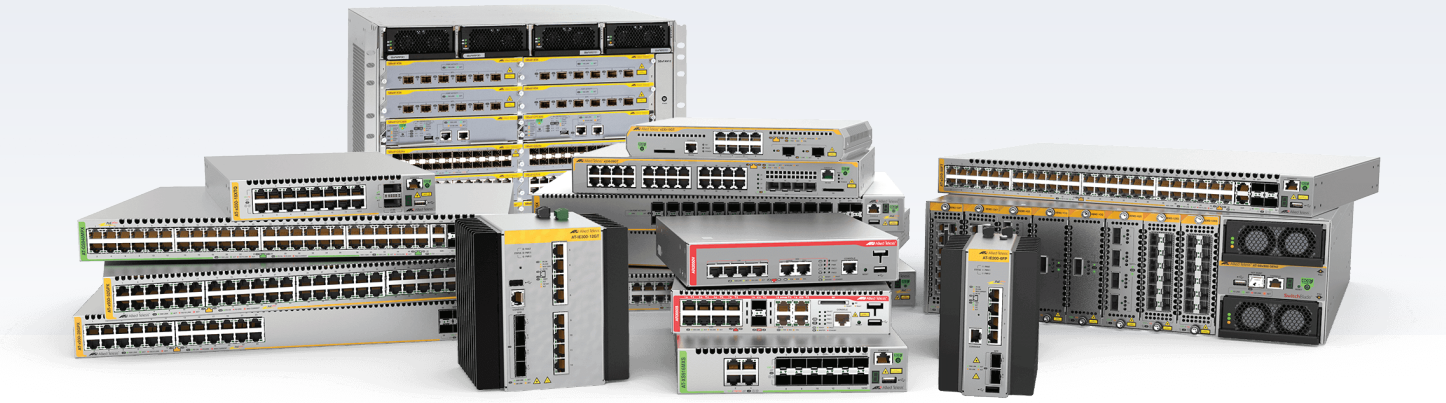
Release Note for AlliedWare Plus Software Version 5.5.0-2.x



AlliedWare Plus OPERATING SYSTEM

» SBx8100 Series » SBx908 GEN2 » x950 Series » x930 Series
» x550 Series » x530 Series » x510 Series » IX5 Series
» x320 Series » x310 Series » x230 Series » x220 Series
» IE500 Series » IE340 Series » IE300 Series » IE210L Series » IE200 Series
» XS900MX Series » GS980M Series » GS980EM Series » GS970M Series
» GS900MX/MPX Series » FS980M Series » AMF Cloud
» AR4050S » AR3050S » AR2050V » AR2010V » AR1050V

» 5.5.0-2.1 » 5.5.0-2.2 » 5.5.0-2.3 » 5.5.0-2.4 » 5.5.0-2.5 » 5.5.0-2.6 » 5.5.0-2.7 » 5.5.0-2.8 » 5.5.0-2.9 » 5.5.0-2.11
» 5.5.0-2.12

Acknowledgments

Getting the most from this Release Note

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

Content

What's New in Version 5.5.0-2.12

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.12.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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-5.5.0-2.12.iso (VAA OS) vaa-5.5.0-2.12. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.12.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2021	SBx81CFC960-5.5.0-2.12.rel
SBx908 GEN2	SBx908 GEN2	11/2021	SBx908NG-5.5.0-2.12.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	11/2021	x950-5.5.0-2.12.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2021	x930-5.5.0-2.12.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2021	x550-5.5.0-2.12.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	11/2021	x530-5.5.0-2.12.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	11/2021	x510-5.5.0-2.12.rel
IX5-28GPX	IX5	11/2021	IX5-5.5.0-2.12.rel
x320-10GH x320-11GPT	x320	11/2021	x320-5.5.0-2.12.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2021	x310-5.5.0-2.12.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2021	x230-5.5.0-2.12.rel
x220-28GS x220-52GT x220-52GP	x220	11/2021	x220-5.5.0-2.12.rel
IE510-28GSX	IE510-28GSX	11/2021	IE510-5.5.0-2.12.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	11/2021	IE340-5.5.0-2.12.rel
IE300-12GT IE300-12GP	IE300	11/2021	IE300-5.5.0-2.12.rel
IE210L-10GP IE210L-18GP	IE210L	11/2021	IE210-5.5.0-2.12.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2021	IE200-5.5.0-2.12.rel
XS916MXT XS916MXS	XS900MX	11/2021	XS900-5.5.0-2.12.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2021	GS980EM-5.5.0-2.12.rel
GS980M/52 GS980M/52PS	GS980M	11/2021	GS980M-5.5.0-2.12.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2021	GS970-5.5.0-2.12.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2021	GS900-5.5.0-2.12.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	11/2021	FS980-5.5.0-2.12.rel
AR4050S AR3050S	AR-Series UTM firewalls	11/2021	AR4050S-5.5.0-2.12.rel AR3050S-5.5.0-2.12.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	11/2021	AR2050V-5.5.0-2.12.rel AR2010V-5.5.0-2.12.rel AR1050V-5.5.0-2.12.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.12 software version is ISSU compatible with previous software versions.

New Features and Enhancements

AMF mixed-platform provisioning

ER-4315: Available on GS900 Series

With version 5.5.0-2.12, you can replace GS900 Series switches with GS980M or x230-52 Series using auto-recovery.

For more information on using auto-recovery and provisioning a replacement node for a specified interface, see the AMF Feature Overview and Configuration Guide.

Issues Resolved in Version 5.5.0-2.12

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-73387	**802.1x**	Previously, unauthorizing supplicants could result in memory exhaustion. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-74068	**ACL, Policy-based-routing**	Previously, on SBx81CFC960 line cards, when a policy-based routing rule was applied, followed by another ACL/QOS rule applied globally/per port, the policy-based routing rule could fail to route the packets matching that rule. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-73727	**ACL, VCStack**	Previously, when modifying an ACL with a large number of filters that was currently attached to a large number of interfaces: ■ if the operation apply time took longer than 10 minutes, it could trigger a system reboot. ■ also, exiting liveupdate mode after first running the **`commit`** command could cause all the changes to be re-applied again, even if no further changes were made. These issues have been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	–	–	–	Y	Y	Y	–	Y	Y	Y	–	–	–	Y	Y	Y	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-71948	**AMF**	Previously, after an AMF network topology change, it was possible in some situations for connectivity to some AMF nodes not to be restored. This issue has been resolved, improvements have been made to the way AMF handles topology changes that involve changes to reachability between virtual and non-virtual links. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-73984	**AMF**	Previously, the '*received packet on xxx with own address as source address*' message was generated at **info** log level. The log message has been changed to **warning** level, to increase its visibility. 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-72009	**ARP / Neighbor Discovery**	Previously, gratuitous ARPs might result in receiving VLANs to incorrectly perform opportunistic neighbor discovery. 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-74354	**AWC-Lite**	Previously, the validation conditions of parameters for the snmp **`community trap`** and **`community read-only`** commands (for AWC-Lite), were incorrect, resulting in characters being rejected which should have been accepted. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	Y	Y	Y	Y	Y	–
CR-74364	**AWC-Lite**	Previously the validation conditions of the <*password*> parameter for the **username (wireless-ap-prof-snmp)** AWC-Lite command were incorrect, resulting in characters being rejected which should have been allowable. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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-73760	**DHCP Snooping**	Previously, DHCP Snooping ACLs may not have been installed correctly and could operate independently on each port. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-73910	**Hardware Health Monitoring**	Previously, under very high network load resulting in sustained packet buffering, it was possible for a card to have internal issues and require a reboot to forward traffic again. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-74082	**IDS / IPS, URL Filter**	Previously, if an Ethernet packet with an error (e.g. FCS error) was received while an AR1050V was running either IPS or URL Filtering, it was possible for that error packet to get stuck in an infinite loop of processing. This would cause the CPU to ramp to 90% and stay there. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-74358	**IDS, IPS**	Previously, on devices with IPS enabled and "category http-events action deny" set, HTTP POST messages containing HTTP Multipart data (e.g. a form submission) might incorrectly be dropped. If this occurred, then an info-level log message would be generated in the form: IPS[4455]: [Drop] IPS: http-events HTTP multipart generic error URL:http://... 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-72178	**PoE**	Previously, the x320-10GH and GS980EM/10H may have incorrectly disconnected PoE to powered devices using low power modes (below 10mA total current across both powered pairs). Additionally, powered devices with low initial current draws (below 10mA) may have been incorrectly denied power while they were still initializing, resulting in such devices being repeatedly power cycled. These issues have been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-74258	**PoE**	Previously, a PoE process was slowly leaking a small amount of memory during PoE connection and disconnection events. 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-73557	**Port Authentication**	Previously, when dynamic VLANs were used in conjunction with MAC authentication, The MAC entry of the new supplicant could be incorrectly removed from the FDB table. The missing MAC may be detected by an auth audit and recovered along with a log message generated indicating the entry was missing. 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-74342	**QoS, Switching**	Previously, if multiple policers, via service-policy, or QSP were added to the x530s series, then they would not work correctly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–
CR-74465	**SNMP**	Previously, certain forms of memory corruption could cause the SNMP process to restart periodically. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	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-74667	**SSH**	Previously, the command **`crypto key destroy hostkey`** could fail to be executed in Secure Mode. 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-74495	**Storm Control**	Previously, storm-control configuration could not be applied to 40G ports on an XLEM card. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-73696	**Switching**	Previously, configuring *Ingress-filter disable* on a switchport could cause traffic to unexpectedly be flooded to the configured port. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-74221	**System**	Previously, an internal error could occur in very rare cases that could deplete some of the switching system resources. Over time it was possible for this to eventually result in a VCStack separation. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-66144	**VCStack**	Previously, when configuration commands were executed (either interactively or as part of an automated script) while a stack member was in the process of joining, the commands could fail to execute and take 5 minutes per command to timeout. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-73925	**VLAN**	Previously If dot1q interfaces were configured, each time the running-configuration was written or displayed, a small memory leak could 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

What's New in Version 5.5.0-2.11

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.11.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		08/2021	vaa-5.5.0-2.11.iso (VAA OS) vaa-5.5.0-2.11. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.11.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2021	SBx81CFC960-5.5.0-2.11.rel
SBx908 GEN2	SBx908 GEN2	08/2021	SBx908NG-5.5.0-2.11.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	08/2021	x950-5.5.0-2.11.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2021	x930-5.5.0-2.11.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2021	x550-5.5.0-2.11.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	08/2021	x530-5.5.0-2.11.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	08/2021	x510-5.5.0-2.11.rel
IX5-28GPX	IX5	08/2021	IX5-5.5.0-2.11.rel
x320-10GH x320-11GPT	x320	08/2021	x320-5.5.0-2.11.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2021	x310-5.5.0-2.11.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2021	x230-5.5.0-2.11.rel
x220-28GS x220-52GT x220-52GP	x220	08/2021	x220-5.5.0-2.11.rel
IE510-28GSX	IE510-28GSX	08/2021	IE510-5.5.0-2.11.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	08/2021	IE340-5.5.0-2.11.rel
IE300-12GT IE300-12GP	IE300	08/2021	IE300-5.5.0-2.11.rel
IE210L-10GP IE210L-18GP	IE210L	08/2021	IE210-5.5.0-2.11.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2021	IE200-5.5.0-2.11.rel
XS916MXT XS916MXS	XS900MX	08/2021	XS900-5.5.0-2.11.rel
GS980EM/10H GS980EM/11PT	GS980EM	08/2021	GS980EM-5.5.0-2.11.rel
GS980M/52 GS980M/52PS	GS980M	08/2021	GS980M-5.5.0-2.11.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2021	GS970-5.5.0-2.11.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2021	GS900-5.5.0-2.11.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	08/2021	FS980-5.5.0-2.11.rel
AR4050S AR3050S	AR-Series UTM firewalls	08/2021	AR4050S-5.5.0-2.11.rel AR3050S-5.5.0-2.11.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	08/2021	AR2050V-5.5.0-2.11.rel AR2010V-5.5.0-2.11.rel AR1050V-5.5.0-2.11.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.11 software version is ISSU compatible with previous software versions.

New Features and Enhancements

Enhanced ping polling for web authentication

Available on all platforms except: AR1050, AR2010, VAA, vFW, AMF container

With version 5.5.0-2.11, you can use ARP ping polling to check that a web authenticated supplicant (client device), is still connected.

A new command is available:

```
(no)auth-web-server ping-poll type {arp|ping}
```

Use this command to set the type of polling used to check that a web authenticated supplicant is still connected. The polling can be done using the default ICMP (ping) messages, or ARP messages. ARP polling works when a firewall is present, while ICMP does not. The polling will not start until ping-polling is enabled and the supplicant has been authorized.

For example, to set the polling type to ARP, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
awplus(config)# auth-web-server ping-poll type arp
```

For more information on the web-authentication and ping polling, see the AAA and Port Authentication Feature Overview and Configuration Guide.

Issues Resolved in Version 5.5.0-2.11

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	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71185	**AWC-Lite**	Previously, running **`enable traps`** in SNMP mode in AWC-Lite could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73260	**AWC-Lite**	Previously, the AWC-Lite security settings could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73261	**AWC-Lite**	Previously, the **`no wireless`** command could cause memory exhasution. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73263	**AWC-Lite**	Previously, the **`auto-config`** command could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73264	**AWC-Lite**	Previously, the **`show wireless auto-config`** command would cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73272	**AWC-Lite**	Previously, the **`wireless download ap`** and **`wireless power-channel ap`** commands could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73273	**AWC-Lite**	Previously, the **`debug wireless`** and **`show debug wireless`** commands could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73274	**AWC-Lite**	With this software update, the following error log messages are added for different types of incorrect AP configuration: ""WDS SSID not found"" ""VAP0 not found"" ""Hwtype does not support CB"" ""CB control VLAN not found"" ""CB key not found"" ""SC SSID not found"" ""SC key not found"" ""SC radio not found"" ""SC channel not found"" ""SC VAP not found"" ""Passpoint security must be WPA Enterprise"""	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73275	**AWC-Lite**	Previously, under rare circumstances, an AWC-Lite capable device could freeze when entering the **`no wireless`** command while the log transfer was still active. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73318	**AWC-Lite**	Previously, incorrect log messages were displayed with the following commands: ■ wireless power-channel ap ■ wireless ap-configuration apply app ■ wireless reset ap ■ wireless download ap This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73319	**AWC-Lite**	With this software update, the maximum captive portal is set to 12,000 rather than 50,000. Also, previously, a memory exhaustion could occur when the management address was applied to the AP. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73328	**AWC-Lite**	Previously, configuring the Channel Blanket eligible channel could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73419	**AWC-Lite**	With this software update, AWC-Lite capable devices can now perform configuration update, firmware upgrade and reboot to an AP without issue.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73446	**AWC-Lite**	Previously, products that support AWC-Lite had an incorrect passpoint value setting. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73577	**AWC-Lite**	Previously, MAC address filter import could cause the AWC-lite daemon to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73655	**AWC-Lite**	Previously, configuring wireless Passpoint could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	Y	Y	–
CR-73615	**Bootup**	Previously, on x510-DP series switches, unexpected errors occurred at startup if the PSU IDs failed to be read before the fan settings were updated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-73776	**Device Security**	With this software update, the command: **`show http`** will display a summary of the server certificate in use, including the SHA-1 and SHA-256 fingerprints. 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-54492	**DHCP Server**	This software update alters the DHCPv4 lease time calculation to avoid roll over errors on 64-bit OS systems when using -1(infinite) or large values for default DHCP lease time. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	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	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-68889	**DHCP Server**	Previously, the commands **`show ip dhcp binding`** and **`show ip dhcp pools`** were unable to process DHCP bindings that included malformed HW addresses and would display"Malformed statement" instead. 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-72171	**DPI**	Previously, a resource leak in DPI (with "provider procera") occurred when either: ■ DPI was disabled and then enabled or ■ when a new DPI resource was installed. The resource leak would start to impact operation after more than 125 iterations. This would require 2 to 3 years at the typical resource release interval. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR - 63798	**Environmental Monitoring**	Previously, the temperature sensor on x950 series and x908 GEN2 could occasionally reported an abnormal condition. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	–
CR-71996	**Hardware**	Previously, a "no xem" configuration line was being automatically added to the running configuration on x950-52XSQ and x950-52ATQm stacking setup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-73892	**IGMP**	Previously on Layer 3 capable devices with large numbers of multicast groups and sources, it was possible for the device to undergo a system reboot while updating multicast entries. 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-73836	**OpenVPN**	This CR resolves OpenVPN security vulnerability: https://nvd.nist.gov/vuln/detail/CVE-2020-15078	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70651	**Pluggable Transceivers**	Previously, 40G QSFP modules could fail to link up when configured as a network port. This issue has now been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	Y	Y	–	–	–	–	–
CR-72568	**Pluggable Transceivers**	Previously, there was an issue where 40G DAC cables could fail to negotiate a link correctly on insertion after the switch had booted up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	Y	Y	–	–	–	–	–
CR-71115	**PoE**	Previously, on IE300 and x320 series, some dual-signature PoE power devices would not draw the minimum DC current for a pair-set unless both pair-sets were powered up simultaneously, resulting in disconnection of the power devices. This issue has been resolved with a new parameter in the command: **`power-inline disconnect-defer`** <disconnect-defer-timeout> This causes the disconnect detection to be enabled 3 seconds after the default pair-set has been powered which gives the power devices enough time to draw power on both pair-sets. The disconnect detection timeout can also be configured longer than 3 seconds if requried. The command "(no) **`power-inline disconnect-defer`**" defers the DC disconnect detection in hardware. It is disabled by default. Some 60W PDs take longer than the 802.3at standard time for drawing the mimimum DC current on an individual pair. By defering the enabling of the DC disconnect logic it allows both sets of pairs to power up and start drawing current. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73223	**SD WAN**	Previously, when Vista Manager was used to configure SD WAN, in certain circumstances (such as tunnels going up and down) the device could consume excess memory, which could eventually cause the device to run out of memory and restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-73207	**SNMP**	Previously, MIB variable 'dot1xPaePortReauthenticate' was not working 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	–
CR-73799	**System**	Previously on very rare occasions an unexpected system re-start could occur. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-72516	**System Memory**	Previously the system free memory could gradually decrease with wireless ap-profile configurations. This issue been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	–	Y	Y	Y	Y	–
CR-73422	**Unicast Routing**	Previously, in certain complex routing situations, rebooting one device could cause another device to reboot as part of transient routing changes. This issue has been resolved. With this software update, the routing calculation has been improved to prevent this from happening. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-72608	**VCStack**	Previously, on rare occasions, a stack member might not join the stack correctly on a reboot or power cycle. 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	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73650	**VCStack**	Previously, it was possible for the stacked device to slowly consume memory over a long period of time (years). 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-73636	**Web Authentication**	Previously, the default web-auth-server ping-polling type was displayed in the running configuration. With this software update, it is removed. 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-73652	**Web Authentication**	With this software update, ARP polling packets for Web-Authentication has been changed from broadcast to unicast since broadcasting ARP polling for Web-Authentication could pose as a small security risk and is likely to have a greater network impact. 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	–

What's New in Version 5.5.0-2.9

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.9.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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		05/2021	vaa-5.5.0-2.9.iso (VAA OS) vaa-5.5.0-2.9. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.9.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	05/2021	SBx81CFC960-5.5.0-2.9.rel
SBx908 GEN2	SBx908 GEN2	05/2021	SBx908NG-5.5.0-2.9.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	05/2021	x950-5.5.0-2.9.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	05/2021	x930-5.5.0-2.9.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2021	x550-5.5.0-2.9.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	05/2021	x530-5.5.0-2.9.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	05/2021	x510-5.5.0-2.9.rel
IX5-28GPX	IX5	05/2021	IX5-5.5.0-2.9.rel
x320-10GH x320-11GPT	x320	05/2021	x320-5.5.0-2.9.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	05/2021	x310-5.5.0-2.9.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2021	x230-5.5.0-2.9.rel
x220-28GS x220-52GT x220-52GP	x220	05/2021	x220-5.5.0-2.9.rel
IE510-28GSX	IE510-28GSX	05/2021	IE510-5.5.0-2.9.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	05/2021	IE340-5.5.0-2.9.rel
IE300-12GT IE300-12GP	IE300	05/2021	IE300-5.5.0-2.9.rel
IE210L-10GP IE210L-18GP	IE210L	05/2021	IE210-5.5.0-2.9.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	05/2021	IE200-5.5.0-2.9.rel
XS916MXT XS916MXS	XS900MX	05/2021	XS900-5.5.0-2.9.rel
GS980EM/10H GS980EM/11PT	GS980EM	05/2021	GS980EM-5.5.0-2.9.rel
GS980M/52 GS980M/52PS	GS980M	05/2021	GS980M-5.5.0-2.9.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2021	GS970-5.5.0-2.9.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	05/2021	GS900-5.5.0-2.9.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	05/2021	FS980-5.5.0-2.9.rel
AR4050S AR3050S	AR-Series UTM firewalls	05/2021	AR4050S-5.5.0-2.9.rel AR3050S-5.5.0-2.9.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	05/2021	AR2050V-5.5.0-2.9.rel AR2010V-5.5.0-2.9.rel AR1050V-5.5.0-2.9.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.9 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.0-2.9

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	DC2552XS/L3	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73392	**ARP Neighbor Discovery**	Previously, ARPs could get stuck in the probe state if an ARP request with a new source MAC address kept arriving. 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-72946	**AWC-Lite**	Previously, a memory leak could occur when the **`administrative address`** command was entered. 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-72947	**AWC-Lite**	Previously, a memory leak could occur when Passpoint 3gpp-info was set on the Access Point. 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-73339	**CLI**	Previously, the **`show system fiber-monitoring`** command required user privilege level 15 to execute. With this software update, it has been reduced to level 7. 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-63798	**Environmental Monitoring**	Previously, the temperature sensor on x950 Series and x908 GEN2 could occasionally reported an abnormal condition. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–
CR-73364	**Multicast Fowarding**	Previously, in some multicast configurations, the processing of JOIN/LEAVE could result in memory depletion. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	DC2552XS/L3	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73456	**OpenFlow**	Previously, packets encapsulated with an 802.3 header (length instead of type) which were not using SNAP encapsulation, could cause hardware flows to be added which would match all Ethernet types, thus adversely affecting OpenFlow switching. This issue has been resolved.	–	Y	Y	Y	–	–	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–	Y	–	–	–	–	–
CR-71828	**PIM-SM Tunnel**	Previously, if PIM-SM or IGMP was configured on a tunnel before it had a valid ifindex or address, the configured commands would fail, and it was not possible for the software to dynamically recover from this issue. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71115	**PoE**	Previously, on IE300 and x320 Series, some dual-signature PoE power devices would not draw the minimum DC current for a pair-set unless both pair-sets were powered up simultaneously, resulting in disconnection of the power devices. The issue could occur when non-standard PDs, such as FLIR (Forward Looking InfraRed) cameras were used. This issue has been resolved by adding a new parameter to the command: **`power-inline disconnect-defer`** The command is now: **power-inline disconnect-defer [<disconnect-defer-timeout>]** For example: To enable disconnect deferral on port 1.0.9 , with a disconnect-defer-timeout of 2 seconds, use the commands: `awplus# configure terminal` `awplus(config)# interface port 1.0.9` `awplus(config-if)# power-inline disconnect-defer 2`	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	DC2552XS/L3	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-72497	**PoE**	With this software update, auto-negotiation is now enbled at 1G speed on the x930 Series switches. Also with this software update, auto-negotiation is enabled on SFP plus ports for the x310 Series.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-73068	**PoE**	Previously, power devices were not showing up as 'Powered' when HANP was disabled on the port but enabled globally on the device. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-73123	**PoE**	Previously, the SFP plus ports on x930 Series switches were not reflecting the speed/duplex/medium-type settings correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-72373	**Port Authentication**	Previously, when using MAC authentication, after a supplicant was successfully authenticated, if the link went down and came up, the supplicant had a short window of time (less than 1 second) where traffic it transmitted could still be forwarded into the network prior to the authentication process starting, when this traffic should have been discarded. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–
CR-73080	**Switching**	Previously, x950 Series and SBx908 GEN2 switches could suffer from frame losses after setting port speed back to the default value. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–
CR-73020	**VCStack**	Previously, resiliency link traffic could be dropped when the device CPU was congested. 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	–	–	–	–	–	–

What's New in Version 5.5.0-2.8

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.8.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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		05/2021	vaa-5.5.0-2.8.iso (VAA OS) vaa-5.5.0-2.8. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.8.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	05/2021	SBx81CFC960-5.5.0-2.8.rel
SBx908 GEN2	SBx908 GEN2	05/2021	SBx908NG-5.5.0-2.8.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	05/2021	x950-5.5.0-2.8.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	05/2021	x930-5.5.0-2.8.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2021	x550-5.5.0-2.8.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	05/2021	x530-5.5.0-2.8.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	05/2021	x510-5.5.0-2.8.rel
IX5-28GPX	IX5	05/2021	IX5-5.5.0-2.8.rel
x320-10GH x320-11GPT	x320	05/2021	x320-5.5.0-2.8.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	05/2021	x310-5.5.0-2.8.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2021	x230-5.5.0-2.8.rel
x220-28GS x220-52GT x220-52GP	x220	05/2021	x220-5.5.0-2.8.rel
IE510-28GSX	IE510-28GSX	05/2021	IE510-5.5.0-2.8.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	05/2021	IE340-5.5.0-2.8.rel
IE300-12GT IE300-12GP	IE300	05/2021	IE300-5.5.0-2.8.rel
IE210L-10GP IE210L-18GP	IE210L	05/2021	IE210-5.5.0-2.8.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	05/2021	IE200-5.5.0-2.8.rel
XS916MXT XS916MXS	XS900MX	05/2021	XS900-5.5.0-2.8.rel
GS980EM/10H GS980EM/11PT	GS980EM	05/2021	GS980EM-5.5.0-2.8.rel
GS980M/52 GS980M/52PS	GS980M	05/2021	GS980M-5.5.0-2.8.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2021	GS970-5.5.0-2.8.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	05/2021	GS900-5.5.0-2.8.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	05/2021	FS980-5.5.0-2.8.rel
AR4050S AR3050S	AR-Series UTM firewalls	05/2021	AR4050S-5.5.0-2.8.rel AR3050S-5.5.0-2.8.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	05/2021	AR2050V-5.5.0-2.8.rel AR2010V-5.5.0-2.8.rel AR1050V-5.5.0-2.8.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.8 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.0-2.8

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71948	**AMF**	Previously, after an AMF network topology change, it was possible in some situations for connectivity to some AMF nodes not to be restored. This issue has been resolved. Improvements have been made to the way AMF handles topology changes that involve changes to reachability between virtual and non-virtual links. 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-72657	**AMF**	Previously, removal of an AMF node could result in a bad entry in the AMF software table, causing disruption in 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	–
CR-70200	**CLI**	Previously, the output displayed for the command **`show interface`** for the field: 'Time since last change' could appear abnormal if the system was up for over 497 days. 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-72550	**CLI** **Tunnel**	Previously, recreating a tunnel interface immediately after it was deleted, could cause the device to restart unexpectedly. This issue has been resolved. Now, when trying to create a tunnel interface immediately after it is deleted, the action is ejected with the following message: "% IFNAME is currently being deleted, please try again".	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70872	**SSL**	This software update addresses the Transport Layer Security (TLS) connection vulnerability specified in CVE-2020-1968. 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-72656	**SSL**	This software update addresses multiple Secure Socket Layers (SSL) vulnerabilities specified in CVE-2020-1971, CVE-2021-23839, CVE-2021-23840 and CVE-2021-23841. 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	–
ER-4077	**Switching**	Enhancement: With this software update, x930 Series 1G pluggables ports no longer have difficulty linking up with some link partners.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-72369	**VCStack**	Previously, if one of the stack members hung, traffic from its ports could still cause learning events on the stack. However, as this member was no longer part of the stack, learning was not the correct thing to do. This issue has been resolved.	–	Y	Y	Y	Y	–	–	–	Y	Y	Y	–	–	Y	–	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-72470	**VCStack**	Previously, configuration could be falsely detected as mismatched on a late-joining stack member. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–

What's New in Version 5.5.0-2.7

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.7.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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		03/2021	vaa-5.5.0-2.7.iso (VAA OS) vaa-5.5.0-2.7. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.7.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2021	SBx81CFC960-5.5.0-2.7.rel
SBx908 GEN2	SBx908 GEN2	03/2021	SBx908NG-5.5.0-2.7.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	03/2021	x950-5.5.0-2.7.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2021	x930-5.5.0-2.7.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2021	x550-5.5.0-2.7.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2021	x530-5.5.0-2.7.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	03/2021	x510-5.5.0-2.7.rel
IX5-28GPX	IX5	03/2021	IX5-5.5.0-2.7.rel
x320-10GH x320-11GPT	x320	03/2021	x320-5.5.0-2.7.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2021	x310-5.5.0-2.7.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2021	x230-5.5.0-2.7.rel
x220-28GS x220-52GT x220-52GP	x220	03/2021	x220-5.5.0-2.7.rel
IE510-28GSX	IE510-28GSX	03/2021	IE510-5.5.0-2.7.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2021	IE340-5.5.0-2.7.rel
IE300-12GT IE300-12GP	IE300	03/2021	IE300-5.5.0-2.7.rel
IE210L-10GP IE210L-18GP	IE210L	03/2021	IE210-5.5.0-2.7.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2021	IE200-5.5.0-2.7.rel
XS916MXT XS916MXS	XS900MX	03/2021	XS900-5.5.0-2.7.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2021	GS980EM-5.5.0-2.7.rel
GS980M/52 GS980M/52PS	GS980M	03/2021	GS980M-5.5.0-2.7.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2021	GS970-5.5.0-2.7.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2021	GS900-5.5.0-2.7.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	03/2021	FS980-5.5.0-2.7.rel
AR4050S AR3050S	AR-Series UTM firewalls	03/2021	AR4050S-5.5.0-2.7.rel AR3050S-5.5.0-2.7.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	03/2021	AR2050V-5.5.0-2.7.rel AR2010V-5.5.0-2.7.rel AR1050V-5.5.0-2.7.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.7 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.0-2.7

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71969	**AWC-Lite**	This software update corrects the calculation method of BSSID for a Channel Blanket VAP.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	Y	Y	–
CR-72079	**AWC-Lite**	This software update adds two DSCP exceptions that are required for managing APs with the command **qos-map-set**.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	Y	Y	–
CR-72081	**AWC-Lite**	This software update adds validation for the following passpoint settings: ■ roaming-oi (Roaming Consortium List) ■ wan-metrics info HEX ■ operating-class HEX Invalid arguments are now rejected.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	Y	Y	–
CR-72108	**System**	Previously, on rare occasions, the SBx908GEN2 and x950 variant switches could restart unexpectedly due to a logic error in the code in the handling of packets received by the switch. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–
CR-72336	**L2TP, VRF-Lite**	Previously, when a VRF interface was deleted, nexthop entries in other VRFs could still be left with the reference to that interface, resulting in traffic not being forwarded correctly. 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	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-72205	**Logging**	Previously, on x510DP-28GTX and x510DP-52GTX models, an error was logged stating that the PWR250-80 (DC with front to back cooling) was not supported. This error has been removed and the PWR250-80 has been added to the list of supported PSUs for these platforms. Combining a PWR250-70 (AC) with a PWR250-80 (DC) is now an accepted configuration. In other words, you can have the PWR250 AC and DC versions together as long as they are both front to back cooling. An error will now be logged if the PSUs installed in an x510DP model have opposing airflows. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-72144	**Loop Protection VCStack**	Previously, network ports were linking up before the configuration was applied. This caused an internal system module on the different stacking nodes to go out of synchronisation, resulting in some CLI configuration failing to be executed. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-72068	**Pluggable Tranceivers**	Previously, PoE ports would not recover after they were disabled due to the voltage going below the minumum required value, even when the voltage returned to the stable state. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-70956	**Pluggable Transceivers**	Previously, with HANP enabled, the PoE LED remained on after rebooting and removing a legacy power device. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-70957	**Pluggable Transceivers**	Previously, a legacy power device showed a max power output of zero when connected and receiving power. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-72440	**Pluggable Transceivers**	Previously, pluggable ports sometimes would not linkup at startup due to configuration replay being run before the pluggables were configured. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-71532	**SMTP**	Previously, it was possible for the SMTP protocol to not process outgoing mail. 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-71524	**SNMP**	Previously, the version of the 'netsnmp package' was upgraded from v5.4.1 to v5.8. This introduced an error in the values the HOST-RESOURCES-MIB returned (1.3.6.1.2.1.25.2.3). This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-72319	**SSH**	With this software update, SSH connections in secure mode now allow AES-CTR, which is compatible with Linux SSH defaults. 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-71715	**Telnet**	Previously, the Telnet process could restart after receiving illegal Telnet 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	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-72262	**Telnet**	With this software update, an illegal Telnet packet no longer interrupts the operation of AlliedWare Plus devices. 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-72439	**User Management**	This software update addresses a vulnerability as stated in CVE-2021-3156 where 'sudo' may be exploited by local privileged users, resulting in heap-based buffer overflow. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-72606	**User Management**	This software update addresses the security vulnerability as stated in CVE-2020-14305, preventing unauthenticated remote users to cause an unexpected reboot of the system on H323 over IPv6 connection tracking. 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-72369	**VCStack**	Previously, if one of the stack members hung, traffic from its ports could still cause learning events on the stack. However, as this member was no longer part of the stack, learning was not the correct thing to do. This issue has been resolved.	–	Y	Y	Y	Y	Y	–	–	Y	Y	Y	–	–	Y	–	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–

What's New in Version 5.5.0-2.6

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.6.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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		03/2021	vaa-5.5.0-2.6.iso (VAA OS) vaa-5.5.0-2.6. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.6.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2021	SBx81CFC960-5.5.0-2.6.rel
SBx908 GEN2	SBx908 GEN2	03/2021	SBx908NG-5.5.0-2.6.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	03/2021	x950-5.5.0-2.6.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2021	x930-5.5.0-2.6.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2021	x550-5.5.0-2.6.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2021	x530-5.5.0-2.6.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	03/2021	x510-5.5.0-2.6.rel
IX5-28GPX	IX5	03/2021	IX5-5.5.0-2.6.rel
x320-10GH x320-11GPT	x320	03/2021	x320-5.5.0-2.6.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2021	x310-5.5.0-2.6.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2021	x230-5.5.0-2.6.rel
x220-28GS x220-52GT x220-52GP	x220	03/2021	x220-5.5.0-2.6.rel
IE510-28GSX	IE510-28GSX	03/2021	IE510-5.5.0-2.6.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2021	IE340-5.5.0-2.6.rel
IE300-12GT IE300-12GP	IE300	03/2021	IE300-5.5.0-2.6.rel
IE210L-10GP IE210L-18GP	IE210L	03/2021	IE210-5.5.0-2.6.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2021	IE200-5.5.0-2.6.rel
XS916MXT XS916MXS	XS900MX	03/2021	XS900-5.5.0-2.6.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2021	GS980EM-5.5.0-2.6.rel
GS980M/52 GS980M/52PS	GS980M	03/2021	GS980M-5.5.0-2.6.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2021	GS970-5.5.0-2.6.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2021	GS900-5.5.0-2.6.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	03/2021	FS980-5.5.0-2.6.rel
AR4050S AR3050S	AR-Series UTM firewalls	03/2021	AR4050S-5.5.0-2.6.rel AR3050S-5.5.0-2.6.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	03/2021	AR2050V-5.5.0-2.6.rel AR2010V-5.5.0-2.6.rel AR1050V-5.5.0-2.6.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.6 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.0-2.6

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-72193	**IPv4, IPv6**	Previously, if an IPv4 and IPv6 dual-stack enabled interface was brought down and then up, then IPv4 routing via the interface could fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

What's New in Version 5.5.0-2.5

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x510 Series
x510L Series
IX5-28GPX
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.5.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.

Caution: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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		03/2021	vaa-5.5.0-2.5.iso (VAA OS) vaa-5.5.0-2.5. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2021	SBx81CFC960-5.5.0-2.5.rel
SBx908 GEN2	SBx908 GEN2	03/2021	SBx908NG-5.5.0-2.5.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	03/2021	x950-5.5.0-2.5.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2021	x930-5.5.0-2.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2021	x550-5.5.0-2.5.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2021	x530-5.5.0-2.5.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	03/2021	x510-5.5.0-2.5.rel
IX5-28GPX	IX5	03/2021	IX5-5.5.0-2.5.rel
x320-10GH x320-11GPT	x320	03/2021	x320-5.5.0-2.5.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2021	x310-5.5.0-2.5.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2021	x230-5.5.0-2.5.rel
x220-28GS x220-52GT x220-52GP	x220	03/2021	x220-5.5.0-2.5.rel
IE510-28GSX	IE510-28GSX	03/2021	IE510-5.5.0-2.5.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2021	IE340-5.5.0-2.5.rel
IE300-12GT IE300-12GP	IE300	03/2021	IE300-5.5.0-2.5.rel
IE210L-10GP IE210L-18GP	IE210L	03/2021	IE210-5.5.0-2.5.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2021	IE200-5.5.0-2.5.rel
XS916MXT XS916MXS	XS900MX	03/2021	XS900-5.5.0-2.5.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2021	GS980EM-5.5.0-2.5.rel
GS980M/52 GS980M/52PS	GS980M	03/2021	GS980M-5.5.0-2.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2021	GS970-5.5.0-2.5.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2021	GS900-5.5.0-2.5.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	03/2021	FS980-5.5.0-2.5.rel
AR4050S AR3050S	AR-Series UTM firewalls	03/2021	AR4050S-5.5.0-2.5.rel AR3050S-5.5.0-2.5.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	03/2021	AR2050V-5.5.0-2.5.rel AR2010V-5.5.0-2.5.rel AR1050V-5.5.0-2.5.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.5 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new feature in 5.5.0-2.5:

Include a DNS search list in Router Advertisements

Available on: FS980M, GS900MX/MPX, GS70M, GS980M, XS900MX, x220, x230/x230L, x310, x510/x510L, x530 / x530L, x550, x930, x950, SBx908Gen2, SBx81CFC960, AR4050S, AR2050V/ AR2010V, AR3050S Series.

From version 5.5.0-2.5 onwards, you can specify a DNS Search List (DNSSL) to be included in the Router Advertisement for a given IPv6 interface.

The command and its option variations are:

- `ipv6 nd dns search-list <domain-name>`
- `no ipv6 nd dns search-list [<domain-name>|]`

where:

- *<domain-name>* – is a string specifying the domain name to be added to the search list, for example: myexample.com
- In the 'no' form, if no domain name is specified, then all domain names previously added will be deleted.

Example To add the domain 'myexample.com' to the search list, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 nd dns search-list myexample.com
```

To delete all domain names added previously, use the command:

```
awplus(config)# no ipv6 nd dns search-list
```

What's New in Version 5.5.0-2.4

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.4.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		02/2021	vaa-5.5.0-2.4.iso (VAA OS) vaa-5.5.0-2.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	02/2021	SBx81CFC960-5.5.0-2.4.rel
SBx908 GEN2	SBx908 GEN2	02/2021	SBx908NG-5.5.0-2.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	02/2021	x950-5.5.0-2.4.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	02/2021	x930-5.5.0-2.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	02/2021	x550-5.5.0-2.4.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	02/2021	x530-5.5.0-2.4.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	02/2021	x510-5.5.0-2.4.rel
IX5-28GPX	IX5	02/2021	IX5-5.5.0-2.4.rel
x320-10GH x320-11GPT	x320	02/2021	x320-5.5.0-2.4.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	02/2021	x310-5.5.0-2.4.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	02/2021	x230-5.5.0-2.4.rel
x220-28GS x220-52GT x220-52GP	x220	02/2021	x220-5.5.0-2.4.rel
IE510-28GSX	IE510-28GSX	02/2021	IE510-5.5.0-2.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	02/2021	IE340-5.5.0-2.4.rel
IE300-12GT IE300-12GP	IE300	02/2021	IE300-5.5.0-2.4.rel
IE210L-10GP IE210L-18GP	IE210L	02/2021	IE210-5.5.0-2.4.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	02/2021	IE200-5.5.0-2.4.rel
XS916MXT XS916MXS	XS900MX	02/2021	XS900-5.5.0-2.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	02/2021	GS980EM-5.5.0-2.4.rel
GS980M/52 GS980M/52PS	GS980M	02/2021	GS980M-5.5.0-2.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	02/2021	GS970-5.5.0-2.4.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	02/2021	GS900-5.5.0-2.4.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	02/2021	FS980-5.5.0-2.4.rel
AR4050S AR3050S	AR-Series UTM firewalls	02/2021	AR4050S-5.5.0-2.4.rel AR3050S-5.5.0-2.4.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	02/2021	AR2050V-5.5.0-2.4.rel AR2010V-5.5.0-2.4.rel AR1050V-5.5.0-2.4.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.4 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new feature in 5.5.0-2.4:

New IPv6 Router Advertisement options

Available on all platforms. ISSU: Effective when ISSU complete

From version 5.5.0-2.4 onwards, a new command has been introduced to provide more specific Router Information Options to Router Advertisements sent from a specific IPv6 interface.

The command and its option variations are:

- `ipv6 nd route-information <ipv6-prefix/length> [<0-4294967295>|infinity|default] [low|medium|high]`
- `ipv6 nd route-information <ipv6-prefix/length>`
- no `ipv6 nd route-information <ipv6-prefix/length>`
- no `ipv6 nd route-information all`

where:

- *<ipv6-prefix/length>* – the IPv6 network prefix and prefix length entered in dotted decimal format for the IPv6 network prefix, then slash notation for the IPv6 prefix length in the format X:X::X:X/ M, e.g. 2001:db8::/64
- `[<0-4294967295>|infinity|default]`
  - `<0-4294967295>` – the length of time in seconds (relative to the time the packet is sent) that the prefix is valid for route determination.
  - `infinity` – specifies that the route advertisement has an infinite lifetime.
  - `default` – is 3 * MaxRtrAdvInterval
- `[low|medium|high]` – the preference value for the route information.

Example To add a route 2001:DBB:1::/48 with a lifetime of 6000 and high preference, use the commands:

```
awplus# configure terminal
awplus(config)# int-vlan1
awplus(config-if)# ipv6 nd route-information 2001:DBB:1::/48
6000 high
```

- To delete the route information, use the command:

```
awplus(config-if)# no ipv6 nd route-information 2001:DBB:1::/48
```

- To delete all route information, use the command:

```
awplus(config-if)# no ipv6 nd route-information
```

Issues Resolved in Version 5.5.0-2.4

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-72072	**802.1x**	Previously, If the **`auth guest-vlan hw-forwarding`** feature was enabled, the device might restart unexpectedly when traffic from the guest was processed. 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-71400	**AMF Vista EX**	Previously, AlliedWare Plus was sending remote link and adjacent node information to Vista Manager when the link was disconnected, resulting in Vista EX incorrectly displaying the link as active. 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	–
ER-3518	**AMF Cloud**	Previously, a 'Connect' button was displayed on the AMF cloud ACS application after a web based shell session was terminated. With this software update, the Connect button has been removed. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-72040	**AWC-Lite**	Previously, when an AP profile was not set, i.e. at its default value or 'not bound', entering the command **`show wireless ap`**, to display the profile, could cause the device to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-72066	**Firewall, DPI**	With this software update, firewall rules will no longer make a different decision on ICMP packets when DPI is enabled.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71578	**IPsec**	Previously, IPsec remote authentication via the default trustpoint would not force the use of the trustpoint's root CA, but rather any configured trustpoints root CA. This issue has been resolved and IPsec now forces remote authentication via the default trustpoint to use the trustpoint's root CA.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71892	**IPsec**	Previously, IPsec tunnels could fail to receive updates from ISAKMP profile modifications in certain circumstances. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-71540	**IPsec**	Previously, trustpoint credentials loaded into IPsec would not be updated if a change was made. Now trustpoint credentials are reloaded into IPsec if a change is detected. Trustpoint profiles previously would still be used if a configured local or remote certificate failed to load, however with this change trustpoint profiles that fail to load a configured local or remote certificate are not used.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71731	**IPv6**	Previously, if multiple VLANs were configured, the device could fail to transmit Router Advertisements's in response to incoming router solicitations out on some VLANs 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-71762	**IPv4**	Previously, it was possible for an AlliedWare Plus device to use the wrong sender IP address if the port VLAN did not have any IP address assigned. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71830	**IPv6, Multicast routing**	Previously, IPv6 static multicast would not work with an IPv6 PIM license. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	Y	–	Y	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-70887	**Pluggable Transceivers, VCStack**	Previously, the AlliedTelesis device could falsely report link events on a stack port when its link partner was still in the process of linking up, resulting in link flapping when stack ports were about to link up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-72117	**Pluggable Transceivers**	Previously, for pluggable ports where no pluggable was present, the **storm-control** command could fail. This issue has been resolved. ISSU: Effective when ISSU complete.		–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-72015	**SD-WAN**	Previously, when SD-WAN was configured on an AMF master and managed by Vista Manager, there was potentially a memory leak on spoke routers that did not have SD-WAN configured. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71852	**Tunelling**	Previously, the **`remote authentication certificate`** command was not shown in the running-config, even it was configured. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70866	**USB Modem**	Previously after a reboot or power cycle some external USB modems would not always transition to link up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-71889	**Web API**	With the software update, rapidly destroying and recreating tunnels from the WebAPI is now more reliable. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70418	**Web-Control**	Previously,when using Web-Controller Antivirus in a high load network, it was possible for the proxy agent to not work properly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

What's New in Version 5.5.0-2.3

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.3.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		01/2021	vaa-5.5.0-2.3.iso (VAA OS) vaa-5.5.0-2.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	01/2021	SBx81CFC960-5.5.0-2.3.rel
SBx908 GEN2	SBx908 GEN2	01/2021	SBx908NG-5.5.0-2.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	01/2021	x950-5.5.0-2.3.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	01/2021	x930-5.5.0-2.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2021	x550-5.5.0-2.3.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	01/2021	x530-5.5.0-2.3.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	01/2021	x510-5.5.0-2.3.rel
IX5-28GPX	IX5	01/2021	IX5-5.5.0-2.3.rel
x320-10GH x320-11GPT	x320	01/2021	x320-5.5.0-2.3.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	01/2021	x310-5.5.0-2.3.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2021	x230-5.5.0-2.3.rel
x220-28GS x220-52GT x220-52GP	x220	01/2021	x220-5.5.0-2.3.rel
IE510-28GSX	IE510-28GSX	01/2021	IE510-5.5.0-2.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	01/2021	IE340-5.5.0-2.3.rel
IE300-12GT IE300-12GP	IE300	01/2021	IE300-5.5.0-2.3.rel
IE210L-10GP IE210L-18GP	IE210L	01/2021	IE210-5.5.0-2.3.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	01/2021	IE200-5.5.0-2.3.rel
XS916MXT XS916MXS	XS900MX	01/2021	XS900-5.5.0-2.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	01/2021	GS980EM-5.5.0-2.3.rel
GS980M/52 GS980M/52PS	GS980M	01/2021	GS980M-5.5.0-2.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2021	GS970-5.5.0-2.3.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	01/2021	GS900-5.5.0-2.3.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	01/2021	FS980-5.5.0-2.3.rel
AR4050S AR3050S	AR-Series UTM firewalls	01/2021	AR4050S-5.5.0-2.3.rel AR3050S-5.5.0-2.3.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	01/2021	AR2050V-5.5.0-2.3.rel AR2010V-5.5.0-2.3.rel AR1050V-5.5.0-2.3.rel

Caution: Software version 5.5.0-2.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-2.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.3 software version is ISSU incompatible with previous software versions.

New Features and Enhancements

This section summarizes the new features in 5.5.0-2.3:

Web Redirect in proxy chaining mode

Available on AR4050S, AR3050S, AR2050V, and AR2010V Series

From version 5.5.0-2.3 onwards, you can configure Web Redirect in **proxy** chaining mode. Web Redirect in proxy chaining mode, forwards all HTTP/HTTPS traffic to an upstream explicit proxy server. You can add exclusions to the web-redirect rules for this mode, namely, exclusions by DPI applications and by URL regular expressions. Valid excluded DPI and URL traffic is sent directly to the Internet.

Enterprises use the feature by utilizing a proxy server to handle additional security processing of their network traffic. The feature can exempt low security risk traffic from additional security processing and send it directly to the Internet, reducing the load on the proxy server. There are two exclusion commands available: **exclude app** and **exclude url**.

Example First set Web Redirect in **proxy** chaining mode and configure a **proxy-host**:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# mode proxy
awplus(config-web-redirect)# proxy-host <ip-address> port
<port-number>
```

- To configure a DPI application exclusion on Skype traffic, use the command:

```
awplus(config-web-redirect)# exclude app skype
```

- To configure a URL exclusion on Microsoft traffic, use the command:

```
awplus(config-web-redirect)# exclude url .microsoft.com
```

With the above two examples, traffic identified as **skype** or meant for **.microsoft.com** is sent directly on to the Internet.

For more information on Web Redirect in proxy chaining mode, see the Web Redirect Feature Overview and Configuration Guide.

Configure SSH server to use only best-current-practice key exchange algorithms

Available on AlliedWare Plus devices

From version 5.5.0-2.3 onwards, the AlliedWare Plus SSH server has been modified to allow users to specify only key exchange algorithms which are consistent with key exchange algorithms currently considered as best-current-practice to be used by the SSH server and the algorithm list does not include diffie-hellman-group-exchange-sha1 key exchange algorithm.

The new command is as follows:

```
awplus(config)#(no) ssh server secure-kex
```

Specifying the command will result in the following key exchange algorithms being used by the AlliedWare Plus SSH server:

- curve25519-sha256@libssh.org,
- ecdh-sha2-nistp521
- ecdh-sha2-nistp384
- ecdh-sha2-nistp256
- diffie-hellman-group-exchange-sha256

The **show ssh server** command output has also been modified to show the current ciphers in use.

For example:

```
awplus(config)#show ssh server

Secure Shell Server Configuration
-----------------------------------------------------------------------------
SSH Server : Disabled
Protocol : None
Port : 22
Version : 2,1
Services : scp, sftp
User Authentication : publickey, password
Resolve Hosts : Disabled
Session Timeout : 0 (Off)
Login Timeout : 60 seconds
Maximum Authentication Tries : 6
Maximum Startups : 10
Debug : NONE
Ciphers : aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
KEX : curve25519-sha256@libssh.org,
                                        ecdh-sha2-nistp521,ecdh-sha2-nistp384,
                                        ecdh-sha2-nistp256,
                                        diffie-hellman-group-exchange-sha256 "
```

Reducing IGMP hardware entries

Available on XS900MX, FS980, GS900MX, GS980M, GS980MX, x320, x530, x530L, x550, x930, x950, SBx8100 CFC960, and SBx908 GEN2 Series.

From version 5.5.0-2.3 onwards, a new multicast command is available:

```
ip igmp flood-group
```

This command adds an all sources multicast entry into the switches multicast hardware table to flood multicast packets to all ports within the VLAN without mirroring the traffic to the CPU. This significantly reduces the number of hardware entries consumed.

To configure an IGMP flooding group to L2 ports only use the following commands. This will flood any UDP packet to group 239.255.255.250 to all ports in vlan1.

```
awplus(config)#int vlan1
awplus(config-if)#ip igmp flood-group 239.255.255.250
```

For more information on IGMP flooding, see the IGMP/MLD Feature Overview and Configuration Guide.

Issues Resolved in Version 5.5.0-2.3

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70673	**AMF Application-Proxy**	Previously, after a blocked device was removed from a quarantine VLAN, attempting to return the device to the quarantine VLAN could fail. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–
CR-71653	**AMF Application-Proxy**	Previously, adding two **`application-proxy`** commands could result in a device restart due to the software referencing a null pointer. 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-71559	**AMF Application-Proxy, Tri Authentication**	Previously, an unhelpful debug log message was generated if a user tried to set a quarantine action on a quarantine VLAN. This log has been replaced with a more useful message. This issue has been resolved.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-70758	**AMF Cloud (VAA)**	This software change contains several efficiency improvements when very large numbers of AMF containers (>295) are created. Additionally, previously when large numbers of AMF containers were created it was possible for AMF application-proxy to have an unexpected re-boot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-71400	**AMF Vista EX**	Previously, AlliedWare Plus was sending remote link and adjacent node information to Vista Manager when the link was disconnected, resulting in Vista EX incorrectly displaying the link as active. 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	–
CR-70656	**BFD**	Previously BFD echo mode was not inter-operating correctly with some other switch vendors. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71654	**CLI**	Previously, on the x530L-10GHXm, in the command **`show system environment`** CLI 'Fan 2' was reporting the fan speed for the fan physically connected to the FAN3 port, and 'Fan 3' was reporting the FAN2 speed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-71504	**CWM, Web API**	Previously, the API version in ap_profiles was incorrect, resulting in the Web API being unable to be accessed via the expected path. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-70998	**Device GUI, HTTP Service, Web API**	Previously, it was possible to download certain files from the device over HTTPS without authorization if the: ■ HTTP service was enabled ■ AlliedWare Plus Device GUI was not installed on the device. 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	–
CR-70704	**DHCP Client IPv6**	Previously, a state change, either an IPv6 address being removed, or configuration changing, could cause the IPv6 prefix to no longer be advertised. This issue has been resolved.	Y	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-70921	**DHCP Client IPv6**	Previously, when a DHCPv6 client had been assigned with a prefix by an upstream DHCPv6 server, and the server changed the prefix assignment to a different prefix, resetting the upstream interface could cause the default route via the upstream server to disappear. This issue has been resolved.	Y	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71037	**DHCP Client IPv6**	Previously, a DHCPv6-PD client configured with the **`default-route-to-server`** command might end up with multiple default routes, after the upstream link went down and up again accompanied by a change of DHCP server. As a result, the default route with the nexthop of the previous DHCP server would fail to be withdrawn. 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-71616	**DHCPv6 Client, IPv6**	Previously, if an AlliedWare Plus DHCP client received a reply with status code of "NoBinding" after sending a "REBIND", then it would keep using the assigned address until expiry. This meant that the server pool could have been renumbered without doing a RECONFIGURE, or the server could have been replaced by a new server with a different address pool, but the client would not be updated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-71129	**DHCPv6 Prefix Delegation**	Previously, when a DHCPv6-PD client was running on an interface (connected to the PD server), if: ■ the interface went down and up multiple times ■ and the PD server assigned different prefixes resulting in a DHCPv6 rebind and reply packets exchanges, then occasionally the NSM module could undergo an unexpected re-boot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–
CR-71215	**DHCPv6 Prefix Delegation**	Previously, if a DHCP-PD client received prefix-delegations for a new prefix with lifetimes of 0, the AlliedWare Plus management daemon could restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69890	**Firewall - IPS**	Previously some active FTP connections could not be tracked by IPS with its default built-in rules. This issue has been resolved by introducing a new IPS category that specifically tracks active FTP connections.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70309	**IGMP Snooping**	Previously, packets destined to the IPv4 all-routers address could have been incorrectly blocked in hardware after IGMP snooping was disabled and re-enabled. 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	–
CR-71578	**IPsec**	Previously, IPsec remote authentication via the default trustpoint would not force the use of the trustpoint's root CA, but rather any configured trustpoints root CA. This issue has been resolved and IPsec now forces remote authentication via the default trustpoint to use the trustpoint's root CA.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71194	**IPv6 Tunnel**	Previously, for source IPv6 prefix selection, MAP-E used to select the first IPv6 prefix found that was in the vendor accepted range. With this software update, MAP-E now, in addition to checking the vendor accepted range, prefers undeprecated IPv6 prefixes over deprecated IPv6 prefixes for source IPv6 prefix selection. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71387	**IPv6 Tunnel**	Previously, MAP-E used to request map rules in a loop when multiple upstream IPv6 prefixes were used. This issue has been resolved. With this software update, it now uses the most valid address, based on if it is deprecated or not.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71540	**ISAKMP**	Previously, trustpoint credentials loaded into IPsec would not be updated if a change was made. Now trustpoint credentials are reloaded into IPsec if a change is detected. Trustpoint profiles previously would still be used if a configured local or remote certificate failed to load, however with this change trustpoint profiles that fail to load a configured local or remote certificate are not used.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70911	**MAC Authentication**	Previously, If a supplicant was authorized on a port and dynamically assigned as a tagged member of a VLAN, the tagged VLAN was not being removed from the port even after the supplicant was unauthorized then reauthorized onto a different tagged VLAN. This prevented an LLDP-MED device from using a different voice VLAN until the switch was rebooted. This issue has been resolved.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-70068	**MLDv2 IGMPv3**	Previously L2 and L3 multicast hardware entries on some switch platforms could be unexpectedly removed in MLDv2 or IGMPv3 networks when the command **`platform l2mc-overlap`** was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-71023	**MRP**	Previously, MRP could incorrectly set up port state machine transitions resulting in MRP clients remaining in blocking state on startup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-70789	**Multicast routing**	Previously the error log "*No more free mll pairs*" could be generated frequently due to a slight mis-match between the software and hardware MLL table limit on some LIFs. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70937	**Multicast Routing**	Previously, shadow multicast routes were not aged out on VCStack backup members, which had the potential to cause "*multicast table full*" errors following a failover. This issue has been resolved by enabling ageing on multicast routes for VCStack backup members.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-70910	**Pluggable Tranceivers**	Previously, switchport LEDs on the SBx81CFC960v2 were not being lit when the port links up when set to "auto 1-000". This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-70983	**Pluggable Transceivers**	Previously, when using the SP10TM pluggable at 5 / 2.5 Gbps on an AT-SBx81XLEM/XS8 or AT-x530(/DP/L) SFP+ port, the amount of traffic forwarded was slightly lower than line-rate. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–
CR-71019	**Pluggable Transceivers**	Previously, the SP10TM was not operating correctly at 5Gbps or 2.5Gbps on some platforms. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-71084	**Pluggable Transceivers**	Previously the AT-SPTXc could sometimes not link up after a hot-swap on the x530 Series. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-70687	**PoE**	Previously, on an IE300 switch, it was possible for the PoE state reported by the various GUIs did not reflect the configured state. This issue has been resolved.	–	–	–	–	–	–	–	–	–		–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59904	**PoE**	Previously, the IE300 could not power some 60W PoE cameras due to differences in pre-802.3bt standard implementations. Now, you can use the command **`power-inline disconnect-defer`** to power these devices correctly. This command defers the DC disconnect detection in hardware. Some 60W PDs take longer than the 802.3at standard time for drawing the minimum DC current on an individual pair. By deferring the enabling of the DC disconnect logic it allows both sets of pairs to power up and start drawing current.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-70641	**PoE**	Previously, 'Legacy Mode' on the FS980M was displayed as 'disabled' despite being enabled by default. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-70936	**PoE**	Previously, legacy setting did not apply to a stack member when it joined the stack or a LIF when it came up in an x8100 chassis. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	Y	–	–	–	Y	–	–	–	–	–	–	–
CR-70785	**Policy Based Routing (PBR)**	Previously when **`match tcp-flag`** was set in a class-map, any PBR nexthops within the same policy-map may not have been automatically resolved when matching traffic flows through the device. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–	–
CR-70923	**Port Authentication**	Previously, application of a dynamic VLAN by port authentication would not work if that VLAN was preceded by a user named VLAN in the VLAN database. This issue only occurred if the two VLANs had consecutive VIDs. This issue has been resolved.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70388	**Private VLAN MLD Snooping**	Previously an error message - for example: "*DBG:hsl_hw_impl_l2_add_fdb 1802: Could not add MC MAC. ifx 5002 3333.ff9d.e1cb vid 2*" could be generated when IPv6 multicast traffic was received on a member port of a private VLAN on which MLD snooping was enabled. 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-70672	**Routing**	Previously, if a connected route was down (for example due to the VLAN interface being shut down) and was replaced by a route from a routing protocol, then when the VLAN came back up the connected route could fail to be reinstated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-70899	**SSH Server**	The AlliedWare Plus SSH server has been modified to allow users to specify only key exchange algorithms which are consistent with key exchange algorithms currently considered as best-current-practice to be used by the SSH server. There is a new command available to configure this feature: **(no) ssh server secure-kex** Note: The algorithm list does not include the diffie-hellman-group-exchange-sha1 key exchange algorithm.	Y	Y	Y	Y	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-71468	**Tunnel**	Previously, after changing the IP address on a tunnel, traffic was not being forwarded. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70866	**USB Modem**	Previously after a reboot or power cycle some external USB modems would not always transition to link up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71514	**VCStack**	Previously, a VCStack could fail to form if 5Gbps speed was configured on an interface used for stacking. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–

What's New in Version 5.5.0-2.2

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.2.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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		12/2020	vaa-5.5.0-2.2.iso (VAA OS) vaa-5.5.0-2.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	12/2020	SBx81CFC960-5.5.0-2.2.rel
SBx908 GEN2	SBx908 GEN2	12/2020	SBx908NG-5.5.0-2.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	12/2020	x950-5.5.0-2.2.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	12/2020	x930-5.5.0-2.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	12/2020	x550-5.5.0-2.2.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	12/2020	x530-5.5.0-2.2.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	12/2020	x510-5.5.0-2.2.rel
IX5-28GPX	IX5	12/2020	IX5-5.5.0-2.2.rel
x320-10GH x320-11GPT	x320	12/2020	x320-5.5.0-2.2.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	12/2020	x310-5.5.0-2.2.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	12/2020	x230-5.5.0-2.2.rel
x220-28GS x220-52GT x220-52GP	x220	12/2020	x220-5.5.0-2.2.rel
IE510-28GSX	IE510-28GSX	12/2020	IE510-5.5.0-2.2.rel
IE340-20GP IE340L-18GP	IE340	12/2020	IE340-5.5.0-2.2.rel
IE300-12GT IE300-12GP	IE300	12/2020	IE300-5.5.0-2.2.rel
IE210L-10GP IE210L-18GP	IE210L	12/2020	IE210-5.5.0-2.2.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	12/2020	IE200-5.5.0-2.2.rel
XS916MXT XS916MXS	XS900MX	12/2020	XS900-5.5.0-2.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	12/2020	GS980EM-5.5.0-2.2.rel
GS980M/52 GS980M/52PS	GS980M	12/2020	GS980M-5.5.0-2.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	12/2020	GS970-5.5.0-2.2.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	12/2020	GS900-5.5.0-2.2.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	12/2020	FS980-5.5.0-2.2.rel
AR4050S AR3050S	AR-Series UTM firewalls	12/2020	AR4050S-5.5.0-2.2.rel AR3050S-5.5.0-2.2.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	12/2020	AR2050V-5.5.0-2.2.rel AR2010V-5.5.0-2.2.rel AR1050V-5.5.0-2.2.rel

Caution: Software version 5.5.0-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-1.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.2 software version is ISSU incompatible with previous software versions.

Issues Resolved in Version 5.5.0-2.2

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70704	**DHCP Client IPv6**	Previously, a state change, either an IPv6 address being removed, or configuration changing, could cause the IPv6 prefix to no longer be advertised. 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	–
CR-70921	**DHCP Client IPv6**	Previously, when a DHCPv6 client had been assigned with a prefix by an upstream DHCPv6 server, and the server changed the prefix assignment to a different prefix, resetting the upstream interface could cause the default route via the upstream server to disappear. 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-71037	**DHCP Client IPv6**	Previously, a DHCPv6-PD client configured with the **`default-route-to-server`** command might end up with multiple default routes, after the upstream link went down and up again accompanied by a change of DHCP server. As a result, the default route with the nexthop of the previous DHCP server would fail to be withdrawn. 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	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71194	**IPv6 Tunnel**	Previously, for source IPv6 prefix selection, MAP-E used to select the first IPv6 prefix found that was in the vendor accepted range. With this software update, MAP-E now, in addition to checking the vendor accepted range, prefers undeprecated IPv6 prefixes over deprecated IPv6 prefixes for source IPv6 prefix selection. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71387	**IPv6 Tunnel**	Previously, Map-E requested map rules in an unnecessary repeating cycle when multiple upstream IPv6 prefixes were used. With this software update, it now uses the most valid address, based on if it is deprecated or not.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

What's New in Version 5.5.0-2.1

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-2.1.

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: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 107.

For instructions on how to update the web-based GUI, see "Accessing the Web-based GUI on Switches" on page 109 or "Accessing the Web-based GUI on AR-Series Devices" on page 111. 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		11/2020	vaa-5.5.0-2.1.iso (VAA OS) vaa-5.5.0-2.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-2.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2020	SBx81CFC960-5.5.0-2.1.rel
SBx908 GEN2	SBx908 GEN2	11/2020	SBx908NG-5.5.0-2.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	11/2020	x950-5.5.0-2.1.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2020	x930-5.5.0-2.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2020	x550-5.5.0-2.1.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GTX x530L-52GPX x530L-28GTX x530L-28GPX	x530 and x530L	11/2020	x530-5.5.0-2.1.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	11/2020	x510-5.5.0-2.1.rel
IX5-28GPX	IX5	11/2020	IX5-5.5.0-2.1.rel
x320-10GH x320-11GPT	x320	11/2020	x320-5.5.0-2.1.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2020	x310-5.5.0-2.1.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2020	x230-5.5.0-2.1.rel
x220-28GS x220-52GT x220-52GP	x220	11/2020	x220-5.5.0-2.1.rel
IE510-28GSX	IE510-28GSX	11/2020	IE510-5.5.0-2.1.rel
IE340-20GP IE340L-18GP	IE340	11/2020	IE340-5.5.0-2.1.rel
IE300-12GT IE300-12GP	IE300	11/2020	IE300-5.5.0-2.1.rel
IE210L-10GP IE210L-18GP	IE210L	11/2020	IE210-5.5.0-2.1.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2020	IE200-5.5.0-2.1.rel
XS916MXT XS916MXS	XS900MX	11/2020	XS900-5.5.0-2.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2020	GS980EM-5.5.0-2.1.rel
GS980M/52 GS980M/52PS	GS980M	11/2020	GS980M-5.5.0-2.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2020	GS970-5.5.0-2.1.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2020	GS900-5.5.0-2.1.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	11/2020	FS980-5.5.0-2.1.rel
AR4050S AR3050S	AR-Series UTM firewalls	11/2020	AR4050S-5.5.0-2.1.rel AR3050S-5.5.0-2.1.rel
AR2050V AR2010V AR1050V	AR-Series VPN routers	11/2020	AR2050V-5.5.0-2.1.rel AR2010V-5.5.0-2.1.rel AR1050V-5.5.0-2.1.rel

Caution: Software version 5.5.0-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-1.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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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

The 5.5.0-2.1 software version is ISSU incompatible with previous software versions.

New Products

Version 5.5.0-2.1 supports the following upcoming and recently-released products.

x950-52XSQ Expandable 10G/40G/100G Stackable Layer 3+ Switches

Supported since 5.5.0-1.1

These switches have 48 x 1/10G SFP+ ports, 4 x 40G/100G uplink ports. They are designed to be a powerful local or distributed core solution.

Key features include:

- Large switching and routing tables support multiple services and connected devices
- VCStack up to 8 units locally or over distance for a resilient network core
- Autonomous Management Framework (AMF) for network automation
- SDN for network intelligence with OpenFlow v 1.3

For more information, see our website at www.alliedtelesis.com/products/switches/x950-52xsq.

New Features and Enhancements

This section summarizes the new features in 5.5.0-2.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 102.

Autonomous Management Framework (AMF) Enhancements

The Allied Telesis Autonomous Management Framework (AMF) is a suite of features that combine to simplify network management across all supported network equipment from the core to the edge.

AMF provides simplified device recovery and firmware upgrade management, enables you to manage your entire network from any AlliedWare Plus node within the network, enables you to configure multiple devices simultaneously, and makes it easy to add new devices into the network.

Version 5.5.0-2.1 includes the following AMF enhancements.

AMF Cloud support for VMware vSphere Hypervisor(ESXi) 7.0

Available on AMF Cloud

From version 5.5.0-2.1 onwards, AMF Cloud is supported on VMware vSphere Hypervisor (ESXi) version 7. This means AMF Cloud is now supported on the following Virtual Machine (VM) environments:

- VMware vSphere Hypervisor (ESXi) 6.0, 6.5, 6.7, and 7.0.
- Citrix XenServer 6.5
- Microsoft Hyper-V

For more information on supported VM environments and server specifications, see the AMF Cloud Datasheet.

For more information on AMF, AMF secure mode, and AMF links, see the AMF Feature Overview and Configuration Guide.

BFD - Rapid detection of communication failures

Available on x930 Series

From version 5.5.0-2.1 onwards, you can configure the Bi-direction Forwarding Detection (BFD) service on x930 Series devices.

BFD is a standards based protocol initially defined in RFC 5880, whose sole purpose is to detect communication failure between two devices quickly and efficiently. Allied Telesis' BFD implementation supports Layer three protocols and is based on the RFC.

This is how it works

BFD is a simple Hello protocol that, in many respects, is similar to the detection components of well-known routing protocols. A pair of systems transmit BFD packets periodically over each path between the two systems, and if a system stops receiving BFD packets for long enough, some component in that particular bidirectional path to the neighboring system is assumed to have failed.

- A path is only declared to be operational when two-way communication has been established between systems, though this does not preclude the use of unidirectional links.
- A separate BFD session is created for each communications path and data protocol in use between two systems.
- Each system estimates how quickly it can send and receive BFD packets in order to come to an agreement with its neighbor about how rapidly detection of failure will take place.

This implementation of BFD is interoperable with implementations of RFC 5880 from other manufacturers. BFD is also used by an existing feature - Border Gateway Protocol (BGP). A BGP neighbor can be registered with BFD so that a peer session is created which will listen for BFD events and ask BGP to shutdown its neighbor connection immediately if the peer session goes down. Even though BFD is responsible for detecting failures, BGP can use this information and make routing decisions independently.

For more information about how to configure the BFD service, see the BFD for Routing Protocols Feature Overview and Configuration Guide.

Media Redundancy Protocol (MRP)

Available on IE340, IE340L, IE510, and x930 Series switches.

From 5.5.0-2.1 onwards, you can use Media Redundancy Protocol (MRP) to provide redundancy in Ethernet networks via a ring.

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

Ethernet technology does not allow physical loops, as they cause packets to circulate endlessly and overload the network. This means providing media redundancy within an Ethernet network requires the use of a protocol that is able to monitor and resolve the physical loops introduced by redundant pathways. This protocol must ensure that, even with multiple physical pathways to any device, only one is activated at any one time and the remaining are in standby mode. This is achieved by:

- monitoring links,
- detecting interruptions, and
- switching to an alternative path in the event of failure as soon as possible.

Media Redundancy Protocol (MRP) is a protocol for providing redundancy in Ethernet networks via a ring. MRP is specified for ring networks with up to 50 devices. It guarantees fully predictable switch-over behavior. Varying parameter sets are available, with worst-case switch-over times being 500, 200, 30, or 10ms.

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

Link Monitoring SNMP MIB

Available on all AlliedWare Plus devices

From version 5.5.0-2.1 onwards, you can use a new SNMP MIB called AT- LINKMON-MIB. This MIB provides you with link monitoring information on the health of a link, especially probes and probe history used for reporting link metrics.

Objects in this group have the object identifier **atLinkMon** { modules 606 } OID 1.3.6.1.4.1.207.8.4.4.4.606.

For more information on all objects in this group see the Support for Allied Telesis Enterprise MIBs in AlliedWare Plus Technical Guide.

VLAN-based Q-in-Q support on x530 Series switches

Added on x530 Series. Previously available on SBx8100 Series.

Version 5.5.0-2.1 supports VLAN ID translation and VLAN double-tagging (Q-in-Q) on the same port for the x530 Series switches.

VLAN translation used together with VLAN double-tagging is used to create a Layer 2 connection between two locations. Service providers use VLAN translation and VLAN double-tagging to transport customers traffic across their network even if they are using overlapping VLANs. They can also bundle customer VLANs over a single transport VLAN.

For more information about VLAN double-tagging and VLAN translation on the same port, see the VLANs Feature Overview and Configuration Guide.

Authentication Priority for Tri-authentication

Available on all devices that support tri-authentication

From version **5.5.0-2.1** onwards, you can set the order of priority for tri-authentication. Tri-authentication is when multiple authentication methods (MAC, 802.1X, and/or web-based) are configured on the same interface. With tri-authentication, a supplicant is authorized to use the network as soon as they are successfully authenticated by any of the configured authentication methods.

When authentication priority is not set, once a supplicant is authenticated any future attempts to authenticate are ignored. When, however, authentication priority is set, and a higher priority authentication attempt is made by the supplicant, a new authentication process starts. The supplicant will then be authorized, or unauthorized, based on the result of this new authentication attempt.

Giving 802.1X a higher priority than MAC authentication could be useful, for example, in the following scenario.

- A supplicant is authorized on a network using MAC authentication.
- This allows the supplicant to receive the information required to initiate an 802.1X authentication attempt.
- The supplicant is then authorized, or unauthorized, based on the result of this 802.1X authentication attempt.

To configure 802.1X authentication to have a higher priority than MAC authentication on interface port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth priority dot1x auth-mac
```

For more information on tri-authentication and setting the order of priority see the AAA and Port Authentication Feature Overview and Configuration Guide.

Storm control enhancement on x220 and GS980M Series switches

From 5.5.0-2.1 onwards, you can set more than one storm control limit type at a time for x220 and GS980M Series switches. For example, you can configure both broadcast and multicast levels on the same port at the same time.

For more information about storm control, see the Switching Feature Overview and Configuration Guide.

Fan noise reduction for x530 and x530L Series switches

From 5.5.0-2.1 onwards, fans on x530 and x530L Series switches run slower at a given temperature or PoE power consumption, for quieter operation.

Disabling the ONM service if unused

Available on all AlliedWare Plus devices that support G.8032 and Connectivity Fault Management (CFM)

From 5.5.0-2.1 onwards, you can disable the ONM service (which underlies CFM and G.8032) if you are not using CFM and G.8032. Disabling the service can reduce memory usage on the switch, particularly when many VLANs are configured on ports.

To disable the service, use the commands:

```
awplus# configure terminal
awplus(config)# no service onm
```

The ONM service is enabled by default. Disabling it will only take effect after you save the configuration and restart the device.

OpenVPN support on AR1050V VPN Routers

From version 5.5.0-2.1 onwards, OpenVPN is supported on AR1050V devices.

AlliedWare Plus OpenVPN is an SSL/TLS-based application used for creating a secure connection from a remote client to a central site. It establishes an encrypted and authenticated tunnel between the client and server and uses that tunnel for transporting traffic across intervening networks. AlliedWare Plus OpenVPN provides a full Data Link Layer access, proven standards-based SSL/TLS authentication and encryption, and implicit firewall/NAT traversal.

AlliedWare Plus OpenVPN is built on a solid and industry-tested security foundation and is very easy to use. It offers you the flexibility to work in a variety of modes that are easy to understand and hard to make insecure.

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

Improvement to handling of Intrusion Prevention System (IPS) alerts

Available on AR4050S, AR3050S, AR2050V, AR2010V and AR1050V

From 5.5.0-2.1 onwards, the AR-Series firewalls and VPN routers will produce a maximum of 6 IPS alerts per minute per destination IP address. This prevents IPS alerts from overwhelming the log files.

If you need to log every packet that matches an IPS rule (for example, for debugging purposes), you can use the following commands to turn the limit off:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no alert-thresholding
```

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.0-x.x and may affect your device or network behavior if you upgrade:

- VCStack compatibility
- Upgrade compatibility for SBx908 GEN2 and x950 Series switches
- Changes that may affect device or network configuration

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

- Software release licensing
- Upgrading a VCStack with rolling reboot - read this if stacking x530 Series switches
- 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 5.5.0-x.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.4.9-1.x version, please check the 5.4.9-2.x release note. Release notes are available from our website, including:

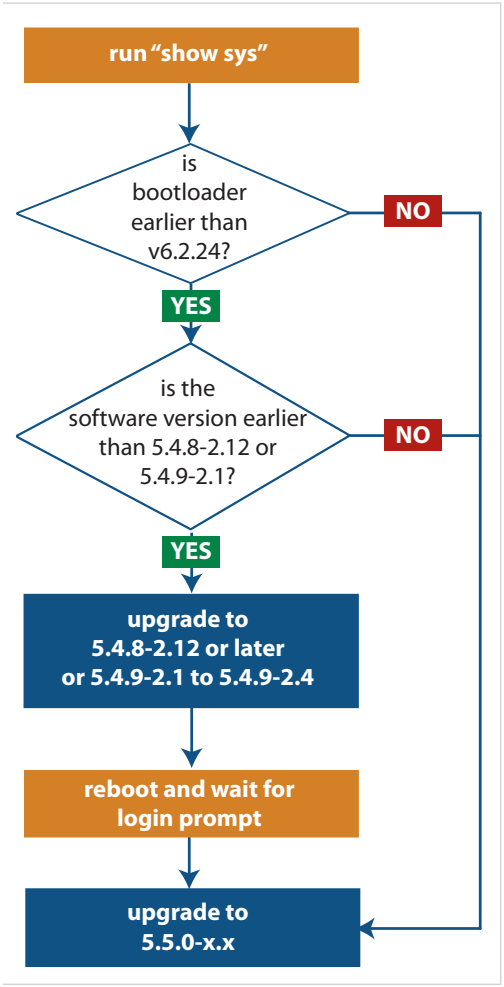
- 5.4.9-x.x release notes
- 5.4.8-x.x release notes
- 5.4.7-x.x release notes
- 5.4.6-x.x release notes

VCStack compatibility

There are restrictions on which software versions you can use rolling reboot with, and restrictions in how to form a new VCStack or add new members to a stack. For details, see "Upgrading a VCStack with rolling reboot" on page 98 and "Forming or extending a VCStack with auto-synchronization" on page 99.

Upgrade compatibility for SBx908 GEN2 and x950 Series switches

On the SBx908 GEN2 and x950 Series switches, please check your bootloader and current software version before you upgrade to AlliedWare Plus version 5.5.0-x.x.



If your bootloader is older than 6.2.24, you can only upgrade to 5.5.0-x.x from the following software versions:

- 5.4.8-2.12, 5.4.8-2.13 or later, or
- 5.4.9-2.1, 5.4.9-2.2, 5.4.9-2.3 or 5.4.9-2.4, or
- any older 5.5.0-x.x version

If your bootloader is older than 6.2.24, your switch must be running one of the above versions when you upgrade to 5.5.0-x.x.

If your bootloader is older than 6.2.24, you cannot upgrade to 5.5.0-x.x directly from:

- **5.4.9-1.x,**
- **5.4.9-0.x, or**
  any version before 5.4.8-2.12

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

```
awplus# show system
```

If you experience issues when upgrading, please contact your Allied Telesis support team. See our website at alliedtelesis.com/support.

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

Changes to port authentication with threat protection.	*All AlliedWare Plus devices*	From version 5.5.0-2.1, you cannot change the port authentication configuration of an interface if that interface has a **quarantine** threat protection action configured on it. Before changing the interface's authentication configuration you must either:
		■ remove the interface's threat protection configuration, or
		■ shutdown the interface.
		
		This affects the following commands, all of which change the authentication configuration on an interface:
		■ **dot1x port-control**,
		■ **auth-mac**,
		■ **auth-web**, and
		■ **application-proxy whitelist enable**
		
		If you attempt to change the authentication configuration on an interface that has threat protection quarantine configured, you will see the following error message:
		`% portx.x.x: Application Proxy quarantine configuration must be removed before port authentication is changed`
		
		To shutdown an interface, use the following commands:
		`awplus# configure terminal`
		`awplus(config)# interface portx.x.x`
		`awplus(config-if)# shutdown`
		
		To remove threat protection from an interface, use the following commands:
		`awplus# configure terminal`
		`awplus(config)# interface portx.x.x`
		`awplus(config-if)# no application-proxy threat-protection`
		
		Threat protection and quarantine actions are configured with the AMF Security product. For more information on AMF Security see the AMF Security Technical Documents.

Summary	Affected devices	Detail
The **copy current-software** command has been removed from the CLI	*All AlliedWare Plus devices*	From version 5.5.0-2.1, the **copy current-software** command has been removed from the CLI. This command copied the running AlliedWare Plus software (i.e. the software the device had booted from) to a destination file. You can instead copy the software from external media (USB/SD card) or by using TFTP/SCP/FTP etc.
In AWC lite, the first character of the AP username must be a letter	*All devices that support Vista Manager mini in the Device GUI*	When using AWC lite, from 5.5.0-2.1 onwards, the first character of the AP username must be a letter. This affects the command: `awplus(config-wireless-ap)#login username <name>` Previously this command incorrectly accepted a number.
VLAN Statistic commands removed from x220, x320 and x530 Series switches	*x220, x320 and x530 Series switches*	From 5.5.0-1.1 onwards, the following commands have been removed from the x220, x320 and x530 Series switches: ■ vlan statistics ■ clear vlan statistics ■ show vlan statistics The commands were removed because the VLAN statistics feature is not available on these products.
Storm Control is improved for large packets	*SBx908 GEN2, x950, x930, x550, x510, x310, x230, XS900MX, GS900MX/MPX, and GS970M Series switches*	The command **storm-control {broadcast|multicast|dlf} level** enables you to limit broadcast, multicast or DLF packets to a percentage of line speed. From 5.5.0-0.1 onwards, this command applies the specified percentage in the same way for packets of all sizes. Previously, larger packets would take more bandwidth than expected. You may need to adjust your specified levels to allow for the changed functionality.
diffie-hellman-group1-sha1 is removed as an SSH key exchange algorithm	*All AlliedWare Plus devices*	From 5.5.0-0.1 onwards, diffie-hellman-group1-sha1 has been removed as an SSH key exchange algorithm option. If you are using a legacy SSH client, you may need to upgrade your client.
Provisioned ports can't be accessed using MODBUS	*All AlliedWare Plus devices that support MODBUS*	Provisioned ports are no longer accessible using MODBUS.
In Secure Mode, devices reboot if they fail to initialize a critical service	*All AlliedWare Plus devices that support Secure Mode*	From 5.5.0-0.1 and 5.4.9-2.3 onwards, in Secure Mode, failure while initializing a critical service will cause the device to reboot.

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.0 license on your switch if you are upgrading to 5.5.0-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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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 5.5.0-2.x from:

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

On these switches, you **cannot** use rolling reboot to upgrade to 5.5.0-2.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 5.5.0-2.x from:

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

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

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

On these switches, auto-synchronization is not supported between 5.5.0-2.x and any version earlier than 5.5.0-0.x.

For CFC960 cards on 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 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 different 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 5.5.0-2.x and:

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

- 5.5.0-1.x
- 5.5.0-0.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 5.5.0-2.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, all nodes must run 5.4.9-0.1 or later.

If using none of the above

If none of the above apply, then nodes running version 5.5.0-2.x are compatible with nodes running:

- 5.5.0-1.x
- 5.5.0-0.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 Feature Guides in the right-hand menu.
- **Datasheets** - find these by searching for the product series and then selecting Datasheets in the right-hand menu.
- **Installation Guides** - find these by searching for the product series and then selecting Installation Guides in the right-hand menu.
- **Command References** - find these by searching for the product series and then selecting Manuals in the right-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 checksum of the release file with the correct checksum for the file. The correct checksum is listed 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 checksum. For example, all x930 Series switches have the same checksum.

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

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                   : 5.5.0
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2021
License expiry date            : N/A
Release                        : 5.5.0
```

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                   : 5.5.0
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2021
License expiry date            : N/A
Release                        : 5.5.0
```

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 103 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 105.

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 SBx8100-5.5.0-2.12.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.0-2.12.rel`
x950 series	`awplus(config)# boot system x950-5.5.0-2.12.rel`
x930 series	`awplus(config)# boot system x930-5.5.0-2.12.rel`
x550 series	`awplus(config)# boot system x550-5.5.0-2.12.rel`
x530 series	`awplus(config)# boot system x530-5.5.0-2.12.rel`
x510 series	`awplus(config)# boot system x510-5.5.0-2.12.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.5.0-2.12.rel`
x320 series	`awplus(config)# boot system x320-5.5.0-2.12.rel`
x310 series	`awplus(config)# boot system x310-5.5.0-2.12.rel`
x230 series	`awplus(config)# boot system x230-5.5.0-2.12.rel`
x220 series	`awplus(config)# boot system x220-5.5.0-2.12.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.5.0-2.12.rel`

Product	Command
IE340 series	`awplus(config)# boot system IE340-5.5.0-2.12.rel`
IE300 series	`awplus(config)# boot system IE300-5.5.0-2.12.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.0-2.12.rel`
IE200 series	`awplus(config)# boot system IE200-5.5.0-2.12.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.0-2.12.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.0-2.12.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.0-2.12.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.0-2.12.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.5.0-2.12.rel`
FS980M series	`awplus(config)# boot system FS980-5.5.0-2.12.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.0-2.12.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.0-2.12.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.5.0-2.12.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.0-2.12.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.0-2.12.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 the Web-based GUI on Switches

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 SBx908 GEN2 switches, x950 Series, x930 Series, x550 Series and x530 Series, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

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

   Alternatively, you can use the default address on unconfigured devices, which is 169.254.42.42.

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 About page in the GUI and check the field called **GUI version**. The version to use with 5.5.0-2.12 is 2.9.0.

If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 112.

Update the GUI if it is not the latest version

Perform the following steps through the 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 v2.9.0 of the GUI is awplus-gui_550_24.gui.

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

2. Copy the file into Flash memory on your switch. You can copy the file into Flash using any of the following methods:

   - TFTP server
   - USB Flash drive
   - SD card

   For example, to copy the v2.9.0 GUI file from your USB Flash drive, use the following commands:

   ```
   awplus>enable
   awplus#copy usb awplus-gui_550_24.gui flash
   ```

   To view all files in Flash and check that the newly installed file is there, use the following command:

   ```
   awplus#dir
   ```

3. Stop and restart the HTTP service:

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

4. 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*.

Accessing the Web-based GUI on AR-Series Devices

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

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 AR4050S, AR3050S, AR2050V and AR2010V devices, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

Browse to the GUI

Perform the following steps to browse to the GUI.

Prerequisite: 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.

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

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

   Alternatively, you can use the default address on unconfigured devices, which is 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 **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.0-2.12 is 2.9.0. If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 112.

Update the GUI if it is not the latest version

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

1. Use the following command to download and install the GUI:

```
awplus# update webgui now
```

2. Stop and restart the HTTP service:

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

3. 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.