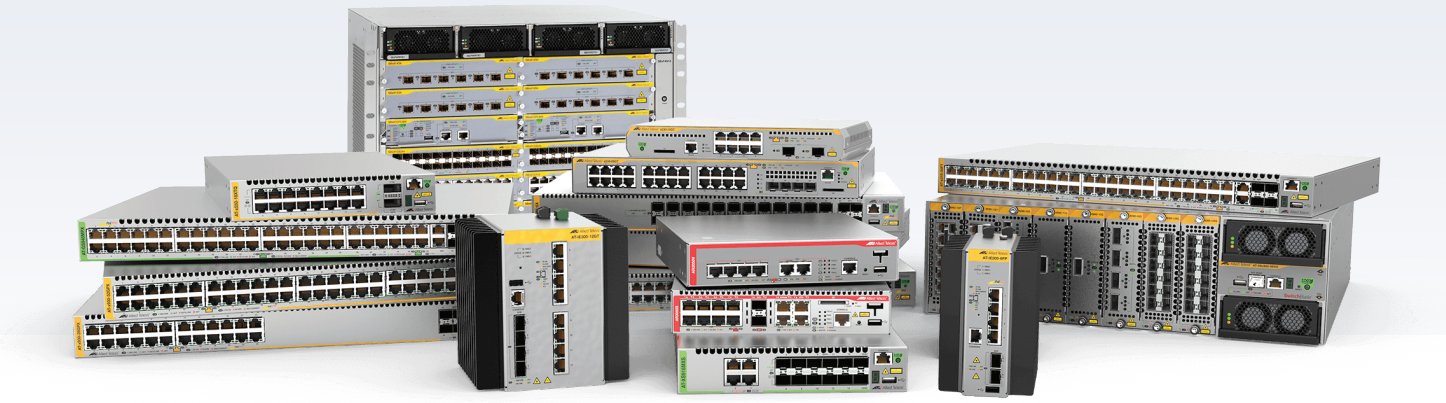
Release Note for AlliedWare Plus Software Version 5.5.0-0.x



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

» 5.5.0-0.1 » 5.5.0-0.3 » 5.5.0-0.4 » 5.5.0-0.5 » 5.5.0-0.6

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 5.5.0-0.6

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 5.5.0-0.6.

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 67.

For instructions on how to update the web-based GUI, see "Installing and accessing the Web-based GUI on switches" on page 69 or "Installing and accessing the Web-based GUI on AR-Series devices" on page 72. 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		08/2020	vaa-5.5.0-0.6.iso (VAA OS) vaa-5.5.0-0.6 vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-0.6.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2020	SBx81CFC960-5.5.0-0.6.rel
SBx908 GEN2	SBx908 GEN2	08/2020	SBx908NG-5.5.0-0.6.rel
x950-28XSQ x950-28XTQm	x950	08/2020	x950-5.5.0-0.6.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2020	x930-5.5.0-0.6.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2020	x550-5.5.0-0.6.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	08/2020	x530-5.5.0-0.6.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	08/2020	x510-5.5.0-0.6.rel
IX5-28GPX	IX5	08/2020	IX5-5.5.0-0.6.rel
x320-10GH	x320	08/2020	x320-5.5.0-0.6.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2020	x310-5.5.0-0.6.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	08/2020	x230-5.5.0-0.6.rel
x220-28GS x220-52GT x220-52GP	x220	08/2020	x220-5.5.0-0.6.rel
IE510-28GSX	IE510-28GSX	08/2020	IE510-5.5.0-0.6.rel
IE340-20GP IE340L-18GP	IE340	08/2020	IE340-5.5.0-0.6.rel
IE300-12GT IE300-12GP	IE300	08/2020	IE300-5.5.0-0.6.rel
IE210L-10GP IE210L-18GP	IE210L	08/2020	IE210-5.5.0-0.6.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2020	IE200-5.5.0-0.6.rel
XS916MXT XS916MXS	XS900MX	08/2020	XS900-5.5.0-0.6.rel
GS980EM/10H	GS980EM	08/2020	GS980EM-5.5.0-0.6.rel
GS980M/52 GS980M/52PS	GS980M	08/2020	GS980M-5.5.0-0.6.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2020	GS970-5.5.0-0.6.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2020	GS900-5.5.0-0.6.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	08/2020	FS980-5.5.0-0.6.rel
AR4050S AR3050S	AR-series UTM firewalls	08/2020	AR4050S-5.5.0-0.6.rel AR3050S-5.5.0-0.6.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	08/2020	AR2050V-5.5.0-0.6.rel AR2010V-5.5.0-0.6.rel AR1050V-5.5.0-0.6.rel

Caution: Software version 5.5.0-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.0 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. 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 63 and
- "Licensing this version on an SBx8100 Series CFC960 control card" on page 65.

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

The 5.5.0-0.6 software version is ISSU compatible with previous software versions.

Issues resolved in version 5.5.0-0.6

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-69767	**AMF**	Previously, a very unusual combination of AMF provisioning commands left the file system pointing to a non-existent directory. As a result, when AMF backup was performed, AMF became confused attempting to locate the non-existent directory. This software update addresses the issue by ensuring the AMF backups return to the home directory before initiating the backup.. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y
CR-69942	**AMF**	Previously, a transition from an active amf-link to an amf-cross-link on active ports would not work. 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-69557	**ARP** **Neighbor Discovery**	Previously, multicast traffic with a TTL value of "1" could be incorrectly reflected out a trunk port configured for NLB. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	Y	–	Y	Y	–	–	Y	Y	–	Y	Y	–	–	Y	–	–	–	–	–
CR-63424	**Device Security**	This software update addressed the Linux security vulnerability issue outlined in CVE-2019-11068 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-65671	**Device Security**	This software update addressed the OpenSSL security vulnerability issue outlined in CVE-2019-1563. 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	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-65672	**Device Security**	This software update addressed the TFTP and FTP security vulnerability issue outlined in CVE-2019-5481 and CVE-2019-5482 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-66034	**Device Security**	This software update addressed the HTTP security vulnerability issue outlined in CVE-2019-17420 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-68475	**Device Security**	This software update addressed the HAProxy loadbalancing security vulnerability issue outlined in CVE-2020-11100 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-69946	**Flow Control**	Previously, ports connected to a SPTx pluggable could link up even if disabled. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–
CR-69373	**MAC Thrashing**	Previously, MAC entries could randomly get deleted from some SBx8100 line cards running on the same chassis while traffic was flowing, resulting in unnecessary unicast traffic flooding. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-69506	**MAC Thrashing Trigger**	Previously, if thrash-limiting with action **`vlan-disable`** on aggregators as well as the findme trigger were both configured, port LEDs could sometimes continue to flash indefinitely if ports linked down while thrash-limiting was active. This issue has been resolved. ISSU: Effective when ISSU complete.	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-68468	**RADIUS**	This software update addressed the radius security vulnerability issue outlined in CVE-2019-17185 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-70115	**SNMP**	Previously, SNMP information was unable to be obtained by IPv6. 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-67464	**SSH DOS Detection**	Previously, when IPS was enabled, every packet that matched a drop rule would result in an alert message being logged. As a result, under DoS condition, SSH was unresponsive because the device was busy logging. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70026	**VCStack**	Previously, there was a small chance that if a stack member left the stack and rebooted in less than a minute, then the remote mounts for the rebooted stack node would not be added properly. 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-69760	**Web API**	Previously, the CPU load value in the device GUI on AlliedWare+ devices could show a different value to the values shown on the CLI. This was due to a difference in the way that the values were calculated. 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	–

What's new in version 5.5.0-0.5

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
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 5.5.0-0.5.

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

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 67.

For instructions on how to update the web-based GUI, see "Installing and accessing the Web-based GUI on switches" on page 69 or "Installing and accessing the Web-based GUI on AR-Series devices" on page 72. 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		08/2020	vaa-5.5.0-0.5.iso (VAA OS) vaa-5.5.0-0.5. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-0.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2020	SBx81CFC960-5.5.0-0.5.rel
SBx908 GEN2	SBx908 GEN2	08/2020	SBx908NG-5.5.0-0.5.rel
x950-28XSQ x950-28XTQm	x950	08/2020	x950-5.5.0-0.5.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2020	x930-5.5.0-0.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2020	x550-5.5.0-0.5.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	08/2020	x530-5.5.0-0.5.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	08/2020	x510-5.5.0-0.5.rel
IX5-28GPX	IX5	08/2020	IX5-5.5.0-0.5.rel
x320-10GH	x320	08/2020	x320-5.5.0-0.5.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2020	x310-5.5.0-0.5.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	08/2020	x230-5.5.0-0.5.rel
x220-28GS x220-52GT x220-52GP	x220	08/2020	x220-5.5.0-0.5.rel
IE510-28GSX	IE510-28GSX	08/2020	IE510-5.5.0-0.5.rel
IE340-20GP IE340L-18GP	IE340	08/2020	IE340-5.5.0-0.5.rel
IE300-12GT IE300-12GP	IE300	08/2020	IE300-5.5.0-0.5.rel
IE210L-10GP IE210L-18GP	IE210L	08/2020	IE210-5.5.0-0.5.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2020	IE200-5.5.0-0.5.rel
XS916MXT XS916MXS	XS900MX	08/2020	XS900-5.5.0-0.5.rel
GS980EM/10H	GS980EM	08/2020	GS980EM-5.5.0-0.5.rel
GS980M/52 GS980M/52PS	GS980M	08/2020	GS980M-5.5.0-0.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2020	GS970-5.5.0-0.5.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2020	GS900-5.5.0-0.5.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	08/2020	FS980-5.5.0-0.5.rel
AR4050S AR3050S	AR-series UTM firewalls	08/2020	AR4050S-5.5.0-0.5.rel AR3050S-5.5.0-0.5.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	08/2020	AR2050V-5.5.0-0.5.rel AR2010V-5.5.0-0.5.rel AR1050V-5.5.0-0.5.rel

Caution: Software version 5.5.0-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.0 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. 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 63 and
- "Licensing this version on an SBx8100 Series CFC960 control card" on page 65.

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

The 5.5.0-0.5 software version is ISSU compatible with previous software versions.

Issues resolved in version 5.5.0-0.5

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-68760	**802.1x**	Previously, the force-authorization option for port AUTH could fail if the port was configured for dot1x and eapol v2. 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-68868	**AMF**	Previously, AMF backup and recovery could fail due to an incorrect permission set on some directories. 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-69350	**AMF**	Previously, when an AMF guest link was configured on a port that already had an AMF link configured, the AMF process could restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-69722	**AMF**	Previously, an AMF guest node could be reset (i.e. leave and then re-join the AMF network) with every LLDP neighbour information update. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-69834	**ARP Neighbor Discovery**	Previously, clearing ipv6 neighbours did not remove dynamically learned 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	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-69141	**ARP** **Neighbor Discovery** **VCStack**	Previously, it was possible for NLB traffic to be dropped after a stack master failover. This issue has been resolved.	–	–	Y	Y	Y	–	–	–	–	–	–	Y	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-68555	**Auto-negotiation**	Previously, it was possible for an x530 variant switch to not detect a port speed change when the link-partner renegotiated the link speed down to 100M (on 2.5G or 5G ports). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-69062	**AWC-lite**	Previously, the AWC-Lite task status was not updated after the AWC-Lite daemon re-initialised. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	Y	Y	Y	–
CR-69714	**BGP**	Previously, when redistributing IPv4 OSPF or RIP routes with route tags attached into other routing protocols, the tag was not included as part of the redistribution. This prevented route-maps from being able to filter these tagged routes. This issue has been resolved. Now, any routes with tags attached will have the tag preserved when redistributing into a protocol, allowing route-maps to filter those tagged routes. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-69174	**EPSR**	Previously, a truncated EPSR packet on the EPSR control VLAN could result in ESPR failing to process the EPSR control VLAN packets, resulting in a broken EPSR ring. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-68869	**IGMP**	Previously, when jumbo frames support was enabled on a switch, it was possible for IGMP snooping to cause the switch to unexpectedly restart. 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-69048	**Ipv6 Multicast Forwarding**	With this software update, the handling of Layer 3 multicast learning has been improved. 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-68774	**IPv6 Tunneling**	Previously, in a mixed configuration of MAP-E, (for example involving dual redundant IPv6 transition tunnels), MAP-E would not work correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-69158	**IPv6 Tunneling**	Previously, the MAP-E mesh-mode could fail to process locally destined packets correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-69392	**IPv6 Tunneling**	Previously, MAP-E could trigger multiple requests to the map rule server. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-69422	**IPv6 Tunneling**	Previously, a long IPv6 address (for example without containing double colons representing contiguous zeros) could fail to be added to the tunnel interface configuration. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-69706	**Layer 3 Switching**	Previously, Layer 3 tables were not configured correctly and could report being full before they actually were. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–
CR-68737	**Logging**	Previously, the log facility command did not work after the 5.5.0-0.1 software release. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-68757	**Logging** **Hardware Health Monitoring**	Previously, on GS900MX and XS900 variant switches, there was a very small chance that a spurious voltage alarm could be raised. This issue has been resolved. Now, when an alarm is detected for voltage sensors, the value is rechecked before raising an alarm. Additionally, on 5.5.0 and newer releases, counters have been added for environment sensors. The counters provide an additional level of diagnostics for hardware/ environmental issues. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-68301	**MLD** **Multicast Routing**	Previously, a large number of IGMP or MLD traffic streams could cause a x930 variant switch to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-69815	**Multicast Forwarding**	Previously, after a dynamic channel group went down, and then up again, the multicast traffic over the aggregator link would not recover. This issue has been resolved.	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-67405	**NTP**	Previously, when NTP detected a time difference and changed the system clock internally, it was possible for this to affect some internal messaging within the device, resulting in an internal communication failure error message to be logged. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-69087	**PIM**	Previously, multicast replication on the source VLAN was not handled correctly. This issue has been resolved. ISSU: Effective when ISSU complete.	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-68321	**Pluggable Transceivers**	Previously, a 10G fiber pluggable would not link up when used in a XEM2-12XSv1 XEM on a x950 variant switch. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-69401	**Pluggable Transceivers**	Previously, the SP10T pluggable would not link up on an x950 variant switch. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-66988	**PoE** **Port Configuration**	Previously, the port mapping configuration of PoE ports was not correct. This issue has been resolved. Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-68523	**PoE** **Web API**	Previously, PoE service was incorrectly activated on non-PoE devices when PoE was enabled using the command: **`service power-inline`**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	Y	Y	–	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-69201	**Port Configuration**	Previously, the XEM2-4QS XEM module could fail to initialize after it was inserted into an x950 variant switch if the breakout mode was configured. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-69322	**SNMP**	With this software update, MIB support for GP24v2 LIF for SBx81CFC960v2 is added. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-69788	**SNMP**	Previously, when using SNMP discovery with some devices, it was possible for the process to lock up. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	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-68471	**SNMP VCStack**	Previously, changing the PVID of a port on a backup member could result in MAC address table entries for the previous VLAN not being deleted from the MAC address table. 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-60459	**SSH**	This software update addresses the OpenSSH user enumeration vulnerability as described in CVE-2018-15473. I 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-69105	**SSH**	With this software update, the SSH server has been modified to selectively allow only secure ciphers which are consistent with ciphers currently offered by OpenSSH by default, and does not include CBC ciphers. The new command as part of this implementation is: **`(no)ssh server secure-ciphers`** In addition, the **`show ssh server`** command output has also been modified to show the current ciphers in use. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69398	**SSH**	From software version 5.4.9-2.1 onwards, there was an issue where the SSH client would only negotiate the hmac-sha1 algorithm for hash-based message authentication code. This issue has been resolved. Now, the SSH client by default will negotiate the following algorithms for HMAC: ■ umac-64-etm@openssh.com ■ umac-128-etm@openssh.com ■ hmac-sha2-256-etm@openssh.com ■ hmac-sha2-512-etm@openssh.com ■ hmac-sha1-etm@openssh.com ■ umac-64@openssh.com ■ umac-128@openssh.com ■ hmac-sha2-256 ■ hmac-sha2-512 ■ hmac-sha1 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-67464	**SSH DOS Detection**	Previously, when IPS was enabled, every packet that matched a drop rule would result in an alert message being logged. As a result, under DoS conditions, SSH was unresponsive because the device was busy logging. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-67808	**VCStack**	Previously, configuration replay could sometimes fail for a late joining stack member. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	Y	–	–	–	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	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-68318	**VCStack**	Previously, interface state changes could sometimes cause audit inconsistencies on a stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	Y	Y	–	–	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR-68316	**VCStack** **VRF-lite**	Previously, when there was a large number of VLANs and VRFs configured on a stack, the configuration could occasionally fail to synchronise across the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR-69622	**VLAN**	Previously, it was possible to configure several VLAN translation statements with the same defined internal VLAN on a single port. With this software update, this is no longer allowed, and will result in an error message being displayed. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	Y	Y	–	–	–	–	–	–	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR-69812	**VLAN**	With this software update, adding multiple VLAN stacking rules on the same port is now possible. 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-69703	**Web API**	Previously, when using the Web API, it was possible for some data to become corrupted when doing SETs or POSTs. This could cause invalid configuration or GETs to not work and could potentially cause the HTTP server to restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

Enhancements in version 5.5.0-0.5

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
ER-3539	**SNMP**	With this software update, a new entry "atFiberMonLastReading" has been added to the state table in the at-fiber-monitoring MIB at .1.3.6.1.4.1.207.8.4.4.3.27.3.1.9. This entry returns the last reading read by fiber-monitoring on an interface as an integer. Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-3543	**CLI** **Router High Availability**	With this software update, it is now possible to manually activate the bypass mode of WAN interfaces on the AR4050S, AR3050S, and AR2050V Series by using the CLI. When the bypass mode is activated, the bypass relay electrically disconnects the cable plugged into the WAN port and reconnects it to the bypass port. This allows the WAN cable to be fed through to another device. This feature is useful if you want to make use of WAN Bypass Ports but do not want to use VRRP. Bypass mode is deactivated by default. Bypass mode can be activated by entering Interface Mode and for the WAN interface and using the **wan-bypass** command. Example: `awplus(config)#` interface eth1 `awplus(config-if)#` wan-bypass ■ Bypass mode can be deactivated by entering Interface Mode for the WAN interface and using the **no wan-bypass** command. ■ If bypass mode for a WAN interface has been activated manually it is not possible to associate it with a VRRP instance. Bypass mode must be manually deactivated first. ■ Similarly, it is not possible to manually activate bypass mode if the WAN interface is currently associated with a VRRP instance. To manually control bypass mode, remove the association from the VRRP instance using the **no ha associate** command.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–

What's new in version 5.5.0-0.4

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 5.5.0-0.4.

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 67.

For instructions on how to update the web-based GUI, see "Installing and accessing the Web-based GUI on switches" on page 69 or "Installing and accessing the Web-based GUI on AR-Series devices" on page 72. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		06/2020	vaa-5.5.0-0.4.iso (VAA OS) vaa-5.5.0-0.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-0.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	06/2020	SBx81CFC960-5.5.0-0.4.rel
SBx908 GEN2	SBx908 GEN2	06/2020	SBx908NG-5.5.0-0.4.rel
x950-28XSQ x950-28XTQm	x950	06/2020	x950-5.5.0-0.4.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	06/2020	x930-5.5.0-0.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2020	x550-5.5.0-0.4.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	06/2020	x530-5.5.0-0.4.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	06/2020	x510-5.5.0-0.4.rel
IX5-28GPX	IX5	06/2020	IX5-5.5.0-0.4.rel
x320-10GH	x320	06/2020	x320-5.5.0-0.4.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	06/2020	x310-5.5.0-0.4.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	06/2020	x230-5.5.0-0.4.rel
x220-28GS x220-52GT x220-52GP	x220	06/2020	x220-5.5.0-0.4.rel
IE510-28GSX	IE510-28GSX	06/2020	IE510-5.5.0-0.4.rel
IE340-20GP IE340L-18GP	IE340	06/2020	IE340-5.5.0-0.4.rel
IE300-12GT IE300-12GP	IE300	06/2020	IE300-5.5.0-0.4.rel
IE210L-10GP IE210L-18GP	IE210L	06/2020	IE210-5.5.0-0.4.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2020	IE200-5.5.0-0.4.rel
XS916MXT XS916MXS	XS900MX	06/2020	XS900-5.5.0-0.4.rel
GS980EM/10H	GS980EM	06/2020	GS980EM-5.5.0-0.4.rel
GS980M/52 GS980M/52PS	GS980M	06/2020	GS980M-5.5.0-0.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2020	GS970-5.5.0-0.4.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2020	GS900-5.5.0-0.4.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	06/2020	FS980-5.5.0-0.4.rel
AR4050S AR3050S	AR-series UTM firewalls	06/2020	AR4050S-5.5.0-0.4.rel AR3050S-5.5.0-0.4.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	06/2020	AR2050V-5.5.0-0.4.rel AR2010V-5.5.0-0.4.rel AR1050V-5.5.0-0.4.rel

Caution: Software version 5.5.0-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.0 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. 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 63 and
- "Licensing this version on an SBx8100 Series CFC960 control card" on page 65.

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

The 5.5.0-0.4 software version is ISSU compatible with previous software versions.

Issues resolved in version 5.5.0-0.4

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-68843	**Device GUI**	Previously, the output formatting of the CLI shell did not have proper line spacing. With this software update, the output formatting of the CLI shell in the Device GUI is now correct. 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	–

What's new in version 5.5.0-0.3

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
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 5.5.0-0.3.

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

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 67.

For instructions on how to update the web-based GUI, see "Installing and accessing the Web-based GUI on switches" on page 69 or "Installing and accessing the Web-based GUI on AR-Series devices" on page 72. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		06/2020	vaa-5.5.0-0.3.iso (VAA OS) vaa-5.5.0-0.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-0.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	06/2020	SBx81CFC960-5.5.0-0.3.rel
SBx908 GEN2	SBx908 GEN2	06/2020	SBx908NG-5.5.0-0.3.rel
x950-28XSQ x950-28XTQm	x950	06/2020	x950-5.5.0-0.3.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	06/2020	x930-5.5.0-0.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2020	x550-5.5.0-0.3.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	06/2020	x530-5.5.0-0.3.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	06/2020	x510-5.5.0-0.3.rel
IX5-28GPX	IX5	06/2020	IX5-5.5.0-0.3.rel
x320-10GH	x320	06/2020	x320-5.5.0-0.3.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	06/2020	x310-5.5.0-0.3.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	06/2020	x230-5.5.0-0.3.rel
x220-28GS x220-52GT x220-52GP	x220	06/2020	x220-5.5.0-0.3.rel
IE510-28GSX	IE510-28GSX	06/2020	IE510-5.5.0-0.3.rel
IE340-20GP IE340L-18GP	IE340	06/2020	IE340-5.5.0-0.3.rel
IE300-12GT IE300-12GP	IE300	06/2020	IE300-5.5.0-0.3.rel
IE210L-10GP IE210L-18GP	IE210L	06/2020	IE210-5.5.0-0.3.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2020	IE200-5.5.0-0.3.rel
XS916MXT XS916MXS	XS900MX	06/2020	XS900-5.5.0-0.3.rel
GS980EM/10H	GS980EM	06/2020	GS980EM-5.5.0-0.3.rel
GS980M/52 GS980M/52PS	GS980M	06/2020	GS980M-5.5.0-0.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2020	GS970-5.5.0-0.3.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2020	GS900-5.5.0-0.3.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	06/2020	FS980-5.5.0-0.3.rel
AR4050S AR3050S	AR-series UTM firewalls	06/2020	AR4050S-5.5.0-0.3.rel AR3050S-5.5.0-0.3.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	06/2020	AR2050V-5.5.0-0.3.rel AR2010V-5.5.0-0.3.rel AR1050V-5.5.0-0.3.rel

Caution: Software version 5.5.0-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.0 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. 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 63 and
- "Licensing this version on an SBx8100 Series CFC960 control card" on page 65.

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

The 5.5.0-0.3 software version is not ISSU compatible with previous software versions.

Issues resolved in version 5.5.0-0.3

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-67953	**Aggregation-LACP** **VCStack**	Previously, on a VCStack with a late joiner, occasionally if a port-channel went down, the log "Failed to complete post detach mux from aggregator po1 for port port5.0.52, error -1" was generated. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	Y	–	Y	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-68336	**AMF**	Previously on all x530L models, the AMF-Guest and AMF-Starter license were not included in the base license. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-68139	**AMF** **Web API**	Previously, on AMF masters/controllers other than the SBx81CFC960, AMF nodes coming/going from the AMF network could result in API requests to AMF nodes via the controller/or master being lost. This was due to the service responsible for proxying these requests being restarted each time a node came or went. 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-67959	**ARP Security**	With this software update, rate limiting can be applied to ARP security on GS900, x310, x510 and x550 series switches.	–	–	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	Y	–	–	–	–	–	–	–	–	–
CR-68781	**AWC-Lite**	Previously, when a MAC filter entry was registered, a small amount of memory was not freed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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-68787	**AWC-Lite**	Previously, following a reboot of a VCStack managing wireless nodes with AWC lite, an CMSG error "% CMSG internal error" could be generated in response to commands on the backup member in (config-wireless) mode. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-67588	**Firewall**	Previously, on occasion, attempting to modify a firewall entity that was in use could result in an error, and the modification would fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-68492	**Firewall**	When a firewall is enabled, it detects packets arriving with a source address that is not reachable via any of the routes in the main routing table. Those packets are logged as having a "Martian source" and are dropped. When a firewall is disabled (after being enabled) this check should no longer be performed. Previously, in some cases the check was still being performed. This could have been a problem in configurations involving Policy Based Routing, as they may have involved hosts that were only reachable via routes that were not in the main route table. Note: This wasn't an issue if the device was booted without Firewall enabled. This issue has now been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-67949	**IGMP**	With this software update, known multicast packets will no longer be reflected out the source port if the source port is also configured as a trunk port for NLB.	–	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-68345	**IPSec**	Previously, using IKEv1 Aggressive mode with NAT-T, the NAT-T information in the command **show ipsec peer** always showed as being off until the first rekey. This was due to the ISAKMP SA being established and the information recorded before the NAT-T information was known. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-68110	**LLDP** **PoE**	Previously, when an x320-10 variant switch was connected with a PD device that supported 802.3bt and LLDP, the switch did not send LLDP with type 3 and 4 fields. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-68287	**LLDP** **PoE**	Previously, with LLDP, sending power via MDI requests would not be processed. 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-68224 **CR-68284**	**Loop protection**	Previously, an error was sometimes shown when entering the command **loop protection action none** on an interface (with or without a timeout), despite the command completing successfully. 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-68340	**Mirroring**	Previously, the command **switchport remote-mirror-egress** was missing in the running-configuration when configured on a provisioned port. 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-68374	**Multicast forwarding hardware**	Previously, the command **show platform table ipmulti** could result in the PIM process to restart unexpectedly. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	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-68084	**Multicast forwarding hardware**	Previously, switching multicast traffic at Layer 2 with frames larger than 1500 bytes was not supported. With this software update, now, provided the ports have their MRU set to the appropriate size, jumbo frames can be correctly Layer 2 switched. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-68263	**Multicast routing**	Previously, IP multicast-routing was unable to be enabled on the GS980EM model. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-68244	**OpenFlow**	Openflow on the x530 model does not support VLAN double tagging. Previously, these flows were still being processed in software, resulting in undesirable behaviour. 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-68229	**PIM-SM**	Previously, it was possible for the PIM-SM process to restart when it was busy adding routes to the hardware table. This issue has been resolved. With this software update, it is now possible to configure how many internal updates PIM-SM, PIM-DM or PIM6-SM process at a time. This can be configured by the command **ip pim sparse-mode event-queue-length <num>**. ■ Configuring a shorter event queue length allows PIM to allocate more CPU time to handling PIM packets and PIM timeout events. ■ Configuring a longer event queue length allows PIM to allocate more CPU time to updating hardware. It is also possible to diagnose how busy PIM is by executing the command **show ip pim sparse-mode event-queue.** It is also now possible to configure how often PIM-SM polls for nexthop reachability. By default every 5 seconds PIM-SM checks that the nexthop for each source for each multicast route has not changed. This results in a high CPU load on networks with large numbers of MC groups all from different sources. This can now be configured by **ip pim nexthop-timer-interval <num>**. Setting the interval larger reduces the CPU load on the system at the cost of not realising the nexthop for a multicast source has changed for a little longer. This has no impact in networks where nexthop routing is not expected to change.	–	–	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-68176	**Pluggable transceivers**	Previously, communication was not recovered after removing or inserting the SFP module on x950 models. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-68533	**Pluggable transceivers**	Previously, when an SP10T/SP10Ta was removed and re-inserted, it could fail to work. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-68820	**Pluggable transceivers**	Previously, AT-SP10T modules could sometimes fail to link up on some platforms. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-66988	**PoE** **Port configuration**	Previously, the AT-GS980MX series switch might start up with PoE reporting odd or even ports transposed. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-61145	**Port authentication**	Previously, multiple dynamic VLANs did not work on an aggregator interface. 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-68550	**Port authentication**	Previously, Tri-authentication with 802.1x did not authorise supplicants if multiple supplicants were trying to connect at the same time. 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-66534	**Port configuration**	Previously, an SFP+ port connected with DAC occasionally might not link up on x530L models. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-67897	**PPP**	Previously, when a static route was configured with the nexthop as a point-to-point interface (i.e. using the command **ip route 0.0.0.0/0 ppp0**) and if the interface went down, it was possible for the routing table to make an incorrect decision, causing the route to no longer work as intended (traffic would be dropped). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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-67752	**QoS**	Previously on some switch models containing 2 switch chips, an ACL which changed a packet's user priority was also changing the CPU priority of the packet. This could result in the CPU being starved of more important traffic breaking protocols such as OSPF. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–	–	Y	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-68362	**QoS storm protection**	Previously, if QoS Storm Protection was configured to shut down ports in conjunction with Loop Protection configured similarly, it could interfere with Loop Protection's action to shut the port down. Depending on the configuration this could result in the port being brought up sooner than expected, or the port getting into an unexpected state where it displayed as 'err-disabled' but was still passing traffic and would not respond to either the **shutdown** or **no shutdown** commands. This issue has been resolved. Now when both protocols are in use together, QoS Storm Protection will not apply actions when Loop Protection (or any other protocol) has already shut the port down.	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-61186	**SNMP**	Previously, net-snmp was vulnerable to DoS due to null pointer vulnerability stated in CVE-2018-18065 and CVE-2018-18066. This software update addresses the vulnerability.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	–	–	Y	Y	–
CR-68252	**Storm Control**	Previously, you could not set storm-control settings greater than 16%. This issue has been resolved.	–	–	–	–	–	–	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-68273	**URL Offload**	Previously, if an HTTP server port was configured to serve a URL offload PAC file, but the HTTP service was disabled and the http/https server ports were not set to "none", it was still possible to access the GUI/API. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-68282	**URL Offload**	Previously, the PAC file generated by the URL Offload feature had some incorrect JavaScript code which meant that traffic might not be correctly matched. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-65948	**VCStack**	Previously on an x530 or SBxCFC960 stack, when multiple members were joining at the same time, some members could get stuck in the Initiation state and fail to join the stack. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-68322	**VCStack**	Previously, during a VCStack failover on an x950 or x908Gen2 switch it was possible for SFP+ ports to take longer than expected to shut down, resulting in a longer failover time and traffic disruption. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–
CR-68323	**VCStack**	Previously, on a x530 stack, the stack port could fail to link up after removing and re-inserting a stackXS cable. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-68102	**VCStack**	Previously, when a single SBx81XLEM line-card was restarted, any multicast traffic could delay the card from re-joining the chassis. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-68594	**VLAN**	Previously, VLAN statistics commands were present but they did not work. With this software update, the redundant commands have been removed.	–	–	–	–	–	–	–	–	–	–	–	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-67522	**Web API**	Previously the **show users** command could report incorrect output for VTY lines that were in use by the Web API. 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	–

Enhancements in version 5.5.0-0.3

URL offload

From version 5.5.0-0.3 onwards, URL offload is able to fully parse the URL data from the Microsoft endpoint data. Previously any URL retrieved from the Microsoft endpoint that was not a valid FQDN (for example, *test.example.com) was marked as 'unusable'.

For more information on URL offload, see the URL Offload Feature Overview and Configuration Guide.

AWC emergency mode

Available on AR4050S, AR3050S, AR2050V, and AR2010V firewalls and VPN routers, x950, x930, x550, x530 x530, and SBx908 GEN2 Series switches.

From version 5.5.0-0.3 onwards, you can set an emergency mode on a wireless network. You can use emergency mode to prevent people from being isolated from infrastructure in the event of a natural disaster such as an earthquake or typhoon.

Wireless networks in emergency mode are only active when AWC is also in emergency mode.

For example, to configure an emergency mode for network 5, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 5
awplus(config-wireless-network)# emergency-mode
```

For more information on wireless networks, see the User Guide: Vista Manager mini.

IPv6 Source Address Dependent Routing

Available on AR4050S, AR3050S, AR2050V, and AR2010V firewalls and VPN routers

From version 5.5.0-0.3 onwards, you can configure IPv6 Source Address Dependent Routing (SADR).

IPv6 SADR is useful where there are two or more active IPv6 WAN links originating from an AlliedWare Plus firewall or VPN router, with each WAN link connecting via different ISPs. Using PIv6 SADR, each upstream ISP router only accepts traffic originating from global scoped prefixes they have allocated for use. All other traffic originating from other prefixes associated with a different ISP is denied. IPv6 SADR allows routes to be used for a subset of all prefixes. This ensures traffic sourced from prefixes allocated by an ISP is routed only to that ISP.

For more information about IPv6 Source Address Dependent Routing, see the IPv6 Feature Overview and Configuration Guide.

Two-step port authentication order

Available on all devices that support two-step port authentication.

From version 5.5.0-0.3 onwards, you can configure the order for two-step port authentication using the **auth two-step order** command.

The default two-step authentication order depends on the combination of the authentication methods configured on an interface:

- If MAC authentication is configured then MAC authentication will be the first method.
- If MAC authentication is **not** configured then 802.1X authentication will become the first method.
- If only two methods are configured then the remaining method becomes the second method.
- If all three methods are configured then the second method is chosen based on the packet type received (802.1X authentication for an EAPOL packet and web authentication for an HTTP packet).

If, for example, you would like to configure the two-step authentication order to be 802.1X authentication (dot1x) followed by MAC authentication (auth-mac) use the following 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 two-step enable
awplus(config-if)# auth two-step order dot1x auth-mac
```

For more information about two-step port authentication see the AAA and Port Authentication Feature Overview and Configuration Guide.

Device Discovery using SNMP

Available on all AlliedWare Plus™ products that are AMF master capable, running the device GUI version 2.5.2 or later

From version 5.5.0-0.3 onwards, SNMP Device Discovery is available from the AlliedWare Plus CLI. SNMP Device Discovery discovers the devices and then can receive traps for them. This means that you are able to see the attached devices, and see alerts if there are problems with them. Vista Manager mini reports notable events from third party vendor devices. This feature provides information that you can use to display and monitor third party vendor device data in real time.

After you configure Device Discovery, you can see SNMP discovery nodes from the Network MAP. All SNMP nodes are automatically displayed in positions where they are located on the topology map. If the discovery node is located under an AMF member, it automatically displays under that AMF member.

Use this feature to monitor SNMP trap events from the Network Map. From the 'Node List' you access SNMP devices, and the SNMP Recent Events List. The recent event list information displays: Date, Target Name, Model Name, Event Name, and Message.

See the following documents for more detailed information about how to configure SNMP, SNMP MIBs, and AMF:

- For more information about SNMP, see the SNMP Feature Overview and Configuration Guide.
- For more information about SNMP Management Information Base traps, see the Support for Allied Telesis Enterprise MIBs in AlliedWare Plus Technical Guide.
- This feature makes use of an existing AMF network to supply this information to the device GUI. For more information about AMF, see the AMF Feature Overview and Configuration Guide.

What's new in version 5.5.0-0.1

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960[1]
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

1. SBx8100 Series switches are not supported by 5.5.0-0.1. They will be supported by a later maintenance release.

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.0-0.1.

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

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 67.

For instructions on how to update the web-based GUI, see "Installing and accessing the Web-based GUI on switches" on page 69 or "Installing and accessing the Web-based GUI on AR-Series devices" on page 72. 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		03/2020	vaa-5.5.0-0.1.iso (VAA OS) vaa-5.5.0-0.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-0.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	SBx8100 Series switches are not supported by 5.5.0-0.1. They will be supported by a later maintenance release.	
SBx908 GEN2	SBx908 GEN2	03/2020	SBx908NG-5.5.0-0.1.rel
x950-28XSQ x950-28XTQm	x950	03/2020	x950-5.5.0-0.1.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2020	x930-5.5.0-0.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2020	x550-5.5.0-0.1.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	03/2020	x530-5.5.0-0.1.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	03/2020	x510-5.5.0-0.1.rel
IX5-28GPX	IX5	03/2020	IX5-5.5.0-0.1.rel
x320-10GH	x320	03/2020	x320-5.5.0-0.1.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2020	x310-5.5.0-0.1.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	03/2020	x230-5.5.0-0.1.rel
x220-28GS x220-52GT x220-52GP	x220	03/2020	x220-5.5.0-0.1.rel
IE510-28GSX	IE510-28GSX	03/2020	IE510-5.5.0-0.1.rel
IE340-20GP IE340L-18GP	IE340	03/2020	IE340-5.5.0-0.1.rel
IE300-12GT IE300-12GP	IE300	03/2020	IE300-5.5.0-0.1.rel
IE210L-10GP IE210L-18GP	IE210L	03/2020	IE210-5.5.0-0.1.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2020	IE200-5.5.0-0.1.rel
XS916MXT XS916MXS	XS900MX	03/2020	XS900-5.5.0-0.1.rel
GS980EM/10H	GS980EM	03/2020	GS980EM-5.5.0-0.1.rel
GS980M/52 GS980M/52PS	GS980M	03/2020	GS980M-5.5.0-0.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2020	GS970-5.5.0-0.1.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2020	GS900-5.5.0-0.1.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	03/2020	FS980-5.5.0-0.1.rel
AR4050S AR3050S	AR-series UTM firewalls	03/2020	AR4050S-5.5.0-0.1.rel AR3050S-5.5.0-0.1.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	03/2020	AR2050V-5.5.0-0.1.rel AR2010V-5.5.0-0.1.rel AR1050V-5.5.0-0.1.rel

Caution: Software version 5.5.0-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.0 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. 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 63 and
- "Licensing this version on an SBx8100 Series CFC960 control card" on page 65.

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

The 5.5.0-0.1 software version is ISSU incompatible with previous software versions.

New products

Version 5.5.0-0.1 supports the following upcoming and recently-released products.

x530-52GPXm and x530-52GTXm Stackable Multi-Gigabit Layer 3 Switches

Supported since 5.4.9-2.1

These switches are high-performing and feature-rich, with 40 x 100M/1G and 8 x 100M/1G/2.5G/5G ports, and 4 x 10G uplinks. Key features include:

- Support for high-speed wireless, and network upgrades over legacy cabling, with 2.5G and 5G connectivity
- VCStack up to 8 units locally or over distance to support resilient networking
- Ethernet Protection Switched Ring (EPSRing™) and G.8032 ERPS supports high-speed resilient ring-based networksActive Fiber Monitoring prevents eavesdropping on fiber communications.
- On the x530-52GPXm model, Power over Ethernet Plus (PoE+) supplies up to 30 Watts to connect and power endpoints such as PTZ security cameras, POS terminals, and wireless access points.

For more information, see our website at www.alliedtelesis.com/products/switches/x530-series.

x320-10GH Gigabit Layer 3 PoE++ Switch

Supported since 5.4.9-2.1

8 x 10/1000/1000T PoE++ ports, 2 x 100/1000X SFP uplinks, and a power budget of up to 720W make the x320-10GH ideal to connect and power today's high-power access and security devices. Key features include:

- Up to 90 Watts of PoE++ per port
- EPSRing™ and G.8032 for resilient rings
- Active Fiber Monitoring
- Static and dynamic routing
- Fanless design for silent operation
- Flexible deployment options including DIN rail mounting.

GS980EM/10H Gigabit Layer 3 Lite PoE++ Switch

Supported since 5.4.9-2.1

8 x 10/1000/1000T PoE++ ports, 2 x 100/1000X SFP uplinks, and a power budget of up to 720W make the GS980EM/10H ideal to connect and power today's high-power access and security device. Key features include:

- Up to 90 Watts of PoE++ per port
- EPSRing™ and G.8032 for resilient rings
- Active Fiber Monitoring
- Static routing, RIP, OSPFv2
- Fanless design for silent operation
- Flexible deployment options including DIN rail mounting.

New features and enhancements

This section summarizes the new features in 5.5.0-0.1:

To see how to find full documentation about all features on your product, see "Obtaining user documentation" on page 62.

URL Offload

Available on AR2010V, AR2050V, AR3050S and AR4050S

From 5.5.0-0.1 onwards, you can speed up access to cloud services when your network architecture routes all traffic to a VPN or proxy server by default. You can use this feature to bypass a proxy or VPN link for certain URLs/IPs, by offloading them directly to the internet instead. This improves the performance of cloud services and reduces the bandwidth demands on VPN links.

This feature fetches endpoint data about which URLs and IP addresses need to be offloaded from an 'endpoints service'. Currently, we support the Microsoft Office365 endpoints service. It is also a reliable way of fetching all of the endpoints in use by Microsoft Office365.

The endpoints data can then be used to generate and serve a Proxy Auto-Configuration (PAC) file to PC clients. The PAC file is configured as part of the DHCP server configuration and is downloaded by clients served directly from the router. You can use a default template, or you can configure a custom template for the PAC file. This feature automatically keeps the PAC file used by network clients up to date, removing this burden from a network administrator.

URL offload also generates dynamic firewall entities based on the endpoints data. This allows a network administrator to easily configure filtering and routing based on the endpoints data. This secures your network against PC clients trying to bypass a proxy or VPN link without authorization.

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

IPv6 support on USB Cellular Modem interfaces

Available on AR-Series firewalls and routers

From 5.5.0-0.1 onwards, 3G or 4G modems connecting to carriers that support dual stack (IPv4/IPv6) connectivity are able to utilize this capability.

Modems supporting dual stack functionality are typically configured as cellular interfaces with PPP encapsulation. IPv6 is enabled on the cellular interface, to enable dual stack mode in the MODEM via the default internal chat script. Additionally the PPP interface is also configured with both IPv4 and IPv6 options for dual stack operation. Options can include IPv6 and IPv6 MSS clamping, IPv4 address negotiation and DNS. IPv6 is also enabled on the PPP interface to invoke IPV6 SLAAC via the cellular PPP link.

Additionally, the cellular PPP WAN can also be used for WAN backup purposes, by configuring the IPv6 routing path via the cellular PPP interface to be a higher cost. This means that it is only used if the primary IPv6 routing path via the alternative WAN interface goes down.

For more information, see the USB Cellular Modem Feature Overview and Configuration Guide.

IPv6 over IPv4 Tunneling

Available on x530 and x930 Series switches

From 5.5.0-0.1 onwards, you can configure static IPv6 over IPv4 tunnels.

IPv6 over IPv4 tunnels are point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures. This allows isolated IPv6 end systems and devices to communicate without the need to upgrade the IPv4 infrastructure that exists between them.

When moving a network from IPv4 addressing to IPv6 addressing, the transition necessarily proceeds in stages, with islands of IPv6 developing within the IPv4 network, and gradually growing until they cover the whole network. During early transition, IPv4 networks are widely deployed and IPv6 networks are isolated sites. An IPv6 over IPv4 tunnel allows IPv6 packets to be transmitted on an IPv4 network and connects all IPv6 sites.

For more information, see the IPv6 over IPv4 Tunneling Feature Overview and Configuration Guide.

Faster OpenFlow IPv6 traffic matching for SBx908 GEN2 and x950 Series switches

From 5.5.0-0.1 onwards, the SBx908 GEN2 and x950 Series switches have been improved to achieve optimal behavior for OpenFlow IPv6 traffic.

Most of the IPv6 match criteria combinations now result in hardware processing instead of software.

For more information about OpenFlow support and configuration, see the OpenFlow Feature Overview and Configuration Guide.

New MODBUS heartbeat registers

Available on IE300, IE340, x930 and x950 Series switches

From 5.5.0-0.1 and 5.4.9-2.3 onwards, MODBUS supports three new heartbeat registers that can be used by MODBUS clients to monitor the liveliness of the MODBUS server.

They are as follows:

ADDRESS (HEX)	SIZE	TYPE	ACCESS	DESCRIPTION
Stack Global System Information				
0x004A	2 words	UINT	R	TCP Connection Uptime (in seconds)
0x004C	1 word	HEX	R/W	Master Heartbeat Time (in seconds, up to 255s)
0x004D	1 word	HEX	R	Slave Heartbeat

Increased VRF Support

Available on x950 and SBx908GEN2 Series Switches

From 5.5.0-0.1 onwards, the number of user defined VRFs is increased to 600.

This allows you to configure a larger number of VLANs, routes and/or routing protocols.

To use the extended VRF feature on the AT-x950 or AT-SBx908Gen2 Series, you will need to obtain a license for it. Please contact your Allied Telesis representative for more information.

8-unit stacking support for x950 Series switches

Available on x950 Series switches

From 5.5.0-0.1 and 5.4.9-2.3 onwards, VCStack enables you to stack up to eight x950 series switches. VCStack provides a highly available system where network resources are spread out across stacked units, reducing the impact if one of the units fails.

ACL Memory Optimization

Available on x530 Series Switches

From 5.5.0-0.1 onwards, ACL memory usage is more efficient.

Previously, global rules were duplicated for each port that had a per-port rule, which increased memory usage. With this software version, ports are able to share some rules to optimist total ACL memory usage.

You can see this in the output of the command **show platform classifier statistics utilization brief**. The output will now show fewer entries occupied.

Before software version 5.5.0-0.1:

```
awplus#show platform classifier statistics utilization brief
...
                    Used/Total
...
Global ACL          84
ACL                 28
...
Total               112 /   512 (21.88%)
```

After software version 5.5.0-0.1:

```
awplus#show platform classifier statistics utilization brief
...
                    Used/Total
...
Global ACL          3
ACL                 1
...
Total               4 /   512 (0.78%)
```

Improvements to logging commands

Available on all AlliedWare Plus devices

From 5.5.0-0.1 onwards, it is possible to use the **no** form to return the following settings to their default value:

Setting	Command
the external log size	no log external size
the external rotate value	no log external rotate
the permanent log size	no log permanent size
the buffered log size	no log buffered size

Displaying status of wireless and LACP debugging

Available on all AlliedWare Plus devices that support wireless management or LACP

From 5.5.0-0.1 onwards, output of the command **show debugging** now includes whether debugging is turned on for wireless management and LACP. The following pre-existing commands also show this:

- show debugging wireless
- show debugging lacp

Configure a "cost" value in OSPF summary routes

Available on all AlliedWare Plus devices that support OSPFv2

From 5.5.0-0.1 onwards, when using the **area range** command in OSPFv2, you can specify an optional **cost** parameter.

Normally, when summary routes are generated, the metric sent in the LSA is the largest of all possible paths that can be used to reach the destination network. When the **cost** parameter is specified, the metric sent in the LSA will be overridden by whatever value you specify in the **cost** parameter.

OSPFv2 command now available on routers

Added to AR2010V, AR2050V, AR3050S and AR4050S

From 5.5.0-0.1 onwards, these AR-Series firewalls and routers support the command **distribute-list route-map**. This command was previously only available on Layer 3 switches. The command applies a route-map which you can use to filter the routes installed into the OSPF RIB that are generated from OSPF's LSA database.

Disabling unused services

Available on all AlliedWare Plus devices that support PIM or URL Offload

Sometimes it may be desirable to disable unused services, in order to reduce memory use. From 5.5.0-0.1 onwards, you can disable the following services:

Service	Command
PIM-SM for IPv4	no service pim
PIM-SM for IPv6	no service pim6
PIM-DM for IPv4	no service pmd
URL Offload (AR2010V, AR2050V, AR3050S and AR4050S)	no service url_offload

These services are enabled by default. Disabling the PIM services will only take effect after you save the configuration and restart the device.

Wireless controller on x550 Series switches

Added to x550 Series. Already available on a number of other AlliedWare Plus devices

From 5.5.0-0.1 onwards, x550 Series switches support AWC for Wireless Management. AWC automatically optimizes wireless output and channel selection. It minimizes coverage gaps and reduces AP interference.

You can manage your wireless network through the Vista Manager mini menu in version 2.5.1 or later of the switch's Device GUI, or you can use the command line's wireless commands to do so.

For more information about AWC on the Device GUI, see Vista Manager mini and AWC for Wireless Management on AlliedWare Plus Devices.

For information about the commands, see the Command Reference.

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:

- Upgrade compatibility for SBx908 GEN2 and x950 Series switches
- Adding a CFC960 to an SBx8100 chassis or stack
- Changes that may affect device or network configuration

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

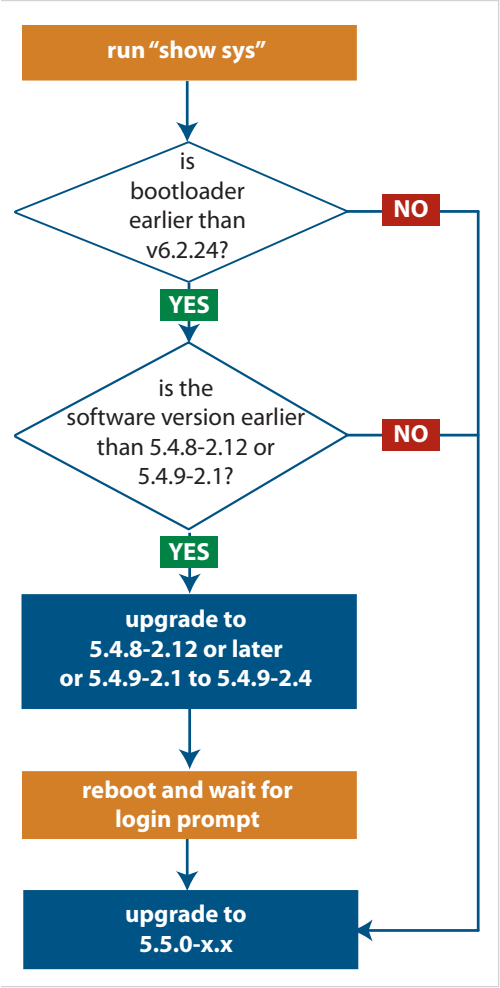
- Software Release Licensing
- Upgrading a VCStack with rolling reboot - read this if stacking x530 Series switches
- Forming or extending a VCStack with auto-synchronization
- AMF software version compatibility
- Upgrading all devices in an AMF network

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

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

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.

Adding a CFC960 to an SBx8100 chassis or stack

If you want to combine CFC960 v2 and earlier CFC960 cards in a chassis or stack, make sure that the earlier cards are running 5.5.0-0.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.

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
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 are no longer accessible 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 63 and
- "Licensing this version on an SBx8100 Series CFC960 control card" on page 65.

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 x530 Series switches using DAC to stack

If you are using DACs (Direct Attach Cables) to connect stack members, you **cannot** use rolling reboot to upgrade to 5.5.0-0.x from:

- 5.4.9-2.x
- 5.4.9-1.x

This is because, in these versions, the DAC's speed is different than in 5.5.0-0.x.

You **can** use rolling reboot to upgrade to 5.5.0-0.x from:

- 5.4.9-0.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 5.5.0-0.x from:

- 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.

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 5.5.0-0.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 all other stacks

Unless you are putting a CFC960 v2 card in an SBx8100 system, auto-synchronization is supported between 5.5.0-0.x and:

- 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 5.5.0-0.x and 5.4.6-1.1 or **any** earlier releases.

AMF software version compatibility

Applies to all AlliedWare Plus devices

We strongly recommend that all nodes in an AMF network run the same software release. If this is not possible, please be aware of the following compatibility limitations.

If using an AMF controller

If your Controller or **any** of your Masters are running 5.4.7-1.1 or later, then the Controller and **all** of the Masters must run 5.4.7-1.1 or later. However, the software on Member nodes can be older than 5.4.7-1.1.

Otherwise, the "show atmf area nodes" command and the "show atmf area guests" command will not function, and Vista Manager EX will show incorrect network topology.

If using secure mode

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

If using Vista Manager EX

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

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

If using none of the above

If none of the above apply, then nodes running version 5.5.0-0.x are compatible with nodes running:

- 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 SBx908 GEN2, x950, x930, x550, x530, x320, x220, IE340, and XS900MX Series switches, 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-2019
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-2020
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-2019
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-2020
License expiry date            : N/A
Release                        : 5.5.0
```

Installing this software version

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.

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 63 and
- "Licensing this version on an SBx8100 Series CFC960 control card" on page 65.

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 SBx8100-5.5.0-0.6.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.0-0.6.rel`
x950 series	`awplus(config)# boot system x950-5.5.0-0.6.rel`
x930 series	`awplus(config)# boot system x930-5.5.0-0.6.rel`
x550 series	`awplus(config)# boot system x550-5.5.0-0.6.rel`
x530 series	`awplus(config)# boot system x530-5.5.0-0.6.rel`
x510 series	`awplus(config)# boot system x510-5.5.0-0.6.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.5.0-0.6.rel`
x320 series	`awplus(config)# boot system x320-5.5.0-0.6.rel`

Product	Command
x310 series	`awplus(config)# boot system x310-5.5.0-0.6.rel`
x230 series	`awplus(config)# boot system x230-5.5.0-0.6.rel`
x220 series	`awplus(config)# boot system x220-5.5.0-0.6.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.5.0-0.6.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.0-0.6.rel`
IE300 series	`awplus(config)# boot system IE300-5.5.0-0.6.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.0-0.6.rel`
IE200 series	`awplus(config)# boot system IE200-5.5.0-0.6.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.0-0.6.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.0-0.6.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.0-0.6.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.0-0.6.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.5.0-0.6.rel`
FS980M series	`awplus(config)# boot system FS980-5.5.0-0.6.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.0-0.6.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.0-0.6.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.5.0-0.6.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.0-0.6.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.0-0.6.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
```

Installing and 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.

The steps for installing and accessing the GUI depend on whether the latest GUI has been pre-installed on your device in the factory.

Check if the GUI is installed

To tell if the GUI is installed on your device, simply browse to it, as described below.

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. If you do not see a login page, you need to install the GUI, as described in "Install the GUI if it is not installed" on page 73. If you see a login page, log in. 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 5.5.0-0.6 is 2.6.2.

If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 73.

Install the GUI if it is not installed

Perform the following steps through the command-line interface if your AlliedWare Plus switch does not currently have a GUI installed.

1. Obtain the GUI file from our Software Download center. The file to use with 5.5.0-0.6 is awplus-gui_550_18.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 GUI file from your USB Flash drive, use the following commands:

   ```
   awplus>enable
   awplus#copy usb awplus-gui_550_18.gui flash
   ```

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

   ```
   awplus#dir
   ```

3. Delete any previous Java switch GUI files.

   If you have been using the previous Java switch GUI, we recommend you delete the old GUI file to avoid any conflict. To do this, delete any Java files (.jar) from the switches Flash memory. For example:

   ```
   awplus#del x510-gui_547_02.jar
   ```

4. If you haven't already, add an IP address to a VLAN on the switch. For example:

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

5. Make sure the HTTP service is running:

   ```
   awplus# configure terminal
   awplus(config)# service http
   ```

6. 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*.

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 file to use with 5.5.0-0.6 is awplus-gui_550_18.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 GUI file from your USB Flash drive, use the following commands:

   ```
   awplus>enable
   awplus#copy usb awplus-gui_550_18.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*.

Installing and 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.

The steps for installing and accessing the GUI depend on whether the latest GUI has been pre-installed on your device in the factory.

Check if the GUI is installed

To tell if the GUI is installed on your device, simply browse to it, as described below.

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. If you do not see a login page, you need to install the GUI, as described in "Install the GUI if it is not installed" on page 73. If you see a login page, log in. 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 5.5.0-0.6 is 2.6.2. If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 73.

Install the GUI if it is not installed

Perform the following steps through the command-line interface if your AR-series device does not currently have a GUI installed.

1. If the device's firewall is enabled, 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.

2. If you haven't already, create one or more IP interfaces and assign them IP addresses, including configuring WAN connectivity. For information about configuring PPP, see the PPP Feature Overview and Configuration Guide. For information about configuring IP, see the IP Feature Overview and Configuration Guide.

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

```
awplus# update webgui now
```

4. Make sure the HTTP service is running:

```
awplus# configure terminal
awplus(config)# service http
```

5. 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.

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.