing**	Previously, if **`ipv6 mld snooping`** was disabled, IPv6 multicast routing may not have recovered after a network outage. 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-79250	**NLB**	Previously, the NLB unicast packets were not being transferred. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	–	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-79179	**Pluggable Transceivers**	Previously, on the IE510 Series, removal and insertion of SFPs would not be shown in the log and might not have worked correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	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	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-77790	**Policy-based-routing, DPI**	Previously, some PBR rules with DPI applications would not work if the DPI provider was Procera. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-76402	**Port Authentication, VCStack**	Previously, the authd task on each stack member could terminate after a stack failover when an interface had the following configuration: `auth-mac enable` `auth host-mode multi-host` `auth dynamic-vlan-creation` `auth multi-vlan-session` This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	–	Y	–	–	–	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-77529	**Port Authentication**	Previously, there was a possibility that stale IP information for a MAC authenticated supplicant could cause an authenticating web-auth supplicant to incorrectly report authentication completion before it had actually finished. 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	–
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-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-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	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-77587	**QoS**	Previously, the egress-rate-limiting may not have been applied correctly to provisioned ports. 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-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	–
CR-78189	**Security**	This software update addresses security vulnerability issues as specified in: CVE-2022-37434. 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-78382	**SNMP Security**	This software update addresses security vulnerability issues as specified in: CVE-2022-44792 and CVE-2022-44793 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-77793	**SSH**	Previously, the inability to save known SSH hosts properly, meant you needed to type in "yes" to accept connections to hosts that had been previously 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	Y	Y	Y	Y
CR-79386	**SSH**	With this software upgrade, OpenSSH has been upgraded. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-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-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	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	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-76141	**VCStack**	Previously, on a stack device, if the audit inconsistency log appeared, it could continue to output every minute. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	–	Y	–	–	–	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-77971	**VCStack**	Previously, on x930 Series switches, the setting for egress rate limits on different queues could change after a port had been brought up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-78570	**VCStack**	Previously, if a stack was under heavy CPU load, there was a small chance that a rejoining stack member would 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	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 timeouts and resiliency link healthcheck failures. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–

Enhancements

The following enhancement is available with this software update:

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	AMF Cloud
ER-5399	**Port Authentication**	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. 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.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

What's New in Version 5.5.1-2.7

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G GbE UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.7.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		05/2023	vaa-5.5.1-2.7.iso (VAA OS) vaa-5.5.1-2.7. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.7.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	05/2023	SBx81CFC960-5.5.1-2.7.rel
SBx908 GEN2	SBx908 GEN2	05/2023	SBx908NG-5.5.1-2.7.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	05/2023	x950-5.5.1-2.7.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	05/2023	x930-5.5.1-2.7.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2023	x550-5.5.1-2.7.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	05/2023	x530-5.5.1-2.7.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	05/2023	x510-5.5.1-2.7.rel
IX5-28GPX	IX5	05/2023	IX5-5.5.1-2.7.rel
x330-10GTX	x330	05/2023	x330-5.5.1-2.7.rel
x320-10GH x320-11GPT	x320	05/2023	x320-5.5.1-2.7.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	05/2023	x310-5.5.1-2.7.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2023	x230-5.5.1-2.7.rel
x220-28GS x220-52GT x220-52GP	x220	05/2023	x220-5.5.1-2.7.rel
IE510-28GSX	IE510-28GSX	05/2023	IE510-5.5.1-2.7.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	05/2023	IE340-5.5.1-2.7.rel
IE300-12GT IE300-12GP	IE300	05/2023	IE300-5.5.1-2.7.rel
IE210L-10GP IE210L-18GP	IE210L	05/2023	IE210-5.5.1-2.7.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	05/2023	IE200-5.5.1-2.7.rel
XS916MXT XS916MXS	XS900MX	05/2023	XS900-5.5.1-2.7.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	05/2023	GS980MX-5.5.1-2.7.rel
GS980EM/10H GS980EM/11PT	GS980EM	05/2023	GS980EM-5.5.1-2.7.rel
GS980M/52 GS980M/52PS	GS980M	05/2023	GS980M-5.5.1-2.7.rel
GS970EMX/10	GS970EMX	05/2023	GS970EMX-5.5.1-2.7.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2023	GS970-5.5.1-2.7.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	05/2023	GS900-5.5.1-2.7.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	05/2023	FS980-5.5.1-2.7.rel
10Gbe UTM Firewall		05/2023	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.7.app
AR4050S AR3050S	AR-series UTM firewalls	05/2023	AR4050S-5.5.1-2.7.rel AR3050S-5.5.1-2.7.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	05/2023	AR2050V-5.5.1-2.7.rel AR2010V-5.5.1-2.7.rel AR1050V-5.5.1-2.7.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.7 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.7

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

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-77839	**ACL**	Previously, ACLs could be installed incorrectly at startup in some cases leading to unexpected behaviour. This issue has been resolved. ISSU: Effective when ISSU complete.	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	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	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	Y	Y	Y	Y
CR-77489	**ARP, Neighbor Discovery, VCStack**	Previously, in specific VCStack configurations utilizing static aggregators and VCStack resiliency links, ARP entries might not get flushed correctly when a VCStack master failover occured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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	–
CR-77837	**DHCP Server**	This software update addresses the DHCP server vulnerability issues as stated in CVE-2022-2928 and CVE-2022-2929. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	Y	–	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-78239	**DHCP Snooping**	Previously, DHCP Snooping per VLAN command was not enabled on x510 series. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-77783	**IGMP**	Previously, multicast routes were not correctly removed from the hardware table upon reception of an IGMP or MLD group leave message. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	Y	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-77844	**MAC Thrashing**	Previously, when MAC thrash action was set to "port disable", the port would not show that MAC thrashing had been detected in the output of the **`show interface`** command. This issue has been resolved.	–	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-77685	**PoE**	Previously, the IE300-12GP variant was not able to supply full power to PoE class 4 devices. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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	–
CR-77463	**PSU**	Previously, errors were generated at startup or when a PSU was powered up on an IE510. These errors could be safely ignored, but the source of these errors has now been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-74574	**QoS hardware**	Previously, the commands **`remark-map to new-dscp <num>`** and **`remark-map to new-bandwidth-class <class>`** could silently 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	–
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-77485	**RADIUS VCStack**	Previously, it was possible the local RADIUS server failed to run on the new stack master after failover. 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	–	–	–	–	–
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	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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 Solar-winds, 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	–
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	–
CR-77416	**SSH, TACACS+**	Previously, TACACS+ user login via SSH was only successful at every second attempt. The first login attempt would 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	–
CR-78392	**Static Aggregation, QoS HW, VCStack**	Previously, using the **`static-channel-group member-filters`** command on a switchport could fail during VCStack bootup if there was a service-policy configured on the same switchport. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	–	Y	Y	–	–	–	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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-78066	**VCStack, VRRP**	Previously, VRRP advertisement packets could occasionally be dropped as a result of a buffer overflow. This triggered the VRRP transition message to be logged. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–

What's New in Version 5.5.1-2.6

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G Virtual UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.6.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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-5.5.1-2.6.iso (VAA OS) vaa-5.5.1-2.6. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.6.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2022	SBx81CFC960-5.5.1-2.6.rel
SBx908 GEN2	SBx908 GEN2	11/2022	SBx908NG-5.5.1-2.6.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	11/2022	x950-5.5.1-2.6.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	11/2022	x930-5.5.1-2.6.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2022	x550-5.5.1-2.6.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	11/2022	x530-5.5.1-2.6.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	11/2022	x510-5.5.1-2.6.rel
IX5-28GPX	IX5	11/2022	IX5-5.5.1-2.6.rel
x330-10GTX	x330	11/2022	x330-5.5.1-2.6.rel
x320-10GH x320-11GPT	x320	11/2022	x320-5.5.1-2.6.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	11/2022	x310-5.5.1-2.6.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2022	x230-5.5.1-2.6.rel
x220-28GS x220-52GT x220-52GP	x220	11/2022	x220-5.5.1-2.6.rel
IE510-28GSX	IE510-28GSX	11/2022	IE510-5.5.1-2.6.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	11/2022	IE340-5.5.1-2.6.rel
IE300-12GT IE300-12GP	IE300	11/2022	IE300-5.5.1-2.6.rel
IE210L-10GP IE210L-18GP	IE210L	11/2022	IE210-5.5.1-2.6.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2022	IE200-5.5.1-2.6.rel
XS916MXT XS916MXS	XS900MX	11/2022	XS900-5.5.1-2.6.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	11/2022	GS980MX-5.5.1-2.6.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2022	GS980EM-5.5.1-2.6.rel
GS980M/52 GS980M/52PS	GS980M	11/2022	GS980M-5.5.1-2.6.rel
GS970EMX/10	GS970EMX	11/2022	GS970EMX-5.5.1-2.6.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2022	GS970-5.5.1-2.6.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2022	GS900-5.5.1-2.6.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	11/2022	FS980-5.5.1-2.6.rel
10G Virtual UTM Firewall		11/2022	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.6.app
AR4050S AR3050S	AR-series UTM firewalls	11/2022	AR4050S-5.5.1-2.6.rel AR3050S-5.5.1-2.6.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	11/2022	AR2050V-5.5.1-2.6.rel AR2010V-5.5.1-2.6.rel AR1050V-5.5.1-2.6.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.6 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.6

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76022	**5G Modem**	Previously, when running the **`platform 5g update firmware`** command, some error logs were generated due to the 5G modem being reset. The severity of these messages have now been reduced as the logged behaviour is expected during a reset of the 5G modem. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-76880	**5G Modem**	Previously, if the 5G modem was busy, the temperature reading could fail resulting in a "0" value. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-76949	**5G Modem**	Previously, SIM failover detection would try to attach the network and swap carriers even though the radio was disabled by shutting down the wwan0 interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-76595	**5G Modem**	Previously, deleting a modem's firmware could sometimes cause the modem to stop responding. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-76690	**5G Modem**	Previously, on rare occacions, the 5G modem would not operate correctly on startup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-76820	**ACL, API**	Previously, ACL API could return incorrect information with IPv6 host groups. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-77444	**AMF**	Previously, on very rare occasions, when the AMF application proxy is placed under extreme load, it is 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	Y	Y	Y	Y	Y	Y	Y	Y
CR-77077	**AMF**	Previously, the traffic for a node reachable via an AMF virtual link would not be passed through the virtual link as intended. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77518	**API**	Previously, if you opened a web-shell session from the device GUI and then logged out of the device GUI, the browser would request basic authentication credentials for the shell. If these were entered, the browser would cache the basic authentication credentials and send them with all future HTTPS requests to the device while the browser remained open, even if this was not necessary (due to form authentication for the GUI). This issue has been resolved. The web-shell no longer sets the header that induces the browser to request basic authentication credentials after the device GUI is logged out. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-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	Y	–	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76761	**AWC Lite**	Previously, the Passpoint security could not be used when 3gpp-info was not set. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-76988	**AWC Lite**	Previously, when deleting an AP-profile that was using a channel blanket, the BSSID information that was being used would not be removed. This issue has been resolved	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-76951	**Boot**	Previously, on x330 Series, occassionally, external media would not be detected and autoboot configuration would be missed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-73756	**Environmental Monitoring**	Previously, on the x530 Series, it was possible for some temperature sensors to get hot enough to trigger temperature alarms without the fan RPM increasing. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-77533	**Environmental Monitoring**	Previously, it was possible for an IE340 device to encounter an exception error at startup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-77630	**FindMe**	Previously, with **`findme trigger`** configured (or using findme as a CLI command), under some circumstances it was possible for the device to unexpectedly reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77502	**Firewall, GUI**	Previously, statistics monitoring was not operating correctly for the firewall history. This issue is now resolved and the firewall history is correctly monitored.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-77493	**HTTP Service**	With this software update, HTTPS access to Alliedware Plus devices has been enhanced to use only strong ciphersuites. The ciphersuites supported from this release and onward are: ■ ECDHE-ECDSA-AES128-GCM-SHA256 ■ ECDHE-RSA-AES128-GCM-SHA256 ■ ECDHE-ECDSA-AES256-GCM-SHA384 ■ ECDHE-RSA-AES256-GCM-SHA384 ■ DHE-RSA-AES128-GCM-SHA256 ■ DHE-RSA-AES256-GCM-SHA384 I ISSU: Effective when CFCs upgraded.	–	Y	–	Y	Y	–	–	–	Y	–	–	Y	Y	–	–	–	Y	Y	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	–
CR-77680	**IPv4**	Previously, when IP directed-broadcast was enabled on an interface, Layer 3 broadcast packets were duplicated to the local network. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76910	**LACP, SNMP**	Previously, a storm could occur when using multiple stack resiliency links that formed a loop. This was observed when **no ip igmp snooping** was configured. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-77845	**LLDP**	Previously, packets that were not LLDP and were sent to multicast addresses: 01:80:c2:00:00:0e, 01:80:c2:00:00:03, 01:80:c2:00:00:00 , would cause the following log message: '*Unrecognised ethernet type*'. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76808	**Loop Protection**	Previously, when the **clear loop-protection counters** command was used, the VLAN information could be incorrectly cleared. 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-77076	**Loop Protection, VCStack**	Previously, if a stack member joined the stack as a late-joiner, the member's loop-protection configuration would not be present in the running-config. 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	–	–	–	–	–
CR-76751	**MRP**	Previously, a sequence of link down, link up events could result in both MRP ring ports being left in a blocking state. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–
CR-77620	**OSPF**	Previously, on rarely occassions in large OSPF networks, when the SPF calculation was performed periodically, it could cause a device to restart. 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-76775	**OSPFv2**	Previously, it was not possible to configure the maximum number of ECMP routes. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76984	**OSPFv2**	Previously, syncing OSPF Database Description packets could write values to unknown parts of memory. This could have potentially caused some random OSPF issues. 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-75846	**Pluggable Transceivers**	Previously, on the, x550, x950 series and SBx908 Gen2, on rare occasions, entering the **show platform port** command could cause a 10G copper port to go down then back up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	–	–	–	–	–
CR-76101	**PoE**	Previously, a PD could request more power than was allowed for its class. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	Y	Y	–	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-77423	**Port Authentication**	Previously, sometimes with MAC-based Port Authentication, a supplicant could become unauthenticated immediately after being authenticated. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77463	**PSU**	Previously, errors were generated at startup or when a PSU was powered up on an IE510. These errors could be safely ignored, but the source of these errors has now been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-75781	**QoS**	Previously, the command **`set dscp`** entered within a QoS class-map was accepted but not added to the running-configuration. This meant that if the configuration was saved this command would not be preserved over a reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	–	–	–	–	Y	Y	–	–	–	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-77500	**QoS**	Previously, disabling MLS QoS might cause a line card on a SBx8100 to reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	Y	Y	–	–	–	–	–	Y	Y	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-77339	**RIP**	Previously, when a 'port-up' occurs with **`ip summary-address rip`** configured, the ripd process 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	–
CR-76134	**Secure Logging**	Previously, using the **`log host A.B.C.D secure`** configuration command could cause a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-76909	**sFlow**	Previously, sFlow sampled packets could be incorrectly forwarded. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76063	**SSL**	This software update addresses the SSL security vulnerabilities specified in CVE-2022- 1292 and CVE-2021-4160. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77504	**SSL**	This software update addresses an SSL vulnerability as specified in CVE-2021-3712. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77534	**SSL**	This software update addresses an SSL vulnerability as specified in CVE-2022-2068. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75908	**Static Aggregation** **VCStack**	Previously, deleting a static aggregator could cause a stack break. This issue has been resolved.	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-76178	**STP** **Static Agregators**	Previously, using static aggregators on a stack with spanning tree could result in ports being blocked at startup. This issue has been resolved.	–	–	Y	Y	–	–	–	–	–	–	–	Y	–	Y	Y	–	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-76905	**Switching**	Previously, an SP10Ta or SP10TM module that experienced fast retrains of a 10G link could see a 'link down - link up' event. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	–	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR-76591	**System**	This software update addresses security vulnerability issues as specified in CVE-2020 36516. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76779	**System**	This software update addresses security vulnerability issues as specified in: CVE-2022-1055. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76816	**System**	This software update addresses security vulnerability issues as specified in: CVE-2022-28391. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76819	**System**	Previously, memory exhaustion could occur when processing some packets. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-76907	**System**	This software update addresses the linux kernel vulnerability specified in: CVE-2022-1353. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76929	**System**	This software update addresses the Linux kernel vulnerability specified in: CVE-2022-0847. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77010	**System**	This software update addresses the linux kernel vulnerability specified in: CVE-2022-30594. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77012	**System**	This software update addresses the linux kernel vulnerability specified in: CVE-2022-29581. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77084	**System**	This software update addresses a file system vulnerability as specified in: CVE-2022-1348. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-77450	**TACACS+**	Previously, if a TACACS+ key contained the character hash '#', the communication between the AlliedWare Plus device and the TACACS+ server could fail. This issue has been resolved by not allowing '#' in a TACACS+ key. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-77262	**USB Modem**	Previously, re-initialising the 5G modem WWAN interface would not remove the former DNS and route information. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-75835	**VCStack**	Previously, it was possible for packet corruption to occur on the stack links, resulting in the packet being discarded with an FCS error. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	–	–	–	–	–
CR-76564	**VCStack**	Previously, when x930 VCStack members were booted up individually in a staggered way, audit inconsistencies error logs could be generated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-76722	**VCStack**	Previously, under rare circumstances, some stack links could link up incorrectly at startup, resulting in the stack not forming. This issue has been resolved.	–	–	Y	Y	–	–	–	–	–	–	–	Y	–	–	Y	–	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-77530	**VCStack**	Previously, it was possible for an x950 or SBx908NG stack to restart unexpectedly during MAC address learning and aging. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–
CR-77593	**VCStack**	Previously, when a stack had been up for between approx 100 and 200 days, a rebooted stack member would not be able to rejoin the stack unless the entire stack was rebooted. This issue has been resolved.	Y	–	Y	Y	–	Y	Y	–	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-77619	**VCStack**	Previously, during a rolling reboot , a "*stack not formed after rolling reboot*" message could be output during a normal reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76725	**VLAN**	Previously, the MTU setting was not working correctly on the x330 Series. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-77597	**VRRP, VCStack**	Previously, a late joining card or stack member could have ACLs previously configured on aggregators applied globally to the card/member instead. Also, previously, on a x530 stack, ACLs configured on aggregators with member ports on a late joining member could have those ACLs incorrectly applied, especially if different ACLs were applied to different aggregators. These issues have been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	Y	Y	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–

Enhancements

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-4813	**User Management**	User password hashes are now calculated using SHA256 instead of MD5. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

What's New in Version 5.5.1-2.4

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G Virtual UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.4.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		05/2022	vaa-5.5.1-2.4.iso (VAA OS) vaa-5.5.1-2.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	05/2022	SBx81CFC960-5.5.1-2.4.rel
SBx908 GEN2	SBx908 GEN2	05/2022	SBx908NG-5.5.1-2.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	05/2022	x950-5.5.1-2.4.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	05/2022	x930-5.5.1-2.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2022	x550-5.5.1-2.4.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	05/2022	x530-5.5.1-2.4.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	05/2022	x510-5.5.1-2.4.rel
IX5-28GPX	IX5	05/2022	IX5-5.5.1-2.4.rel
x330-10GTX	x330	05/2022	x330-5.5.1-2.4.rel
x320-10GH x320-11GPT	x320	05/2022	x320-5.5.1-2.4.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	05/2022	x310-5.5.1-2.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2022	x230-5.5.1-2.4.rel
x220-28GS x220-52GT x220-52GP	x220	05/2022	x220-5.5.1-2.4.rel
IE510-28GSX	IE510-28GSX	05/2022	IE510-5.5.1-2.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	05/2022	IE340-5.5.1-2.4.rel
IE300-12GT IE300-12GP	IE300	05/2022	IE300-5.5.1-2.4.rel
IE210L-10GP IE210L-18GP	IE210L	05/2022	IE210-5.5.1-2.4.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	05/2022	IE200-5.5.1-2.4.rel
XS916MXT XS916MXS	XS900MX	05/2022	XS900-5.5.1-2.4.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	05/2022	GS980MX-5.5.1-2.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	05/2022	GS980EM-5.5.1-2.4.rel
GS980M/52 GS980M/52PS	GS980M	05/2022	GS980M-5.5.1-2.4.rel
GS970EMX/10	GS970EMX	05/2022	GS970EMX-5.5.1-2.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2022	GS970-5.5.1-2.4.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	05/2022	GS900-5.5.1-2.4.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	05/2022	FS980-5.5.1-2.4.rel
10G Virtual UTM Firewall		05/2022	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.4.app
AR4050S AR3050S	AR-series UTM firewalls	05/2022	AR4050S-5.5.1-2.4.rel AR3050S-5.5.1-2.4.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	05/2022	AR2050V-5.5.1-2.4.rel AR2010V-5.5.1-2.4.rel AR1050V-5.5.1-2.4.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.4 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.4

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76458	**ACL**	Previously, executing the command **`show tech support`** might cause a device that had dynamic ACL configured to restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	Y	–	–	–	–	–
CR-75733	**API** **Web Control**	This software update fixes a minor API display issue with cache_size & cache_hits. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-75715	**ARP** **Neighbor Discovery**	Previously, the entries for **`arp-mac-disparity unicast`** were not VLAN aware and could affect traffic on a different VLAN. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73175	**ARP Neighbor Discovery**	Software version 5.5.1-2.0 introduces more strict ARP packet processing, in such a way that only ARP packets with source IP from one of the local subnets of the incoming interface destined to one of the IP addresses of the incoming interface will be processed. With this update, you can re-instate the previous ARP processing behaviour, using a new i**nterface configuration** command. The new command allows less strict ARP packet processing, letting ARPs with source IP address from outside the local subnets of the interface to also be processed. In other words, ARP packets whose source IP address does not belong to the incoming interface's subnet(s) will be processed, otherwise those packets will be silently ignored. The new command is incompatible with any variants of proxy-arp, and when an interface is enabled to do proxy-arp, the behaviour is the same as previously. Also note that clearing the ARP cache might be needed to get rid of undesired existing ARPs after applying the 'no arp-loose-check' command. The new command is: (no) **`arp-loose-check`** ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-75917	**ATMF**	Previously, in some topologies, remote nodes from the core connected via virtual links could become unreachable from the AMF master. 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-75857	**AWC-lite**	This software update removes the temporary file that was created with the MAC filter import/ export function in order to reduce unnecessary memory consumption.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76204	**Firewall**	Previously, under high traffic load, dynamic firewall entities could cause slow memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-75622	**HTTP Service**	Previously, cancelling a file transfer in progress from the GUI (i.e. file download or downloading page elements) could cause the HTTP service on the device to restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76003	**IGMP**	Previously, static IGMP would not be added to the hardware table when multicast routing was enabled. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-75175	**MACSec**	Previously, the command **`show platform macsec`** did not show full tables of data. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-75041	**OSPFv2**	Previously, in networks where routing destinations were learned by both OSPF and BGP, significant topology changes in the network might cause OSPF and BGP events to become out of synchronisation, resulting in route mismatches. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	Y	–	–	Y	Y	Y	–	–	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-76367	**PIM-SM**	Previously, the PIM process restart could consume large amounts of system resources, making the system unresponsive for a period of time. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73888	**Pluggable Transceivers** **Switching**	Previously, when an x530 series switch was connected to a XEM2-12XSv2 with a DAC cable and a shut down command was issued on the x530 port, the 12XSv2 would not indicate the link had dropped. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-76604	**Port Authentication** **ACL**	Previously, the output from the command: **`show access-list counters`** was incorrect when dynamic ACLs were enabled on an interface. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	Y	Y	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR-76621	**Port Authentication** **ACL**	Previously, the dynamic ACL could still be applied even after the supplicant had become unauthenticated. 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-75690	**Port Authentication**	Previously, when using auth-web, it was possible to cause a system reboot if the HTTP headers were too large when accessing the login web page. With this software update, the supported size has been increased, and rather than causing a system reboot it will return an appropriate HTTP error code. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75829	**Port Authentication**	Previously, when replacing a supplicant that was already authenticated via web authentication with a new device of the same IP address, it was possible for the device not to be authenticated. This issue has been resolved. Also, with this software update, a configuration option has been provided for webauth such that if a new supplicant attempting to connect detects a conflicting (already existing) supplicant with the same IP address, the user can configure such that it is the existing supplicant that is logged off to allow the new supplicant to connect. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76741	**QoS**	Previously, the command **`wrr-queue queue-limit`** would not work correctly when an identical set of queue weightings were applied to physical ports belonging to different switch instances (generally ports 1-24, 51-52 and ports 25-50 belong to different instances). This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–
CR-75757	**SNMP**	Previously, the SNMP discovery service was on by default even if it was not enabled, resulting in excessive logs. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76582	**SNMP**	Previously, accessing the temperature sensors of the SBx8100 DC PSU via SNMP could result in a system restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-75954	**SSH** **VRF-lite**	With this software update, SSH access is denied on VRF instances. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76601	**SSL**	This software update addresses the DoS security vulnerability issues found in CVE-2022-0778. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-75998	**VCStack**	With this software update, rolling reboot log is now displayed on the **x330** series.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-76335	**VCStack**	Previously, when changing stacking modes on the x930 series, it was possible for the configuration to show the wrong stack ports. Rebooting with this configuration would not resolve the situation. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-75944	**VCStack ICMP**	Previously, when a member joined a stack that was already operating, some Layer 3 settings were not correctly synced to the new stack member. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-75681	**VXLAN**	This software update removes the command **`platform l3-vxlan enable`** for the x530 Series, as it is not required.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-75563	**WebAPI**	Previously, adding or deleting a hardware ACL from the Web API with an empty body could cause a device to restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

Enhancements

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S
ER-4635	**MRP**	Previously, an MRP license was required to run either MRP client or MRP manager on AlliedWare Plus devices. With this enhancement, an MRP license is only required for running an MRP manager instance.	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
ER-4316	**Snooping DHCP**	With this software update, the 'per-vlan' DHCP Snooping mode is now available on the SBx8100, x530 and x320 Series. ISSU: ISSU Complete	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–

What's New in Version 5.5.1-2.3

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G Virtual UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.3.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		03/2022	vaa-5.5.1-2.3.iso (VAA OS) vaa-5.5.1-2.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2022	SBx81CFC960-5.5.1-2.3.rel
SBx908 GEN2	SBx908 GEN2	03/2022	SBx908NG-5.5.1-2.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	03/2022	x950-5.5.1-2.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	03/2022	x930-5.5.1-2.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2022	x550-5.5.1-2.3.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2022	x530-5.5.1-2.3.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	03/2022	x510-5.5.1-2.3.rel
IX5-28GPX	IX5	03/2022	IX5-5.5.1-2.3.rel
x330-10GTX	x330	03/2022	x330-5.5.1-2.3.rel
x320-10GH x320-11GPT	x320	03/2022	x320-5.5.1-2.3.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	03/2022	x310-5.5.1-2.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2022	x230-5.5.1-2.3.rel
x220-28GS x220-52GT x220-52GP	x220	03/2022	x220-5.5.1-2.3.rel
IE510-28GSX	IE510-28GSX	03/2022	IE510-5.5.1-2.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2022	IE340-5.5.1-2.3.rel
IE300-12GT IE300-12GP	IE300	03/2022	IE300-5.5.1-2.3.rel
IE210L-10GP IE210L-18GP	IE210L	03/2022	IE210-5.5.1-2.3.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2022	IE200-5.5.1-2.3.rel
XS916MXT XS916MXS	XS900MX	03/2022	XS900-5.5.1-2.3.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	03/2022	GS980MX-5.5.1-2.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2022	GS980EM-5.5.1-2.3.rel
GS980M/52 GS980M/52PS	GS980M	03/2022	GS980M-5.5.1-2.3.rel
GS970EMX/10	GS970EMX	03/2022	GS970EMX-5.5.1-2.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2022	GS970-5.5.1-2.3.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2022	GS900-5.5.1-2.3.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	03/2022	FS980-5.5.1-2.3.rel
10G Virtual UTM Firewall		03/2022	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.3.app
AR4050S AR3050S	AR-series UTM firewalls	03/2022	AR4050S-5.5.1-2.3.rel AR3050S-5.5.1-2.3.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	03/2022	AR2050V-5.5.1-2.3.rel AR2010V-5.5.1-2.3.rel AR1050V-5.5.1-2.3.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.3 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.3

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75844	**Logging**	Previoulsy, if the system logging was configured to use an SSH connection, it could consume memory slowly until the system memory was completely exhausted. 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	Y	Y	Y	Y	Y	–
CR-75887	**Loop Protection**	Previously, some loop-detection packets would not be sent from the port despite loop-protection counters reporting the packets as transmitted. This issue has been resolved. The packets are now more reliably sent. However, it is now possible for the send on a packet to timeout. The counters now show when this is the case. A new warning log message has been added if transmitting loop-detection packets takes much longer than expected. It is possible that in some networks with large numbers of loop-protection instances with short loop-detection intervals, that this log message will be emitted: `"Sending loop-detection frames taking longer than expected - too many instances?"` In addition: ■ The output of the command **`show loop-protection counters`** now includes packet tx timeout counter ■ The output of the command **`show loop-protection`** now shows the total number of loop protection instances (one instance per VLAN per port) and what that means for the number of packets that need to be transmitted by the device each second. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76005	**Loop Protection**	Previously, showing the loop-protection counters when a large number of loop-protection instances were present would take a very long time and could cause a system reboot This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76182	**Pluggable Transceivers**	Previously, XEM2-12XSv2 and XEM2-8XSTm on x550 series would not handle remote faults correctly when fibre pluggables were used. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-75848	**Policy-based Routing**	Previously, the QoS rules could be incorrectly ordered in hardware when the class map feature was used. As a result, packets traversing through the device could be improperly classified. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–

What's New in Version 5.5.1-2.2

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G Virtual UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.2.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		03/2022	vaa-5.5.1-2.2.iso (VAA OS) vaa-5.5.1-2.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2022	SBx81CFC960-5.5.1-2.2.rel
SBx908 GEN2	SBx908 GEN2	03/2022	SBx908NG-5.5.1-2.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	03/2022	x950-5.5.1-2.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	03/2022	x930-5.5.1-2.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2022	x550-5.5.1-2.2.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2022	x530-5.5.1-2.2.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	03/2022	x510-5.5.1-2.2.rel
IX5-28GPX	IX5	03/2022	IX5-5.5.1-2.2.rel
x330-10GTX	x330	03/2022	x330-5.5.1-2.2.rel
x320-10GH x320-11GPT	x320	03/2022	x320-5.5.1-2.2.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	03/2022	x310-5.5.1-2.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2022	x230-5.5.1-2.2.rel
x220-28GS x220-52GT x220-52GP	x220	03/2022	x220-5.5.1-2.2.rel
IE510-28GSX	IE510-28GSX	03/2022	IE510-5.5.1-2.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2022	IE340-5.5.1-2.2.rel
IE300-12GT IE300-12GP	IE300	03/2022	IE300-5.5.1-2.2.rel
IE210L-10GP IE210L-18GP	IE210L	03/2022	IE210-5.5.1-2.2.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2022	IE200-5.5.1-2.2.rel
XS916MXT XS916MXS	XS900MX	03/2022	XS900-5.5.1-2.2.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	03/2022	GS980MX-5.5.1-2.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2022	GS980EM-5.5.1-2.2.rel
GS980M/52 GS980M/52PS	GS980M	03/2022	GS980M-5.5.1-2.2.rel
GS970EMX/10	GS970EMX	03/2022	GS970EMX-5.5.1-2.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2022	GS970-5.5.1-2.2.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2022	GS900-5.5.1-2.2.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	03/2022	FS980-5.5.1-2.2.rel
10G Virtual UTM Firewall		03/2022	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.2.app
AR4050S AR3050S	AR-series UTM firewalls	03/2022	AR4050S-5.5.1-2.2.rel AR3050S-5.5.1-2.2.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	03/2022	AR2050V-5.5.1-2.2.rel AR2010V-5.5.1-2.2.rel AR1050V-5.5.1-2.2.rel

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.2 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.1-2.2

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75639	**AMF**	Previously, when a new AMF node was cloned from the original, the hostname in the configuration would remain the same, it wouldn't be the new one. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-75862	**Bootup**	Previously, when booting a device with an empty bootloader environment, the boot would fail with the following console message: "*real_init: base/bootm_mapsize main process (365) terminated with status 1*". This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	–	–	–	–
CR-75699	**DPI**	Previously, disabling the command **`tunnel security-reprocessing`** would not work correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-75919	**DPI**	Previously, certain rare configurations involving the command **`tunnel security-reprocessing`** could experience fatal exceptions when processing fragmented IP packets. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-74702	**Firewall**	Previously, unicast UDP traffic flowing in one direction could incorrectly cause the firewall UDP limit to be reached, resulting in the UDP traffic being dropped. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75914	**ICMP**	The command **`ssh server secure-mac`** has been modified to exclude 'umac-64@openssh.com' from the list of strong MAC algorithms for SSH server to mitigate a security vulnerability. Enabling the command will allow SSH server to only use the following MAC algorithms: ■ umac-128@openssh.com ■ umac-128-etm@openssh.com ■ hmac-sha2-256-etm@openssh.com ■ hmac-sha2-512-etm@openssh.com ■ hmac-sha2-256 ■ hmac-sha2-512 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-75707	**IDS/IDS**	This software update addresses the TCP security vulnerability issues as outlined in CVE-2021-37592.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-75716	**IGMP**	With this software update, the command: **`platform l2mcoverlap`** is now enabled by default on FS980M devices to allow the switch to resolve a large number of multicast routes. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-75596	**IPSec**	This software update addresses multiple IPSec security vulnerabilities as outlined in CVE-2021-41991.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-75545	**IPSec, ISAKMP**	Previously, the IPSec oper-status-control feature was not supported due to a number of issues relating to the 'always-on' tunnel behaviour. These issues have been resolved. The feature is now supported.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75884	**Loop Protection**	Previously, if the loop-protection process restarted, the loop-protection configuration would be reset and no longer shown in the running-configuration. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-75748	**NAT**	Previously a matching NAT rule of type ‘masquerade’ would always take precedence over a matching rule of type ‘src-netmap’, regardless of rule ID. Similarly, a matching NAT rule of type ‘portfwd’ would always take precedence over a matching rule of type ‘dst-netmap’, regardless of rule ID. This was not correct. The rule ID should determine precedence. With this software update, now NAT rules are applied in order of rule ID.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-75086	**Pluggable Transceivers**	Previously, the x530 Series could miss a port link status change event at bootup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75873	**Port Configuration**	With this software update, a new spanning-tree feature (and command) has been added to allow spanning-tree to put a root-inconsistent port into Alternate port role instead of the default Designated port role. The Root Guard feature makes sure that the port on which it is enabled is a designated port. If a Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP). To avoid this situation, you can now configure spanning-tree to put root-inconsistent ports into the alternate role, instead of designated role. In the alternate role the port will not send BPDUs. Use this feature only when there is a possibility that a port enabled with root guard may mistakenly be connected to the root bridge, or a switch downstream of the root bridge. Configuring this feature will add up to a 6 second delay in spanning-tree re-convergence when a port recovers from the root-inconsistent state. To enable or disable this feature, use the command: (no) **`spanning-tree alternate-root-inconsistent`** 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	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-75732	**Port Authentication VCStack**	Previously, if the connection with the RADIUS server was lost when the supplicants were reauthenticated, some supplicants would not be reauthenticated. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75706	**SSH**	With this software update, SSH is upgraded. A number of insecure features were fully deprecated. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-74593	**System**	Previously, the combination of a large number of application-proxy blocks and a large number of incoming MAC addresses could possibly to cause a device to restart unexpectedly. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR-74894	**System**	Previously, there was a potential memory exhaustion issue, in particular when dynamic "fully qualified domain name" (FQDN) were used. 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	Y	Y	Y	Y	Y	Y	–
CR-76114	**System**	This software update addresses the EAP authentication security vulnerability as outlined in CVE-2021-45079. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75890	**TCP**	The use of the TCP timestamp response to approximate host uptime to aid in further attacks has been considered as vulnerable. Additionally, devices might be fingerprinted based on the behavior of the TCP time stamps. This software update introduces a new global configuration mode command to enable/ disable the use of the TCP timestamp option by the device. To enable the TCP timestamp option, use the command: `ip tcp-timestamp` To disable the use of the TCP timestamp option, use the command: `no ip tcp-timestamp` ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-74973	**VCStack**	Previously, when a stack member was joining the stack,the other stack member might experience a duplicate master. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-75643	**VCStack**	Previously, on x530 series switches, if a stackport connected to a stack member was disconnected and connected to a new stack member, it was possible that the new member would never join the stack (without rebooting the stack). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–

What's New in Version 5.5.1-2.1

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
x510 Series
x510L Series
IX5-28GPX
x330-10GTX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
GS900MX/MPX Series
FS980M Series
10G Virtual UTM Firewall
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-2.1.

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.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 131.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 133. 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		11/2021	vaa-5.5.1-2.1.iso (VAA OS) vaa-5.5.1-2.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-2.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2021	SBx81CFC960-5.5.1-2.1.rel
SBx908 GEN2	SBx908 GEN2	11/2021	SBx908NG-5.5.1-2.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	11/2021	x950-5.5.1-2.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	11/2021	x930-5.5.1-2.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2021	x550-5.5.1-2.1.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	11/2021	x530-5.5.1-2.1.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	11/2021	x510-5.5.1-2.1.rel
IX5-28GPX	IX5	11/2021	IX5-5.5.1-2.1.rel
x330-10GTX	x330	11/2021	x330-5.5.1-2.1.rel
x320-10GH x320-11GPT	x320	11/2021	x320-5.5.1-2.1.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	11/2021	x310-5.5.1-2.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2021	x230-5.5.1-2.1.rel
x220-28GS x220-52GT x220-52GP	x220	11/2021	x220-5.5.1-2.1.rel
IE510-28GSX	IE510-28GSX	11/2021	IE510-5.5.1-2.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	11/2021	IE340-5.5.1-2.1.rel
IE300-12GT IE300-12GP	IE300	11/2021	IE300-5.5.1-2.1.rel
IE210L-10GP IE210L-18GP	IE210L	11/2021	IE210-5.5.1-2.1.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2021	IE200-5.5.1-2.1.rel
XS916MXT XS916MXS	XS900MX	11/2021	XS900-5.5.1-2.1.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	11/2021	GS980MX-5.5.1-2.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2021	GS980EM-5.5.1-2.1.rel
GS980M/52 GS980M/52PS	GS980M	11/2021	GS980M-5.5.1-2.1.rel
GS970EMX/10	GS970EMX	11/2021	GS970EMX-5.5.1-2.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2021	GS970-5.5.1-2.1.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2021	GS900-5.5.1-2.1.rel

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

Models	Family	Date	Software File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	11/2021	FS980-5.5.1-2.1.rel
10G Virtual UTM Firewall		11/2021	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.1-2.1.app[1]
AR4050S AR3050S	AR-series UTM firewalls	11/2021	AR4050S-5.5.1-2.1.rel AR3050S-5.5.1-2.1.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	11/2021	AR2050V-5.5.1-2.1.rel AR2010V-5.5.1-2.1.rel AR1050V-5.5.1-2.1.rel

1. Coming soon

Caution: Software version 5.5.1-2.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-2.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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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

The 5.5.1-2.1 software version is not ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features in 5.5.1-2.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 125.

Allied Telesis Autonomous Management Framework (AMF) support for 1000 AMF areas

Available on AMF Cloud

From version 5.5.1-2.1 onwards, AMF Cloud controllers now support up to 1000 AMF areas. When using AMF Cloud as the controller of 301 to 1000 areas, the following restrictions apply:

- Multiple controllers are not supported.
- The controller must be the only master in its area.

AMF Cloud support for AMF areas requires the following virtual environments:

Table 2: Environment for AMF Cloud

AMF AREA SIZE	vCPUs	MEMORY
AMF Cloud 1 to 300 AMF areas	2	2GB
AMF Cloud 301 to 1000 AMF areas	2	4GB

See the AMF Cloud datasheet for full system requirements.

Default self-signed trustpoint

Available on all AlliedWare Plus devices

From version 5.5.1-2.1 onwards, AlliedWare Plus devices generate a default trustpoint named 'default-selfsigned'. This trustpoint contains a self-signed root and server certificate along with their RSA public/private keys. It allows HTTPS clients to establish a secure trusted connection with the AlliedWare Plus device.

The trustpoint root certificate has the common name set to 'AlliedWarePlusCA', while the server certificate's common name is set to 'AlledWarePlusDefault'. Both the trustpoint and server certificate's **serialNumber** attribute are set to the device's MAC address.

If user trustpoints are not configured then the default trustpoint will be used for all HTTPS or secure application connections.

To see details of the default trustpoint, use the following command:

```
awplus#show crypto pki trustpoint
--------------------
Trustpoint "default-selfsigned"
 Type : Self-signed certificate authority
 Root Certificate: 92BC482F 61653B85 11331914 B1736225 7D05E944
 Local Server : The server is enrolled to this trustpoint.
 Server Key : default-selfsigned
```

To see details of the default trustpoint's certificates, use the following command:

```
awplus#show crypto pki certificate
--------------------
Trustpoint "default-selfsigned" Certificate Chain
--------------------
Server certificate
 Subject : /O=Allied-Telesis/CN=AlliedwarePlusDefault
 /serialNumber=0000.cd28.0881
 Issuer : /O=Allied Telesis, Inc./CN=AlliedWarePlusCA
 /serialNumber=0000.cd38.064d
 Valid From : Oct 5 13:00:39 2021 GMT
 Valid To : Sep 23 13:00:39 2071 GMT
 Fingerprint : 39349F56 A5A7432D 15708C09 915345B9 D33425AB

Self-signed root certificate
 Subject : /O=Allied Telesis, Inc./CN=AlliedWarePlusCA
 /serialNumber=0000.cd28.0881
 Issuer : /O=Allied Telesis, Inc./CN=AlliedWarePlusCA
 /serialNumber=0000.cd38.064d
 Valid From : Oct 5 13:00:38 2021 GMT
 Valid To : Sep 23 13:00:38 2071 GMT
 Fingerprint : 92BC482F 61653B85 11331914 B1736225 7D05E944
```

For more information on the AlliedWare Plus PKI implementation, see the Public Key Infrastructure (PKI) Overview and Configuration Guide.

Restricting port authenticated supplicants to one per VLAN

Available on all AlliedWare Plus devices that support port authentication.

From version 5.5.1-2.1 onwards, you can restrict port authenticated supplicants on an interface to one per VLAN. This is useful, for example, if you have configured multiple supplicants on an interface but you want to restrict network access to a single IP phone and a single authorized workstation.

To use this feature first configure port authentication with multiple supplicants on an interface. Then use the following command to limit authorization to a single supplicant per VLAN:

```
awplus(config-if)# auth vlan-restriction
```

The following configuration snippets illustrate how to configure port authentication on interface port1.0.1 and restrict access to an single IP phone and authorized workstation.

RADIUS configuration:

```
radius-server local
 server enable
 nas 127.0.0.1 key awplus-local-radius-server
 user PC1 encrypted password ns3hLyKY5TsY6egEYbP4s1DPtgCSOIBPD7Z435qETec=
 user 00-0b-82-51-65-b4 encrypted password
mssv+c7URUgtfltKy46RtySRkN7n8Jbj8FCgve2soTE=
```

Interface configuration

```
interface port1.0.1
 switchport
 switchport mode access
 switchport access vlan 100
 auth-mac enable
 dot1x port-control auto
 auth host-mode multi-supplicant
 auth vlan-restriction
 auth dynamic-vlan-creation type multi
 spanning-tree portfast
 lldp med-tlv-select all
 switchport voice vlan 15
```

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

Hardware Health Monitoring enhancements for SBx8100

Available on SBx8100

From version 5.5.1-2.1 onwards, you can configure Hardware Health Monitoring (HHM) to provide more resilient function under rare internal system conditions. By default, the device will generate log messages that include recommended action. You can also now enable the device to take recovery action if these conditions occur. We recommend you enable this by using the command:

```
awplus(config)# system hw-monitoring reboot
```

When enabled, if these rare system conditions occur, the affected card would reboot to recover its ability to forward traffic. This action is disabled by default.

Note that other options for this command are intended for technical support.

sFlow support on AR4050S and 10G Virtual UTM Firewalls

Available on AR4050S and 10G Virtual UTM Firewalls

From version 5.5.1-2.1 onwards, sFlow is supported on the AR4050S and 10G Virtual UTM firewalls.

sFlow® is a network monitoring protocol which provides a means for collecting packets, together with interface counters, and then exporting them to an external collector. The collector displays statistics about the traffic flowing through the device. From these statstics you can quickly see:

- what the network is being used for
- trends useful for performance optimisation
- traffic indicating potential security threats
- usage for billing and accounting purposes
- abnormal traffic and indications of its causes

sFlow commands on the firewalls:

- match those on switches, but are available on Layer 3 interfaces rather than switch ports.
- support Layer 3 interfaces (Ethernet, VLANs, PPP, tunnels, 802.1q).
- do not support switch ports on firewalls.

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

WAN load balance weighted lottery mode

Available on AR4050S, AR3050S, AR2050V, AR2010V, AR1050V

From version 5.5.1-2.1 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 new **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 on weighted lottery mode, see the Route Selection Feature Overview and Configuration Guide.

TLS version 1.3 supported for OpenVPN

Available on AR4050S, AR3050S, AR2050V, AR2010V, AR1050V

From version 5.5.1-2.1 onwards, TLS version 1.3 is supported for OpenVPN on AR-series devices.

You can also now set the minimum TLS (Transport Layer Security) version to be version 1.3. To allow this, the following command has been updated:

```
awplus(config-if)# tunnel openvpn tls-version-min {1.1|1.2|
1.3}
```

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

Spanning tree loop guard

Available on all AlliedWare Plus switches

From 5.1.1-2.1 onwards, AlliedWare Plus switches support STP loop guard, which helps prevent spanning-tree loops. Such loops can occur because of a unidirectional link failure on a point-to-point link, or software failures on switches with ports acting as designated ports in a spanning-tree.

Loop guard checks to make sure that root ports and alternate/backup ports keep receiving BPDUs from their designated port on the link. If a port stops receiving BPDUs from its designated port, it transitions to a state called 'loop-inconsistent' and discards packets. The port recovers from this loop-inconsistent state state as soon as it receives a BPDU again from the designated port.

You can enable loop guard on a per-port basis, using the new command:

```
awplus(config-if)# spanning-tree guard loop
```

Note that spanning-tree loop guard cannot be used with spanning-tree root guard. Only one of these may be configured on an interface.

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

MAC notification through SNMP

Available on all AlliedWare Plus switches except IE200 Series

From 5.5.1-2.1 onwards, the MAC notification feature monitors the forwarding database (FDB) and alerts users of changes through SNMP. MAC notification monitors changes to the dynamically added MAC address and port pairings in the FDB and to the Layer 2 FDB utilization.

MAC notification brings three new SNMP trap types:

- MAC change
  Records MAC addresses entering and leaving the FDB.
- MAC move
  Records MAC addresses changing port associations.
- MAC threshold
  Tracks FDB utilization.

These three new trap types are extra ways for you to monitor networks by tracking users through the network, seeing peak connection times, detecting problematic connections or users causing MAC address table instability, and noticing over utilized network nodes.

The command **snmp trap mac-change** enables MAC change traps to track MAC addresses added and removed from a port. At this point the history table exists and can be obtained through SNMP.

The command **snmp-server enable trap <*trap-list*>** enables the switch to transmit the specified traps (notifications). This command is used to enable mac-change, mac move and mac threshold traps.

The command **mac address-table notification mac-change** is used to enable the feature. There are also some optional parameters that you can set using the commands **mac address-table notification mac-change interval** and **mac address-table notification history-size**. The interval is in seconds and this is the time between two MAC change SNMP notifications being sent. The history-size allows you to set an upper limit on the number of entries that the SNMP table may contain.

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

MACsec enhancements and hardware support

Available on SBx908 GEN2, x950, x930, and x550 Series

From 5.5.1-2.1 onwards, MACsec provides support on the following devices:

- MACsec is supported on the x550-18XSQ switch on ports 1-16 (SFP+ ports). (Other x550 Series switches do not support MACsec.)
- The command **crypto random bytes** is now available on all x550 Series switches. This generates cryptographically secure random numbers, which you can use for encryption keys such as the CAK.

From version 5.5.1-2.1 onwards, MACsec includes the following enhancements on MACsec-enabled devices:

- All: You can configure MACsec with 256-bit CAKs (**mka pre-shared-key** command).
- On SBx908 GEN2 and x950 Series with XEM2-12XS v2 or XEM2-8XSTm only: You can configure MACsec to use the cipher suite GCM-AES-256 (**macsec-cipher-suite** command). (Other MACsec-enabled switches and XEMs support only the default cipher suite GCM-AES-128.)

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

VXLAN support on SBx908 GEN2 & x950 Series switches

Available on SBx908 GEN2 and x950 Series switches

From version 5.5.1-2.1 onwards, Virtual Extensible LAN (VXLAN) is supported on the SBx908 GEN2 and x950 Series. Previously, this feature was only available on the x530 Series.

VXLAN is an overlay encapsulation technology. It creates a virtual network overlaid on top of the existing physical network infrastructure. It uses the underlay IP network and builds a flexible Layer 2 overlay logical network on it.

Note that VXLAN in VCStack environments will be supported in an upcoming AlliedWare Plus version.

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

Message about changing the default password

Available on all AlliedWare Plus devices

From version 5.5.1-2.1 onwards, every time a user logs in with the default "manager" account, AlliedWare Plus will check whether the factory default password is set. If it is, the system will print a message onscreen to warn the user to change the default password. For example:

```
awplus login: manager
Password:
AlliedWare Plus (TM) 5.5.1-2.1 10/26/21 15:23:17
% Default password needs to be changed.
```

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

Seeing how many packets match hardware ACLs

Available on all AlliedWare Plus devices that support hardware ACLs

From version 5.5.1-2.1 onwards, a new command lets you see how many packets match one or all of your hardware ACLs, so you can check your ACL configuration. Every time a hardware ACL allows or drops a packet, this command's counter increments. The new command is:

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

where the optional <*acl*> parameter lets you display the matches for a single ACL. You can enter the ACL name or number.

For more information about ACLs, see the Access Control List (ACL) Feature Overview and Configuration Guide.

Forwarding of multicast packets with a TTL of 1

Available on SBx908 GEN2 and x950 Series switches

Previously, if multicast packets had a TTL of 1, SBx908 GEN2 and x950 Series switches would flood them out all ports of the VLAN. This could make clients receive multicast traffic that they hadn't subscribed to. From version 5.5.1-2.1 onwards, the switches only send such packets to members of the appropriate multicast group.

As part of this enhancement, the command **platform l2mc-overlap** has been added to the SBx908 GEN2 and x950 Series switches, to avoid deleting overlapping entries if they are still in use. An overlap exists if the resulting MAC address is the same for two different multicast groups. For example, 224.1.1.1 and 239.1.1.1 will result in a multicast overlap—packets destined for 239.1.1.1 will also be sent to 224.1.1.1.

This command is disabled by default. We recommend you enable it if you have multicast packets with a TTL of 1.

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

Processing IGMP packets immediately

Available on SBx908 GEN2 and x950 Series switches

From version 5.5.1-2.1 onwards, a new command enables SBx908 GEN2 and x950 Series switches to process IGMP packets more quickly in networks with a low rate of IGMP packets. This allows clients to start receiving multicast traffic immediately. Without this command, these switches process IGMP packets after they receive 250 packets or after 1 second, whichever comes first. The new command is:

```
awplus(config)# ip multicast handle-igmp-immediately
```

Enabling this command is only recommended when using up to 4096 multicast streams.

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

Adding a description to static routes

Available on all AlliedWare Plus devices that support static routes

From version 5.5.1-2.1 onwards, you can give static routes descriptions, using the command **ip route** or **ipv6 route**:

```
awplus(config)# ip route description <description>
awplus(config)# ipv6 route description <description>
```

The description is optional and lets you record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device.

To see the description, use the command **show running-configuration**.

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

ECDSA key automatically created for SSH

Available on all AlliedWare Plus devices

From version 5.5.1-2.1 onwards, AlliedWare Plus devices automatically create an Elliptic Curve Digital Signature Algorithm (ECDSA) key when the SSH service is enabled, if an ECDSA key doesn't already exist. This makes it possible for certain older SSH clients to connect to AlliedWare Plus devices securely.

For more information about SSH, see the Secure Shell (SSH) Feature Overview and Configuration Guide.

Allowing only use of strong hashing (MAC) algorithms

Available on all AlliedWare Plus devices

From version 5.5.1-2.1 onwards, you can prevent the SSH service from using less-secure MAC algorithms such as umac-64-etm@openssh.com, hmac-sha1-etm@openssh.com and hmac-sha1. To do this, use the new command:

```
awplus(config)# ssh server secure-mac
```

The list of MAC algorithms allowed by this command are: umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512.

This command joins other existing commands to prevent SSH from using less-secure cyphers and KEX (**ssh server secure-ciphers** and **ssh server secure-kex**). As well, another new command is the equivalent of all 3 commands combined, so you don't have to enter all 3 commands:

```
awplus(config)# ssh server secure-algs
```

The command **show ssh server** now displays the list of currently allowed MAC algorithms.

For more information about SSH, see the Secure Shell (SSH) Feature Overview and Configuration Guide.

Disabling CBC mode ciphers for SSH server in Secure Mode

Available on all AlliedWare Plus switches that support Secure Mode

From 5.5.1-2.1 onwards, you can disable CBC mode ciphers for the SSH server when the switch is in crypto Secure Mode. The SSH server will then only offer aes128-ctr, aes192-ctr, and aes256-ctr cipher algorithms.

To do this, use the new command:

```
awplus(config)# ssh server disallow-cbc-ciphers
```

For more information about SSH, see the Secure Shell (SSH) Feature Overview and Configuration Guide.

VCStack over 1 Gigabit on the x930 Series

Available on x930 Series

From version 5.5.1-2.1 onwards, VCStack is supported on 1G copper ports and SFP ports on the x930 Series.

VCStack, in conjunction with link aggregation, provides a highly available system where network resources are spread out across stacked units, providing excellent resiliency. You can form a stack with up to 4 members using VCStack on 1G copper and SFP ports. Note that you can stack up to 8 units at 2.5/5/10G speeds.

To enable 1 Gigabit stacking on the x930 Series, use the following command:

```
awplus(config)# stack enable front-panel-ports
```

For more information on VCStack, see the Virtual Chassis Stacking Feature Overview and Configuration Guide.

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.1-x.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
- Older SSH clients can't connect to AlliedWare Plus devices using the ssh-rsa algorithm
- 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

If you are upgrading from an earlier version than 5.5.1-x.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.0-1.x version, please check the 5.5.0-2.x release note. Release notes are available from our website, including:

- 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 118 and "Details for x930 Series" on page 119 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:

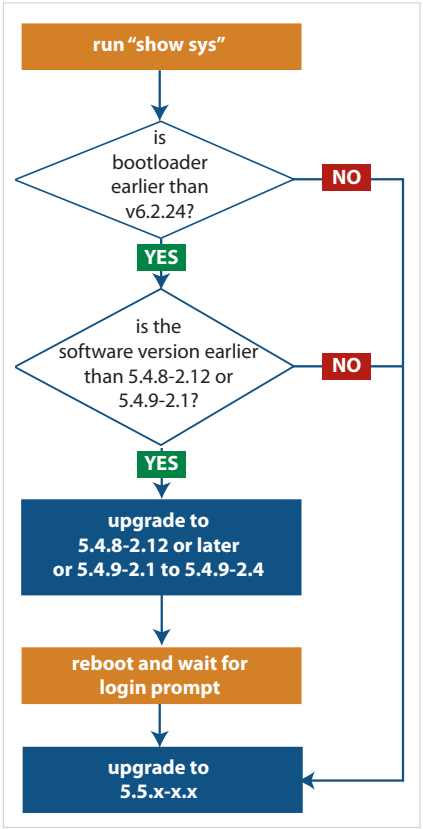
- 5.4.9-1.x
- 5.4.9-0.x
- any version before 5.4.8-2.12.

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:

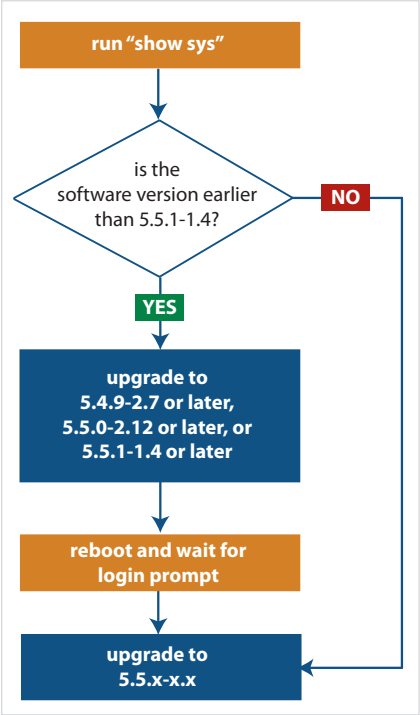



```
awplus# show system
```

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 later
- 5.5.0-2.12 or later
- 5.5.1-1.4 or later.

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
```

Older SSH clients can't connect to AlliedWare Plus devices using the ssh-rsa algorithm

In AlliedWare Plus version 5.5.1-1.1, OpenSSH was upgraded. This means 5.5.1-1.x and 5.5.1-2.x no longer support the following insecure options:

- the ssh-rsa algorithm in OpenSSH, which is based on SHA1
- SSH protocol version 1

Version 5.5.1-2.x automatically creates a key (if necessary) so that older SSH clients can connect using ECDSA instead of the ssh-rsa algorithm—see "ECDSA key automatically created for SSH" on page 115.

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
Some commands not available when accessing CLI via Vista Manager	*All Alliedware Plus devices*	From 5.5.1-0.1 onwards, users accessing the AlliedWare Plus command line via Vista Manager are unable to use the following CLI commands: ■ atmf select-area ■ no atmf select-area

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.1 license on your switch if you are upgrading to 5.5.1-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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

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 5.5.1-2.x from:

- 5.5.1-1.x
- 5.5.1-0.x
- 5.5.0-x.x

On these switches, you **cannot** use rolling reboot to upgrade to 5.5.1-2.x 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 5.5.1-2.x from:

- 5.5.1-1.x
- 5.5.1-0.x
- 5.5.0-x.x
- 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 5.5.1-2.x from:

- 5.5.1-1.x
- 5.5.1-0.x
- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 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 5.5.1-2.x and:

- 5.5.1-1.x
- 5.5.1-0.x
- 5.5.0-x.x

On these switches, auto-synchronization is not supported between 5.5.1-2.x 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 5.5.1-2.x and:

- 5.5.1-1.x
- 5.5.1-0.x
- 5.5.0-x.x
- 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 5.5.1-2.x and:

- 5.5.1-1.x
- 5.5.1-0.x
- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-2.x
- 5.4.6-1.2 and all later 5.4.6-1.x versions.

It is not supported between 5.5.1-0.x 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. If this is not possible, please be aware of the following compatibility limitations.

If using an AMF controller

If your Controller or **any** of your Masters are running 5.4.7-1.1 or later, then the Controller and **all** of the Masters must run 5.4.7-1.1 or later. However, the software on Member nodes can be older than 5.4.7-1.1. Otherwise, the "show atmf area nodes" command and the "show atmf area guests" command will not function, and Vista Manager EX will show incorrect network topology.

If using secure mode

If your AMF network is in secure mode, all nodes must run version 5.4.7-0.3 or later. Upgrade all nodes to version 5.4.7-0.3 or later before you enable secure mode.

If using Vista Manager EX

If you are using Vista Manager EX, then as well as the restrictions above:

- All nodes must run version 5.4.7-0.1 or later
- If any Master node or the Controller is running 5.4.7-0.x, then all nodes must also run 5.4.7-0.x

If using none of the above

If none of the above apply, then nodes running version 5.5.1-2.x are compatible with nodes running:

- 5.5.1-1.x
- 5.5.1-0.x
- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 5.4.4-x.x
- 5.4.3-2.6 or later.

Upgrading all devices in an AMF network

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

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

2. Decide which AMF upgrade method is most suitable.

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

Obtaining User Documentation

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

- **Feature Overview and Configuration Guides** - find these by searching for the feature name and then selecting Configuration Guides in the left-hand menu.
- **Datasheets** - find these by searching for the product series and then selecting Datasheets in the left-hand menu.
- **Installation Guides** - find these by searching for the product series and then selecting Installation Guides in the left-hand menu.
- **Command References** - find these by searching for the product series and then selecting Reference Guides in the left-hand 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 checksum 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
SBx8100	SBx81CFC960-5.5.1-2.17.rel	de2190c6a8d8cf5e5aa3d9fb62e5f53c529234dd1f66372f28af43f518ade39f
SBx908 GEN2	SBx908NG-5.5.1-2.17.rel	0b83e9a91d023670276fd8f078112424f4226932719ae064dbda6b70bc30fe31
x950	x950-5.5.1-2.17.rel	0b83e9a91d023670276fd8f078112424f4226932719ae064dbda6b70bc30fe31
x930	x930-5.5.1-2.17.rel	9a3629d8dee1074f29fe527ce6181cea17cfbd871544ce15d08a8125ec6b9c5a
x550	x550-5.5.1-2.17.rel	07b361838f1463fb8128c2f6fe7ce5aa1ff8791073c063bbec6f26cf8352f6d5
x530 & x530L	x530-5.5.1-2.17.rel	190b5b345b7c75623c9fea7f642c7f7027f0be534676622e6bf6d4526fe2ecc3
x330	x330-5.5.1-2.17.rel	6b641cb9327f0bf6c026496f99cee06b0e7ed182b938c82f39b484ea2caa00ce
x320	x320-5.5.1-2.17.rel	6b641cb9327f0bf6c026496f99cee06b0e7ed182b938c82f39b484ea2caa00ce

Table: Hash values

Product family	Software File	Hash
x230 & x230L	x230-5.5.1-2.17.rel	9b1f5c599519b080c803091901197cc1144d6d19a52835e67ec15ef3e00c672b
x220	x220-5.5.1-2.17.rel	735bb2b95f9d4476530fc95f7197493cfeed69a9d13a8166c50b16677b6c4255
IE340 & IE340L	IE340-5.5.1-2.17.rel	a1fba7834b71abf740534490120c9ee2204f234d66a906080544b9cbb184e05e
XS900MX	XS900-5.5.1-2.17.rel	cf0becd53907522c8c5609dec8bcd124fc52d0429f477880bd17cc9c18a728bd
AR4050S	AR4050S-5.5.1-2.17.rel	5fc1418b8eeaa92a38fc2aa57976cb4780760fd9048945cf24c98b73fa18bf4f
AR3050S	AR3050S-5.5.1-2.17.rel	5fc1418b8eeaa92a38fc2aa57976cb4780760fd9048945cf24c98b73fa18bf4f
AR2050V	AR2050V-5.5.1-2.17.rel	5fc1418b8eeaa92a38fc2aa57976cb4780760fd9048945cf24c98b73fa18bf4f
AR2010V	AR2010V-5.5.1-2.17.rel	5fc1418b8eeaa92a38fc2aa57976cb4780760fd9048945cf24c98b73fa18bf4f
AR1050V	AR1050V-5.5.1-2.17.rel	200b41627724e7fe5e50728552f8d37d6ff19cba5231fb73fcc39cd0ef5c86c4

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                   : 5.5.1
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Aug-2021
License expiry date            : N/A
Release                        : 5.5.1
```

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                   : 5.5.1
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Aug-2021
License expiry date            : N/A
Release                        : 5.5.1
```

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 127 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 129.

Caution: SwitchBlade x908 GEN2, x950 and x930 Series Switches switches can only be upgraded to the most recent software versions from specified older versions. If you attempt to upgrade from other older versions, the software becomes corrupt and the switch will not boot up. For details, see "Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches" on page 117.

To install and enable this software version, 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 SBx8100-5.5.1-2.17.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.1-2.17.rel`
x950 series	`awplus(config)# boot system x950-5.5.1-2.17.rel`
x930 series	`awplus(config)# boot system x930-5.5.1-2.17.rel`
x550 series	`awplus(config)# boot system x550-5.5.1-2.17.rel`
x530 series	`awplus(config)# boot system x530-5.5.1-2.17.rel`
x510 series	`awplus(config)# boot system x510-5.5.1-2.17.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.5.1-2.17.rel`

Product	Command
x330-10GTX	`awplus(config)# boot system x330-5.5.1-2.17.rel`
x320 series	`awplus(config)# boot system x320-5.5.1-2.17.rel`
x310 series	`awplus(config)# boot system x310-5.5.1-2.17.rel`
x230 series	`awplus(config)# boot system x230-5.5.1-2.17.rel`
x220 series	`awplus(config)# boot system x220-5.5.1-2.17.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.5.1-2.17.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.1-2.17.rel`
IE300 series	`awplus(config)# boot system IE300-5.5.1-2.17.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.1-2.17.rel`
IE200 series	`awplus(config)# boot system IE200-5.5.1-2.17.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.1-2.17.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.1-2.17.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.1-2.17.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.1-2.17.rel`
GS970EMX/10	`awplus(config)# boot system GS970EMX-5.5.1-2.17.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.1-2.17.rel`
GS900MX/MPX series	`awplus(config)# boot system GS900-5.5.1-2.17.rel`
FS980M series	`awplus(config)# boot system FS980-5.5.1-2.17.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.1-2.17.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.1-2.17.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.5.1-2.17.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.1-2.17.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.1-2.17.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

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
   ```

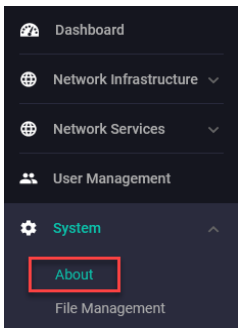
   Alternatively, on unconfigured devices you can use the default address, which is:

   - 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 5.5.1-2.1 is v2.16.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 134 or "Update the GUI on AR-Series devices" on page 135.

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 filename for v2.16.0 of the GUI is **awplus-gui_551_31.gui**.

   The file is not device-specific; the same file works on all devices.

2. Log into the GUI:

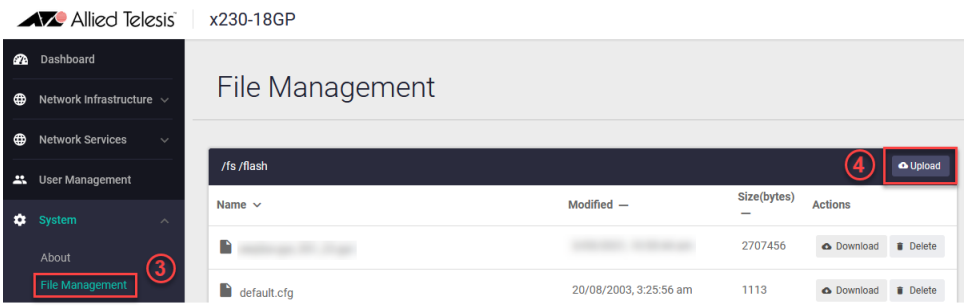
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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

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

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

4. Click **Upload**.



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

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

6. Reboot the switch. Or alternatively, use **System** > **CLI** to access the command line interface, then use the following commands to stop and restart the HTTP service:

   ```
   awplus> enable
   awplus# configure terminal
   awplus(config)# no service http
   awplus(config)# service http
   ```

   To confirm that the correct file is now in use, then use the commands:

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

Update the GUI on AR-Series devices

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

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

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

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

3. Browse to the GUI and check that you have the latest version now, on the **System** > **About** page. You should have v2.16.0 or later.