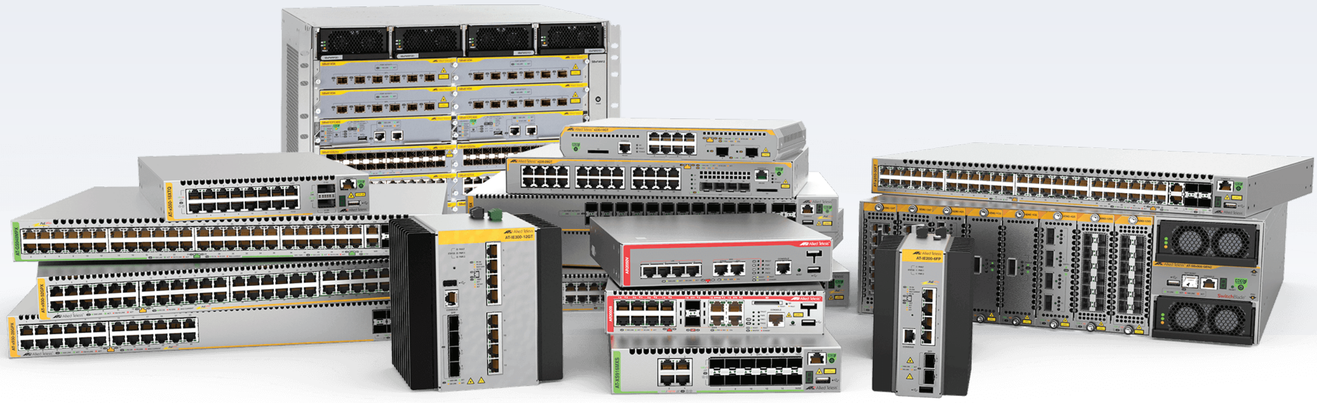
Allied Telesis™

Release Note for AlliedWare Plus Software Version 5.4.9-0.x



AlliedWare Plus
OPERATING SYSTEM

» SBx8100 Series » SBx908 GEN2 » x950 Series » x930 Series

» x550 Series » x530/L Series » x510 Series » IX5 Series

» x310 Series » x230 Series » x220 Series

» IE500 Series » IE300 Series » IE210L Series » IE200 Series

» XS900MX Series » GS980M Series » GS970M Series

» GS900MX/MPX Series » FS980M Series » AMF Cloud

» AR4050S » AR3050S » AR2050V » AR2010V » AR1050V

» 5.4.9-0.1 » 5.4.9-0.2 » 5.4.9-0.3 » 5.4.9-0.5 » 5.4.9-0.6 » 5.4.9-0.7 » 5.4.9-0.8

Acknowledgments

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

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

All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see **www.openssl.org/**

Copyright ©1998-2008 The OpenSSL Project. All rights reserved.

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

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

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

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by registered mail including a check for US$15 to cover production and shipping costs and a CD with the GPL code will be mailed to you.

GPL Code Request
Allied Telesis Labs (Ltd)
PO Box 8011
Christchurch
New Zealand

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

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 5.4.9-0.8

Product families supported by this version:

AR4050S
AR3050S
AR2050V
AR2010V
AR1050V
FS980M Series
GS900MX/MPX Series
GS970M Series
GS980M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220 Series
x230 Series
x310 Series
IX5-28GPX
x510 Series
x530/L Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100: SBx81CFC960
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-0.8.

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

Caution: Software version 5.4.9-0.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 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 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 59 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 61.

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	GUI File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	08/2019	FS980-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2019	GS900-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2019	GS970-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS980M/52 GS980M/52PS	GS980M	08/2019	GS980M-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
XS916MXT XS916MXS	XS900MX	08/2019	XS900-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2019	IE200-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE300-12GT IE300-12GP	IE300	08/2019	IE300-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE210L-10GP IE210L-18GP	IE210L	08/2019	IE210-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE510-28GSX-80	IE500	08/2019	IE510-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x220-28GS x220-52GT x220-52GP	x220	08/2019	x220-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2019	x230-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2019	x310-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IX5-28GPX	IX5	08/2019	IX5-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65

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

Models	Family	Date	Software File	GUI File
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	08/2019	x510-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x530-28GTXm x530-28GPXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	08/2019	x530-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2019	x550-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2019	x930-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x950-28XSQ	x950	08/2019	x950-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx908 GEN2	SBx908 GEN2	08/2019	SBx908NG-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx81CFC960	SBx8100	08/2019	SBx81CFC960-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR4050S AR3050S	AR-series UTM firewalls	08/2019	AR4050S-5.4.9-0.8.rel AR3050S-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR2050V AR2010V AR1050V	AR-series VPN firewalls	08/2019	AR2050V-5.4.9-0.8.rel AR2010V-5.4.9-0.8.rel AR1050V-5.4.9-0.8.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AMF Cloud		08/2019	vaa-5.4.9-0.8.iso (VAA OS) vaa-5.4.9-0.8. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-0.8.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.9-0.x does not support:

- SBx81CFC400 control cards (it does support SBx81CFC960 control cards).

Issues Resolved in Version 5.4.9-0.8

This AlliedWare Plus maintenance version is to address factory testing issues. There are no customer affecting issues resolved in this release.

What's New in Version 5.4.9-0.7

Product families supported by this version:

AR4050S
AR3050S
AR2050V
AR2010V
AR1050V
FS980M Series
GS900MX/MPX Series
GS970M Series
GS980M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220 Series
x230 Series
x310 Series
IX5-28GPX
x510 Series
x530 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100: SBx81CFC960
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-0.7.

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

Caution: Software version 5.4.9-0.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 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 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 59 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 61.

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	GUI File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	07/2019	FS980-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	07/2019	GS900-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2019	GS970-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
GS980M/52 GS980M/52PS	GS980M/MX	07/2019	GS980M-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
XS916MXT XS916MXS	XS900MX	07/2019	XS900-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2019	IE200-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE300-12GT IE300-12GP	IE300	07/2019	IE300-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE210L-10GP IE210L-18GP	IE210L	07/2019	IE210-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE510-28GSX-80	IE500	07/2019	IE510-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
x220-28GS x220-52GT x220-52GP	x220	07/2019	x220-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2019	x230-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2019	x310-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IX5-28GPX	IX5	07/2019	IX5-5.4.9-0.7.rel	See “Installing and Accessing the Web-based Device GUI” on page 65

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

Models	Family	Date	Software File	GUI File
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	07/2019	x510-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x530-28GTXm x530-28GPXm	x530	07/2019	x530-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2019	x550-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2019	x930-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x950-28XSQ	x950	07/2019	x950-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx908 GEN2	SBx908 GEN2	07/2019	SBx908NG-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx81CFC960	SBx8100	07/2019	SBx81CFC960-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR4050S AR3050S	AR-series UTM firewalls	07/2019	AR4050S-5.4.9-0.7.rel AR3050S-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR2050V AR2010V AR1050V	AR-series VPN firewalls	07/2019	AR2050V-5.4.9-0.7.rel AR2010V-5.4.9-0.7.rel AR1050V-5.4.9-0.7.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AMF Cloud		07/2019	vaa-5.4.9-0.7.iso (VAA OS) vaa-5.4.9-0.7. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-0.7.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.9-0.x does not support:

- SBx81CFC400 control cards (it does support SBx81CFC960 control cards).

Enhancements

CR	Module	Description	FS980M	GS980M/MX	GS970M	GS900MX	XS900MX	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-2843	**DHCP Relay**	This enhancement introduces a new command: `ip dhcp-relay use-client-side-address` This command allows you to configure DHCP-Relay to use the client-side interface IP address as the source IP address for all DHCP relayed packet. For maintaining backward compatibility, by default, the source IP address used by packets relayed by DHCP-Relay is the IP address of the egress interface used to reach the DHCP server (i.e. server-side interface IP address). ISSU: CFCs Upgraded .	–	Y	–	–	–	–	Y	Y	–	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

Issues Resolved in Version 5.4.9-0.7

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

CR	Module	Description	FS980M	GS970M	GS980M/MX	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx908	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63793	**Aggregation - LACP** **VCStack**	Previously, after a rolling reboot, there may have been differences in the command output for: **show diagnostics channel-group** between stack members, with errors showing on the backup members. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	Y	Y	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–	–
CR-63510	**AMF**	Previously, if the full length IPv6 address (i.e. 46 characters in string format) was used with AMF, the AMF recovery could fail. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-63789	**AMF**	With this software update, the application Proxy Whitelist NAS now retain the Radius Proxy Information indefinitely. This previously timed out in 60 minutes. ISSU: CFCs Upgraded	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	Y	Y	–	Y	Y	–	–	–	Y	–
CR-62593	**DHCP Snooping**	Previously, when **service dhcp snooping** was enabled, VLANs with DHCP snooping disabled could incorrectly drop some DHCP packets. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	Y	Y	Y	–
CR-63313	**Energy Efficient** **Ethernet**	Previously, 10G links with Energy Efficient Ethernet (EEE) enabled could drop packets or lock up at certain low packet rates. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-63671	**Firewall** **NAT**	Previously, port forwarding would not function correctly when firewall was disabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS980M/MX	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx908	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63692	**IGMP**	Previously, under rare circumstances, the number of sources for an IGMP record could incorrectly be set to 65535 when there were in fact no sources specified by the group, causing a large amount of unnecessary memory usage. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-63734	**IGMP** **VCStack**	Previously, unnecessary error warnings were generated after a CFC960 failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–
CR-63344	**IPv6**	Previously, the tunnel interface could go up and down when updating MAP-E rules. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-63773	**IPv6**	Previous, a device could sometimes start up with the system's name server list update incomplete. As a result, when a curl request was sent to the map rule distribution server, its hostname could not be resolved and would return an error. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-63779	**Multicast Routing** **VCStack**	With this software update, late node insertion event performance on large multicast networks has been improved. This change applies only to platforms that support 32K multicast.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–
CR-63504	**Static Aggregation** **VCStack**	Previously, de-configuring a static channel-group in a stack environment might cause the backup stack member to leave the stack. This issue has been resolved. ISSU: Effective when ISSU complete	Y	–	–	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–	–	–	–
CR-63722	**Switching**	Previously, the copper ports on an AT-x950-28XTQm switch could fail to link up after reboot.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS980M/MX	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx908	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63574	**VLAN**	Previously, on an AR1050V device, when the VLAN name or MTU value was set on VLAN 1, the information would be displayed twice in running configuration. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–

What’s New in Version 5.4.9-0.6

Product families supported by this version:

AR4050S
AR3050S
AR2050V
AR2010V
AR1050V
FS980M Series
GS900MX/MPX Series
GS970M Series
GS980M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220 Series
x230 Series
x310 Series
IX5-28GPX
x510 Series
x530 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100: SBx81CFC960
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-0.6.

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: Software version 5.4.9-0.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 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 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 59 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 61.

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	GUI File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	06/2019	FS980-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2019	GS900-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2019	GS970-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
GS980M/52 GS980M/52PS	GS980M	06/2019	GS980M-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
XS916MXT XS916MXS	XS900MX	06/2019	XS900-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2019	IE200-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE300-12GT IE300-12GP	IE300	06/2019	IE300-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE210L-10GP IE210L-18GP	IE210L	06/2019	IE210-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IE510-28GSX-80	IE500	06/2019	IE510-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
x220-28GS x220-52GT x220-52GP	x220	06/2019	x220-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	06/2019	x230-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
x310-26FT x310-50FT x310-26FP x310-50FP	x310	06/2019	x310-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65
IX5-28GPX	IX5	06/2019	IX5-5.4.9-0.6.rel	See “Installing and Accessing the Web-based Device GUI” on page 65

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

Models	Family	Date	Software File	GUI File
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	06/2019	x510-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x530-28GTXm x530-28GPXm	x530	06/2019	x530-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2019	x550-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	06/2019	x930-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x950-28XSQ	x950	06/2019	x950-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx908 GEN2	SBx908 GEN2	06/2019	SBx908NG-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx81CFC960	SBx8100	06/2019	SBx81CFC960-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR4050S AR3050S	AR-series UTM firewalls	06/2019	AR4050S-5.4.9-0.6.rel AR3050S-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR2050V AR2010V AR1050V	AR-series VPN firewalls	06/2019	AR2050V-5.4.9-0.6.rel AR2010V-5.4.9-0.6.rel AR1050V-5.4.9-0.6.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AMF Cloud		06/2019	vaa-5.4.9-0.6.iso (VAA OS) vaa-5.4.9-0.6. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-0.6.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.9-0.x does not support:

- SBx81CFC400 control cards (it does support SBx81CFC960 control cards).

Enhancements

CR	Module	Description	FS980M	GS980M	GS970M	GS900MX	XS900MX	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-2018	**SSH**	With this enhancement, if 'crypto secure mode' is enabled, then when a user logs into the device via secure-shell and is locally authenticated, previous failed attempts to login with the same user's credentials will be displayed. For example: `!` `awplus login: manager` `Password:` `Login incorrect` `awplus login: manager` `Password:` `Login incorrect` `awplus login: manager` `Password:` `Last failed login: Wed Feb 20 02:10:27 UTC 2019 on ttyS0` `There were 2 failed login attempts since the last successful login.` `AlliedWare Plus (TM) 5.4.8 02/15/19 02:12:49` `!`	–	Y	–	–	–	–	–	–	Y	–	–	–	–	Y	Y	Y	Y	–	Y	–	–	–	–

Issues Resolved in Version 5.4.9-0.6

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

CR	Module	Description	FS980M	GS980M	GS900MX	XS900MX	GS900Mv2	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63586	**AMF**	Previously, ARP-Probe within the SESC Application Proxy could sometimes not work correctly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	–	–	–	Y	Y	–	–	Y	–	–	–	–	–	–
CR-63126	**ARP**	Previously, when ARP security received an ARP message that violated the security policy, it would bring a port link down.With this software update, a new command has been added for ARP Security on a per-port basis, to allow IPv4 link-local ARP probes to be dropped without causing an ARP security violation when received: arp security drop link-local-probes. The new command is: `arp security drop link-local-probes` `no arp security drop link-local-probes` Also, previously, gratuitous ARPs would be incorrectly processed by ARP security as violations.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-63553	**CLI**	Previously, the command prompt could hang and then restart unexpectedly when "no auth ?" was entered in the interface configuration mode. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-63447	**DHCP, OpenVPN**	With this software update, OpenVPN TAP tunnels now correctly support DHCP server. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-63671	**Firewall** **NAT**	Previously, port forwarding would not function correctly when firewall was disabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS980M	GS900MX	XS900MX	GS900Mv2	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63442	**L2 Multicast**	Previously, IGMP Snooping would not forward multicast packets from a non-router port to a router port. 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-63572	**L2 Multicast**	Previously, after a second VLAN configuration change, multicast traffic could stop being forwarded to the multicast network. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-63548	**System**	Previously, a system restart could potentially occur when running an automated software recovery to reset a link on the SBx81CFC960. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-61890	**VCStack**	Previously, it was possible for backup stack members to not initialise properly after a rolling reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	–	–	Y	–	–	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-63005	**VLAN**	Previously, counters for L3 interfaces were not being displayed in the command: **show interface**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–

What's New in Version 5.4.9-0.5

Product families supported by this version:

AR4050S
AR3050S
AR2050V
AR2010V
AR1050V
FS980M Series
GS900MX/MPX Series
GS970M Series
GS980M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220 Series
x230 Series
x310 Series
IX5-28GPX
x510 Series
x530 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100: SBx81CFC960
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-0.5.

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: Software version 5.4.9-0.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 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 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 59 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 61.

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	GUI File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	05/2019	FS980-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	05/2019	GS900-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2019	GS970-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS980M/52 GS980M/52PS* *(available Q4 2019)	GS980M	05/2019	GS980M-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
XS916MXT XS916MXS	XS900MX	05/2019	XS900-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	05/2019	IE200-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE300-12GT IE300-12GP	IE300	05/2019	IE300-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE210L-10GP IE210L-18GP	IE210L	05/2019	IE210-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE510-28GSX-80	IE500	05/2019	IE510-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x220-28GS x220-52GT x220-52GP	x220	05/2019	x220-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2019	x230-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x310-26FT x310-50FT x310-26FP x310-50FP	x310	05/2019	x310-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IX5-28GPX	IX5	05/2019	IX5-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65

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

Models	Family	Date	Software File	GUI File
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	05/2019	x510-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x530-28GTXm x530-28GPXm	x530	05/2019	x530-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2019	x550-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	05/2019	x930-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x950-28XSQ	x950	05/2019	x950-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx908 GEN2	SBx908 GEN2	05/2019	SBx908NG-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx81CFC960	SBx8100	05/2019	SBx81CFC960-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR4050S AR3050S	AR-series UTM firewalls	05/2019	AR4050S-5.4.9-0.5.rel AR3050S-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR2050V AR2010V AR1050V	AR-series VPN firewalls	05/2019	AR2050V-5.4.9-0.5.rel AR2010V-5.4.9-0.5.rel AR1050V-5.4.9-0.5.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AMF Cloud		05/2019	vaa-5.4.9-0.5.iso (VAA OS) vaa-5.4.9-0.5. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-0.5.vhd (for Microsoft Azure)	

New platform

Software version 5.4.9-0.5 introduces support for the Secure VPN Router: **AR1050V**. For more information on this product, see the datasheet.

Note: The GUI file to use with the AR1050V is awplus-gui_549_12.gui.

ISSU compatibility with this software version

Please note that ISSU upgrade is not supported between software versions 5.4.9-0.3 and 5.4.9-0.5. However, ISSU upgrades are compatible between versions 5.4.9-0,1, 2, and 3.

Unsupported devices

Version 5.4.9-0.x does not support:

- SBx81CFC400 control cards (it does support SBx81CFC960 control cards).

Enhancements

CR	Module	Description	FS980M	GS980M	GS970M	GS900MX	XS900MX	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-2790	**VCStack**	With this software update, it is now possible to use Disabled Master Monitoring on a stack using **VCStack Plus**. This is where two stacked SBx8100 chassis, each containing two CFC960s are linked via short distance cabling or long distance fiber connections. Each CFC960 Ethernet interface must be connected to an out-of-band (Layer 2) network. The out-of-band Ethernet port (eth0) must be configured as a **resiliency** port with the command: `awplus(config)#stack resiliencylink eth0` Command information: ■ The global configuration command **stack disabled-master-monitoring** is supported on the SBx81CFC960. ■ The global configuration command **stack resiliencylink <interface-name>** is supported on the SBx81CFC960. Note, the only supported interface is “eth0”. ■ The show command **show stack detail** displays the resiliency link information on the SBx81CFC960.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–

Issues Resolved in Version 5.4.9-0.5

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

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	GS900Mv2	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63328	**AMF**	Previously, on very rare occasions, a VAA with containers configured could fail to initialise. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-62891	**AMF** **Software Licensing**	Previously, after an AMF member was replaced with another member, a warning log regarding “temporary transfer of external licenses” would be generated, even when there was no license required on the device. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-61383	**Antivirus** **Web Control**	Previously, if Antivirus or Web-control was disabled while a high volume of HTTP traffic was being processed the internal "squid"proxy module could suffer a critical error and be restarted. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-62468	**CLI**	With this software update, the command: **show radius local-server user** will no longer show hashed user passwords	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-63312	**Energy Efficient Ethernet**	Previously, ports linked up and configured for EEE would not enter LPI mode immediately after a reboot unless the links were subsequently taken down and up again, either physically or via a shutdown or no shutdown sequence. This issue has been resolved..	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–
CR-63313	**Energy Efficient Ethernet**	Previously, 10G links with Energy Efficient Ethernet (EEE) enabled could drop packets or lock up at certain low packet rates. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–
CR-63290	**IPv6**	Previously, it was possible for a device to lock-up when ECMP routes were in use. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	GS900Mv2	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-62233	**L2 Multicasting**	Previously, when NLB configured with **arp-mac-disparity multicast-igmp enabled**, packets could still be incorrectly flooded to each of the ports in the VLAN. This issue has been resolved.	–	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR-63211	**L2 Switching**	Previously, a full duplex port would sometimes incorrectly run at half duplex. This issue has been resolved.	Y	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	GS900Mv2	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61345	**L2TPv3**	Previously, packets exceeding the MTU would be dropped silently as the "Don't Fragment" bit is set by default. With this software update, a new command has been implemented that clears the DF bit allowing packets greater than the MTU to be transmitted. The new command is: `tunnel df {set|clear}` The purpose of this new command is to specify whether the DF bit should be set or not on outgoing packets from l2tpv3 tunnels. This new command gives the user the opportunity to clear the DF bit allowing packets greater than the MTU to be fragmented and transmitted via the L2TPv3 Ethernet pseudo-wire. The default behaviour is unchanged, that is that the DF bit is always set on outgoing packets. Note: If fragmentation of larger packets occur as a result of setting tunnel Do Not Fragment bit to clear, this may slightly increase latency of the associated traffic flow traversing the VPN, due to the fragmentation and re-assembly that occurs. Example syntax: To specify the DF bit behavior on L2TPv3 tunnels, use the following commands: `awplus(config)# interface tunnel3` `awplus(config-if)# tunnel mode l2tpv3` `awplus(config-if)# tunnel df clear`	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	GS900Mv2	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63229	**L3 Multicast**	Previously, L3 multicast traffic could sometimes fail to recover after a master failover if there were 31K or more multicast streams involved. 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-62073	**LACP**	This software update fixes a memory leak issue that could occur when there were 128 dynamic LACP links being configured. 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-63100	**LACP**	Previously, the error message: “Failed to set STP state for interface xxxx. STP Instance 0" (aggregator interface)" would be displayed when a device started up and there was a large number of aggregator interfaces configured. This issue has been resolved.	Y	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-62975	**Logging**	Previously, it was possible that sometimes a remote-login session shell process (IMISH) could keep running in the background when the corresponding session exited abnormally. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-62976	**Logging**	Previously, under rare circumstances, the syslog-ng module might restart unnecessarily. 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-63191	**Logging**	Previously, it was possible for the syslog configuration **reload rate-limiting** mechanism to stop working correctly on some platforms after 248 days of uptime. This could result in changes to the syslog configuration taking longer than expected to take effect. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	GS900MVv2	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-62287	**Loop Protection**	Previously, the **show loop-protection** command displayed ports out of order after a late stack member late. This issue has been resolved, now the ports are displayed in the correct order.	–	–	Y	Y	Y	–	–	Y	–	–	Y	Y	Y	–	Y	–	Y	Y	–	–	–	–	–	–
CR-63325	**Pluggable Transceivers** **PoE**	Previously, the **show power-inline** command would become slow to display the output when there were PoE faults. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-63493	**Pluggable Transceivers**	This software update addresses two issues: ■ Previously, it was possible for an IE300 series switch to stop detecting SFP insertions and removals. ■ Previously, the insertion and removal of SFPs and the link up and down events for SFPs on x230 series and IE300 series switches, could result in the other SFP links to flip. These issues have been resolved.	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-62223	**PoE**	Previously, a third party powered device could fail to power up when attached to an IE300 series switch. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-63189	**PoE**	Previously, a PoE "over budget message" would sometimes be incorrectly displayed after a power device was connected to the PoE port. This issue has been resolved.	–	–	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–	– *
CR-63293	**Port Configuration**	Previously, the SFP ports on a GS980MX series switch could sometimes fail to link up. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-62879	**SSL**	With this software update, internal OpenSSL daemon has been upgraded to version 1.0.2r to address the security vulnerability addressed in CVE-2019-1559|https://nvd.nist.gov/nvd.cfm?cvename=CVE-2019-1559].	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	XS900MX	GS900MXv2	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63448	**Switch**	Previously, on an SBx81GC40 link card, the front panel port LEDs would not flash when there was link activities. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-63546	**Tunnelling MAP-E**	Previously, in a MAP-E configuration, a system reboot could occur if the upstream interface went up and down quickly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-63182	**VCStack**	Previously, a x530 series stack could fail to form following a master failover when using SFP+ DAC cables or SFP+ fibre pluggables as stacking ports. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-62445	**VCStack**	Previously on SBx908 GEN2 and x950 series switches, in rare cases QSFP ports might not link up correctly. As a result, the stack would not form. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–
CR-62838	**VCStack**	Previously, under very rare circumstances, on a SBx8100 switch, a port might cease to forward traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-63266	**VCStack**	Previously, if a stack member joined a stack after it was formed, a loop-detection configuration may not have been applied correctly. This issue has been resolved.	–	–	Y	Y	Y	–	–	Y	–	–	Y	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-63398	**VCStack**	This software update supports configuring a static-channel group for VLAN stacking.	–	–	Y	Y	Y	–	–	Y	–	–	Y	Y	Y	–	Y	–	–	–	Y	–	–	–	–	–
CR-62263	**Web API**	Previously, the web server could stop and restart while using the terminal provided by Vista Manager or the device GUI. On the third time that the web server stopped, it would not restart. As a result, the Vista Manager would not be able to access the area and the device GUI would not be able to access the device. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

What’s New in Version 5.4.9-0.3

Product families supported by this version:

AR4050S
AR3050S
AR2050V
AR2010V
FS980M Series
GS900MX/MPX Series
GS970M Series
GS980M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220 Series
x230 Series
x310 Series
IX5-28GPX
x510 Series
x530 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100: SBx81CFC960
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-0.3.

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**: Software version 5.4.9-0.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 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 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 59 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 61.

⚠ **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	GUI File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	04/2019	FS980-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	04/2019	GS900-5.4.9-0.30.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2019	GS970-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS980M/52 GS980M/52PS* *(available Q4 2019)	GS980M	04/2019	GS980M-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
XS916MXT XS916MXS	XS900MX	04/2019	XS900-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	04/2019	IE200-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE300-12GT IE300-12GP	IE300	04/2019	IE300-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE210L-10GP IE210L-18GP	IE210L	04/2019	IE210-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE510-28GSX-80	IE500	04/2019	IE510-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x220-28GS x220-52GT x220-52GP	x220	04/2019	x220-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2019	x230-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x310-26FT x310-50FT x310-26FP x310-50FP	x310	04/2019	x310-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IX5-28GPX	IX5	04/2019	IX5-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65

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

Models	Family	Date	Software File	GUI File
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	04/2019	x510-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x530-28GTXm x530-28GPXm	x530	04/2019	x530-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2019	x550-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	04/2019	x930-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x950-28XSQ	x950	04/2019	x950-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx908 GEN2	SBx908 GEN2	04/2019	SBx908NG-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx81CFC960	SBx8100	04/2019	SBx81CFC960-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR4050S AR3050S	AR-series UTM firewalls	04/2019	AR4050S-5.4.9-0.3.rel AR3050S-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR2050V AR2010V	AR-series VPN firewalls	04/2019	AR2050V-5.4.9-0.3.rel AR2010V-5.4.9-0.3.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AMF Cloud		04/2019	vaa-5.4.9-0.3.iso (VAA OS) vaa-5.4.9-0.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-0.3.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.9-0.x does not support:

- SBx81CFC400 control cards (it does support SBx81CFC960 control cards)

Issues Resolved in Version 5.4.9-0.3

This AlliedWare Plus maintenance version includes the following resolved issues:

CR	Module	Description	FS980M	GS980M	GS970M	GS900MX	XS900MX	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63182	**ARP Neighbor Discovery**	Previously, a x530 series stack could fail to form following a master failover when using SFP+ DAC cables or SFP+ fibre pluggables as stacking ports. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-63325	**Pluggable Transceivers**	Previously, the "show power-inline" command could become slow to display the output when there were PoE faults. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-63413	**Switch**	Occasionally, on x550 series switches, MAC learning could fail on some ports. This issue has been resolved	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–

What’s New in Version 5.4.9-0.2

Product families supported by this version:

AR4050S
AR3050S
AR2050V
AR2010V
FS980M Series[1]
GS900MX/MPX Series
GS970M Series
GS980M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220 Series
x230 Series
x310 Series
IX5-28GPX
x510 Series
x530 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100: SBx81CFC960
AMF Cloud

[1] FS980M Series switches were not supported by 5.4.9-0.1. They are supported by software version 5.4.9-0.2 onwards.

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-0.2.

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

Caution: Software version 5.4.9-0.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 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 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 59 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 61.

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	GUI File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	04/2019	FS980-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	04/2019	GS900-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2019	GS970-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS980M/52 GS980M/52PS* *(available Q4 2019)	GS980M	04/2019	GS980M-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
XS916MXT XS916MXS	XS900MX	04/2019	XS900-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	04/2019	IE200-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE300-12GT IE300-12GP	IE300	04/2019	IE300-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE210L-10GP IE210L-18GP	IE210L	04/2019	IE210-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE510-28GSX-80	IE500	04/2019	IE510-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x220-28GS x220-52GT x220-52GP	x220	04/2019	x220-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2019	x230-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x310-26FT x310-50FT x310-26FP x310-50FP	x310	04/2019	x310-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IX5-28GPX	IX5	04/2019	IX5-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65

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

Models	Family	Date	Software File	GUI File
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	04/2019	x510-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x530-28GTXm x530-28GPXm	x530	04/2019	x530-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2019	x550-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	04/2019	x930-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x950-28XSQ	x950	04/2019	x950-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx908 GEN2	SBx908 GEN2	04/2019	SBx908NG-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx81CFC960	SBx8100	04/2019	SBx81CFC960-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR4050S AR3050S	AR-series UTM firewalls	04/2019	AR4050S-5.4.9-0.2.rel AR3050S-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR2050V AR2010V	AR-series VPN firewalls	04/2019	AR2050V-5.4.9-0.2.rel AR2010V-5.4.9-0.2.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AMF Cloud		04/2019	vaa-5.4.9-0.2.iso (VAA OS) vaa-5.4.9-0.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-0.2.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.9-0.x does not support:

- SBx81CFC400 control cards (it does support SBx81CFC960 control cards)

Issues Resolved in Version 5.4.9-0.2

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	FS980M	GS980M	GS970M	GS900MX	XS900MX	IE200, IE210L	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-63211	**VCStack Unicast Forwarding**	Previously, ports on FS980M series switches would sometimes incorrectly run at half duplex. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

What’s New in Version 5.4.9-0.1

Product families supported by this version:

AR4050S
AR3050S
AR2050V
AR2010V
FS980M Series[1]
GS900MX/MPX Series
GS970M Series
GS980M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220 Series
x230 Series
x310 Series
IX5-28GPX
x510 Series
x530 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100: SBx81CFC960
AMF Cloud

[1] FS980M Series switches are not supported by 5.4.9-0.1. They are supported by software version 5.4.9-0.2 onwards.

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-0.1.

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: Software version 5.4.9-0.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 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 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 59 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 61.

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	GUI File
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	FS980M Series switches are not supported by 5.4.9-0.1. They are supported by software version 5.4.9-0.2 onwards.		See "Installing and Accessing the Web-based Device GUI" on page 65
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	03/2019	GS900-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2019	GS970-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
GS980M/52 GS980M/52PS* *(available Q4 2019)	GS980M	03/2019	GS980M-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
XS916MXT XS916MXS	XS900MX	03/2019	XS900-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2019	IE200-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE300-12GT IE300-12GP	IE300	03/2019	IE300-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE210L-10GP IE210L-18GP	IE210L	03/2019	IE210-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IE510-28GSX-80	IE500	03/2019	IE510-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x220-28GS x220-52GT x220-52GP	x220	03/2019	x220-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2019	x230-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2019	x310-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
IX5-28GPX	IX5	03/2019	IX5-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65

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

Models	Family	Date	Software File	GUI File
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	03/2019	x510-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x530-28GTXm x530-28GPXm	x530	03/2019	x530-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2019	x550-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2019	x930-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
x950-28XSQ	x950	03/2019	x950-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx908 GEN2	SBx908 GEN2	03/2019	SBx908NG-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
SBx81CFC960	SBx8100	03/2019	SBx81CFC960-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR4050S AR3050S	AR-series UTM firewalls	03/2019	AR4050S-5.4.9-0.1.rel AR3050S-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AR2050V AR2010V	AR-series VPN firewalls	03/2019	AR2050V-5.4.9-0.1.rel AR2010V-5.4.9-0.1.rel	See "Installing and Accessing the Web-based Device GUI" on page 65
AMF Cloud		03/2019	vaa-5.4.9-0.1.iso (VAA OS) vaa-5.4.9-0.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-0.1.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.9-0.x does not support:

- SBx81CFC400 control cards (it does support SBx81CFC960 control cards)

New Features and Enhancements

This section summarizes the new features in 5.4.9-0.1 since 5.4.8-2.2:

- "Allied Telesis Autonomous Management Framework (AMF) enhancements" on page 43
- "Multipoint VPN" on page 46
- "IPv4 traffic selectors on IPsec IPv6 tunnels" on page 46
- "IPv6 transition technologies: lw4o6, DS-Lite & MAP-E" on page 47
- "Fragmentation of L2TPv3 encapsulated packets" on page 48
- "Using statically-configured DNS servers in preference to dynamically-learned DNS servers" on page 48
- "Support for 32K multicast groups on SwitchBlade x908 GEN2" on page 48
- "Support for 1024 PIM interfaces on x950 Series switches" on page 49
- "Virtual Chassis Stacking (VCStack) enhancements on x950 Series switches" on page 49
- "Disabling a faulty XEM on SBx908 GEN2 and x950 Series switches" on page 49
- "Increased flexibility for link aggregation groups" on page 49
- "2.5Gbps/5Gbps support on x530 Series switches" on page 50
- "VLAN ID translation on x530 Series switches" on page 50
- "Upstream Forwarding Only (UFO) on x530 Series switches" on page 51
- "RADIUS proxy on x530 Series switches" on page 51
- "Display of voltage faults on x530 and x220 Series switches" on page 52
- "Voice VLAN with authentication on GS900MX/MPX Series switches" on page 52
- "Hairpin links on OpenFlow switches" on page 52
- "Detection of PoE legacy devices is now disabled by default" on page 53
- "PoE switches boot up even if there is a PoE hardware fault" on page 53

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 58.

Allied Telesis Autonomous Management Framework (AMF) enhancements

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

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

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

Version 5.4.9-0.1 includes the following AMF enhancements.

AMF secure virtual-links

From 5.4.9-0.1 onwards, you can create secure AMF virtual-links by encapsulating the L2TPv3 frames of the virtual-link with IPsec. AMF secure virtual-links are available on the following products:

- AMF Cloud/ VAA
- AR4050S, AR3050S, AR2050V, AR2010V
- x220, x230L, x230, x310, IX5, x510L and x510 Series

For example to secure an existing AMF virtual-link with link-id '5' and pre-shared key 'secure-password', use the following command:

```
awplus(config)#atmf virtual-link id 5 protection ipsec key
secure-password
```

Note that each side of the virtual-link must be configured with the same protection parameters.

Dynamic tunnel addresses for AMF virtual-links

From version 5.4.9-0.1 onwards, you can configure an AMF virtual-link by using a dynamic local and/or a dynamic remote tunnel address.

Dynamic local address

If an interface acquires its IP address dynamically then the local side of the tunnel can be specified by using the interface's name instead of using its IP address. When using a dynamic local address the remote address of the other side of the virtual-link must be configured with either:

- the IP address of the NAT device the dynamically configured interface is behind, or
- 0.0.0.0, if the virtual-link is configured as a secure virtual-link.

For example, if you wish to create a virtual -link between Site A and Site B where Site A is behind a NAT device with a known static public IP address, use the following commands:

```
siteA(config)#atmf virtual-link id 1 interface eth0 remote-id 1
remote-ip 192.0.2.33
```

```
siteB(config)#atmf virtual-link id 1 ip 192.0.2.33 remote-id 1
remote-ip 192.0.2.34
```

Dynamic remote address

Using a dynamic address for the remote side of an AMF virtual-link is only available on secure AMF virtual-links.

When the IP address of the remote side of a secure AMF virtual-link is unknown you can configure an AMF virtual-link by specifying a dynamic address for the remote side. This is done by setting the remote-ip parameter to 0.0.0.0.

For example, if you wish to create a secure virtual -link between Site A and Site B where Site A has a dynamic local address, use the following commands:

```
siteA(config)#atmf virtual-link id 1 interface eth0 remote-id 1
remote-ip 192.0.2.33
```

```
siteA(config)#atmf virtual-link id 1 protection ipsec key secure-
password
```

```
siteB(config)#atmf virtual-link id 1 ip 192.0.2.33 remote-id 1
remote-ip 0.0.0.0
```

```
siteB(config)#atmf virtual-link id 1 protection ipsec key secure-
password
```

Note that a dynamic remote address cannot be used on both sides of a secure AMF virtual-link.

AMF node recovery and provisioning enhancements

From version 5.4.9-0.1 onwards, enhancements to the AMF node recovery and provisioning feature allows you to:

- Replace an older model AlliedWare Plus device with a newer model equivalent device, even if the replacement device does not belong to the same product family as the device being replaced.
- Provision a node with several different device types so that the new node will automatically select the correct device type when it is attached to the network.

Node recovery

This occurs automatically when a device listed in the following table is substituted with a valid replacement device:

Table 2: Permitted device substitutions

Original device type	Replacement device type
x210 series	x230 series
x510 series	x530 series
IX5-28GPX	x530 series
x610 series	x530 series
x900 series	x930 series or x950 series
x930- series	x950 series

Provisioning

There is a new AMF provisioning mode command that accepts a device type. This allows you to provision a device-specific backup for a node.

```
awplus#atmf provision node <node-name> [device <device-type>]
```

Note that all existing provisioning commands have moved to this new mode.

To use this new feature you should:

- Make a device type specific backup by switching to provisioning mode using the new **atmf provision node** command with a device-type parameter.
- Use the appropriate procedure to create or clone a provisioned backup.
- Run the **atmf provision** command on the interface that the replacement device will be plugged in to.

When a clean device is then plugged into the port it will recover using the relevant device type. Note that only the device substitutions listed in the previous table are permitted.

If you use the **atmf provision node** command without the **device-type** parameter then it will result in provisioning that is backwards compatible with previous versions of AMF.

For a detailed instructions on AMF provisioning, see the provisioning chapter of the AMF Feature Overview and Configuration Guide.

Table 3: Permitted device substitutions

Original device type	Replacement device type
x210 series	x230 series
x510 series	x530 series
IX5-28GPX	x530 series
x610 series	x530 series
x900 series	x930 series or x950 series
x930- series	x950 series

Multipoint VPN

Available on AR-series devices

Version 5.4.9-0.1 adds support for multipoint VPN.

Multipoint VPN is a term that describes the use of point-to-multipoint tunnels to enhance traditional point-to-point VPN networks. Traditional VPN network tunnels are point-to-point with a single destination. This works well if you only have two sites to connect. But if you have many sites to connect, for example a head office and many branch offices, then it requires complex configuration and maintenance. Each branch site needs a separate tunnel configured at the head office. The more branch sites you add, then the more tunnels you need to configure.

GRE (Generic Routing Encapsulation) supports Multipoint VPN using point-to-multipoint mode as the transport protocol for IPv4 and IPv6 traffic. Multipoint VPN simplifies configuration and allows a single tunnel to have multiple endpoints. For example, this means that only a single tunnel configuration is required at a head office to connect to all other branch offices.

For more information about how to configure Multipoint VPN, see the GRE and Multipoint VPNs Feature Overview and Configuration Guide.

IPv4 traffic selectors on IPsec IPv6 tunnels

Available on AR-series devices

From 5.4.9-0.1 onwards, IPv4 traffic selectors are supported on IPsec IPv6 tunnels. It is now possible to optionally configure IPv4 traffic selectors over an IPsec IPv6 tunnel.

For example, if you wanted to configure an IPv6 VPN between the main office and remote office. The Ethernet WAN interfaces can be configured using IPv6 addresses, and the tunnel and VLAN interfaces configured with IPv4 addresses. The IPv4 traffic is encapsulated and transported within the IPv6 VPN.

Tunnel selectors can then be configured to match IPv4 traffic to be encrypted and transported via the IPv6 IPsec VPN.

Note that the default selectors for this tunnel type will match only IPv6 traffic, unless selectors are explicitly configured.

For more information, see the new configuration example “IPv4 over IPv6 tunnel” in the IPsec Feature Overview and Configuration Guide.

IPv6 transition technologies: lw4o6, DS-Lite & MAP-E

Available on AR-series devices

Lightweight 4over6 (lw4o6)

From 5.4.9-0.1 onwards, Lightweight 4over6 is supported on AR-series devices.

Lightweight 4over6 is an IPv6 transition technology. As IPv4 and IPv6 networks are not directly inter-operable, transition technologies permit hosts on either network type to communicate with any other host. Transition technologies bridge between IPv4 and IPv6 and allow the two versions to work side by side.

Lightweight 4over6 (lw4o6) is a method of tunneling IPv4 packets over an IPv6 network. It provides a way for ISPs that operate over a pure IPv6 network to continue to offer IPv4 Internet services to customers. Lw4o6 is defined in RFC 7596, which in turn refers to a wide range of other related RFCs. It is an extension to the Dual-Stack Lite (DS-Lite, RFC 6333) architecture.

Lw4o6 moves the Network Address and Port Translation (NAPT44) function from the service provider to the CPE. This improves the scalability of the translation infrastructure as it removes the requirement for a Carrier Grade NAT function in the tunnel concentrator and reduces the amount of centralized state that must be held to a per-subscriber level. In order to delegate the NAPT44 function and make IPv4 address sharing possible, port-restricted IPv4 addresses are allocated to the CPEs.

Enhancements to Dual Stack-Lite (DS-Lite)

Recent previous releases of AlliedWare Plus contained support for DS-Lite. From 5.4.9-0.1 onwards, you can configure DS-Lite as a Virtual Tunnel Interface (VTI) tunnel. This makes it consistent with other AlliedWare Plus tunnel features.

DS-Lite is an IPv6 transition solution for ISPs with IPv6 infrastructure that wish to connect their IPv4 subscribers to the Internet. DS-Lite uses IPv4-in-IPv6 tunneling to send a subscriber's IPv4 packet through a tunnel on the IPv6 access network to the ISP.

DS-Lite allows a service provider to continue support for existing IP v4 services, while also providing incentive for the deployment of IPv6. DS-Lite decouples the deployment of IPv6 in the service provider's network from the rest of the Internet, making the incremental deployment of IPv6 services within the ISP network easier.

MAP-E

From 5.4.9-0.1 onwards, MAP-E is supported on AR-series devices. MAP-E is a method of tunneling IPv4 packets over an IPv6 network. It is an IPv6 transition technology that provides a way for ISPs that operate over a pure IPv6 network to continue to offer IPv4 Internet services to customers. It supports more efficient use of IPv4 addresses through "Address plus Port" address sharing.

In addition to providing a way for IPv4 traffic to traverse the ISP's network to reach the internet, it also allows for direct connections between customer premises within the ISP's MAP domain over the IPv6 network.

IPv6 transition technology guide

You can find information about these transition technologies in the new Transitioning IPv4 to IPv6 Feature Overview and Configuration Guide. This guide combines all three IPv4 to IPv6 transition mechanisms into one document.

Fragmentation of L2TPv3 encapsulated packets

Available on AR-series devices

From 5.4.9-0.1 onwards, it is possible to configure AR-series devices to allow fragmentation of L2TPv3 encapsulated packets. This may be necessary when an L2TPv3 tunnel is connected to a bridge and MTU-exceeded messages cannot be sent back to clients.

To turn on this behavior, use the following commands in Interface mode for the tunnel, to clear the Don't Fragment bit:

```
awplus(config-if)#tunnel df clear
```

Using statically-configured DNS servers in preference to dynamically-learned DNS servers

Applies to all devices that support DNS

From 5.4.9-0.1 onwards, it is possible to set the device to use statically-configured domain name servers in preference to dynamically learned domain name servers. To do this, use the new command:

```
awplus(config)#ip name-server preferred-order static
```

This new command can be use with both IPv4 and IPv6 servers.

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

Support for 32K multicast groups on SwitchBlade x908 GEN2

From 5.4.9-0.1 onwards, support for multicast group entries has been increased from 8K (8192) to 32K (32768) on the SBx908 GEN2.

The multicast entry limits assume a maximum number of entries to mean a combined count of (*,G) and (S,G) entries. The limit of 32k means up to 32K (*,G) or split as 16K (*,G) and 16K (S,G).

If the SBx908 GEN2 is acting as an IGMP querier, and you have 8192 or more multicast groups, you must turn off IGMP report suppression on all VLANs requiring IGMP group joins. To do this, use the command:

```
awplus(config)#no ip igmp snooping report-suppression
```

There are also two new commands that control the handling of packets received on an unexpected ingress VLAN:

```
awplus(config)#ip pim [vrf <vrf-name>] sparse-mode wrong-vif-suppression
awplus(config)#ip pim [vrf <vrf-name>] dense-mode wrong-vif-suppression
```

If these commands are used, when a multicast packet is received on the wrong interface, a blocking entry is added to hardware to prevent packets coming up to the CPU again. This helps to reduce the CPU load on switches.

For more information, see the following guides, especially the "Support for Large Multicast Networks" section in the PIM-SM and IGMP Guides:

- IGMP: IGMP/MLD Feature Overview and Configuration Guide

- PIM-SM: PIM-SM Feature Overview and Configuration Guide
- PIM-DM: PIM-DM Feature Overview and Configuration Guide.

Support for 1024 PIM interfaces on x950 Series switches

From 5.4.9-0.1 onwards, support for PIM interfaces has been increased to 1024 on the x950 Series.

For more information, see the following guides, especially the “Support for Large Multicast Networks” section in the PIM-SM Guide:

- PIM-SM: PIM-SM Feature Overview and Configuration Guide
- PIM-DM: PIM-DM Feature Overview and Configuration Guide.

Virtual Chassis Stacking (VCStack) enhancements on x950 Series switches

Version 5.4.9-0.1 extends VCStack to support stacking of up to four x950 Series switches, from the previous limit of two switches.

It also enables stacking over 10G SFP+ or 40G QSFP+ modules.

For detailed instructions about how to create a VCStack, see the VCStack Feature Overview and Configuration Guide or the Installation Guide: ATx950-28XSQ Switch and VCStack.

Disabling a faulty XEM on SBx908 GEN2 and x950 Series switches

From 5.4.9-0.1 onwards, a XEM can be kept in a disabled state while a reboot or a hot swap on that XEM bay occurs. This means you can keep a faulty XEM disabled while waiting for its replacement to arrive.

This has been achieved by moving the command "no xem <bayid> enable" to global configuration mode (and the command “xem <bayid> enable”). Saving the “no” variant of this command keeps the XEM disabled even during a reboot.

Increased flexibility for link aggregation groups

Available for SBx908 GEN2, SBx8100, x950, x930, x550, x530, x510, x510L and IX5 Series

From 5.4.9-0.1 onwards, when creating link aggregation groups (LAGs), you can configure any combination of dynamic and static channel groups, up to the maximum number of LAGs for that switch.

For example, in earlier releases on an x510 Series switch, you could create up to 32 dynamic (LACP) channel groups and up to 96 static channel groups, to a total of 128 LAGs. Now, you can create up to 128 dynamic channel groups, or up to 128 static channel groups, or any combination of dynamic and static groups, up to a total of 128.

For more information about LAGs, see the Link Aggregation Feature Overview and Configuration Guide.

2.5Gbps/5Gbps support on x530 Series switches

Version 5.4.9-0.1 enables ports 21-24 of the AT-x530-28GTXm and AT-x530-28GPXm to run at 2.5 Gbps or 5 Gbps. This is as well as those ports' existing 1 Gbps or 100 Mbps speed options. The ports will autonegotiate speed by default.

To set the speed to 2.5 Gbps, use the following command in Interface mode:

```
awplus(config-if)#speed 2500
```

To set the speed to autonegotiate 2.5 Gbps, use the following command in Interface mode:

```
awplus(config-if)#speed 2500 auto
```

To set the speed to 5 Gbps, use the following command in Interface mode:

```
awplus(config-if)#speed 5000
```

To set the speed to autonegotiate 5 Gbps, use the following command in Interface mode:

```
awplus(config-if)#speed 5000 auto
```

VLAN ID translation on x530 Series switches

From 5.4.9-0.1 onwards, AlliedWare Plus supports VLAN ID translation on x530 Series switches. A number of other AlliedWare Plus switches already support VLAN ID Translation.

VLAN ID translation translates a VLAN's VLAN ID to another value for use on the wire.

In Metro networks, it is common for the Network Service Provider to give each customer their own unique VLAN, yet at the customer location, give all the customers the same VLAN ID for tagged packets to use on the wire. VLAN ID translation can be used by the Service Provider to change the tagged packet's VLAN ID at the customer location to the VLAN-ID for tagged packets to use within the NSP's network.

VLAN ID translation is also useful in Enterprise environments where it can be used to merge two networks together without manually reconfiguring the VLAN numbering scheme. This situation can occur if two companies have merged and the same VLAN ID is used for two different purposes.

Similarly, within a Network Service Provider's network, Layer 2 networks may need to be rearranged, and VLAN ID translations make such rearrangement more convenient.

For configuration details, see the VLANs Feature Overview and Configuration Guide.

Upstream Forwarding Only (UFO) on x530 Series switches

From 5.4.9-0.1 onwards, AlliedWare Plus supports Upstream Forwarding Only (UFO) on x530 Series switches. A number of other AlliedWare Plus switches already support UFO.

UFO enables you to create Private VLANs. Private VLANs are needed because some services need to control connections between the port and upstream device. For example, in applications such as Triple-Play networks, VLANs are often shared across subscribers and provide a specific service or set of services. Such VLANs are called Service VLANs.

For example, an Internet Service VLAN that is shared amongst subscribers needs to block subscribers from sending to other subscribers, while a shared Voice Service VLAN needs to let subscribers forward voice traffic directly with each other. Because these two VLANs often have the same port memberships, there is a need to allow isolated VLANs to co-exist with regular VLANs on the same ports. Enabling Private VLAN UFO on the Internet VLAN will provide isolation, while allowing the Voice VLAN to remain operating as a standard or regular VLAN.

UFO is configured on individual VLANs and blocks or isolates traffic at Layer 2. It blocks the forwarding of Ethernet frames between certain ports of a UFO VLAN while allowing forwarding of others. All data from ports associated with a UFO VLAN must be forwarded only to the upstream port, which is why it is called Upstream Forwarding Only.

UFO is configured on a per VLAN basis, and removes many of the Private VLAN trunk restrictions. This means that:

- Regular VLANs can now coexist with UFO VLANs on the same ports.
- VLANs can belong to different port groups.
- Ports do not all have to be trunk ports.

For configuration details, see the VLANs Feature Overview and Configuration Guide.

RADIUS proxy on x530 Series switches

From 5.4.9-0.1 onwards, AlliedWare Plus supports RADIUS proxy on x530 Series switches. Other AlliedWare Plus switches already support RADIUS proxy.

It is possible to configure a RADIUS proxy server so that remote RADIUS servers can hold the user database and validate Network Access Server (NAS) RADIUS requests.

- The NAS sends a RADIUS request to the RADIUS proxy server.
- The proxy server forwards the request to the first available RADIUS server.
- The RADIUS server processes the request and sends the response back to the proxy server.
- The proxy server then forwards the response to the NAS with an accept or reject message.

There are a variety of situations where a RADIUS proxy is useful. For example, multiple RADIUS servers could be configured to each hold a different user database for a specific purpose e.g. one for authenticating switch management sessions, one for authenticating VPN connections, and one for authenticating 802.1X sessions. In this situation it is convenient to use a single IP address on all the NASs to point to the RADIUS proxy server. This server then forwards the request to the correct RADIUS server holding the relevant user database.

For more information about RADIUS proxy see the RADIUS Feature Overview and Configuration Guide.

Display of voltage faults on x530 and x220 Series switches

From 5.4.9-0.1 onwards, if a voltage sensor on a x220 or x530 Series switch detects a fault, it will flash F on the 7-segment display, as well as updating the fault status in output of the “show system” and “show system environment” commands.

Voice VLAN with authentication on GS900MX/ MPX Series switches

From 5.4.9-0.1 onwards, it is possible to use Voice VLAN at the same time as the command "auth dynamic-vlan-creation type multi" on GS900MX/MPX Series.

Previously, this scenario was unsupported because of an issue that meant that after an IP phone had authenticated on the port and begun transmitting packets on the voice VLAN, if a subsequent device (such as a PC) were to authenticate on that port, the voice VLAN authentication would be disrupted. This caused the switch to drop the voice-VLAN tagged packets it received from the phone.

This issue has been resolved. Now, after an IP phone authenticates in this scenario and the voice VLAN is added to the port, subsequent authentication of other devices on the same port will not interfere with the voice VLAN.

For configuration details, see “Configure authentication for Voice VLAN using the local RADIUS server” in the LLDP Feature Overview and Configuration Guide.

Hairpin links on OpenFlow switches

Applies to all AlliedWare Plus switches that support the OpenFlow protocol, except for 50- and 52-port models

From 5.4.9-0.1 onwards, hairpin links are supported on OpenFlow switches. A hairpin link is where two ports in the switch are directly connected to each other. One of the ports is an OpenFlow port, the other a legacy (non-OpenFlow) port. This allows traffic to traverse between the OpenFlow controlled data plane and the legacy controlled data plane.

Note that hairpin links were also supported on software versions prior to 5.4.7.

Hairpin links are not available on the following 50- and 52-port models:

- x510-52GTX
- x510-52GPX
- x510DP-52GTX
- x510L-52GT
- x510-52GP
- x310-50FT
- x310-50FP

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

Detection of PoE legacy devices is now disabled by default

Applies to all AlliedWare Plus PoE switches except FS980M Series

From 5.4.9-0.1 onwards, detection of legacy PoE devices is disabled by default on all AlliedWare Plus PoE switches except FS980M Series.

If you need to enable detection of legacy devices, you can do so by using the following command:

```
awplus(config)#power-inline allow-legacy
```

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

PoE switches boot up even if there is a PoE hardware fault

Applies to all AlliedWare Plus PoE switches

From 5.4.9-0.1 onwards, if PoE hardware fails at startup on a switch, the switch will no longer cycle-reboot. Instead, the switch will bootup to allow user to access the CLI.

Important Considerations Before Upgrading

This section describes changes that are new in 5.4.9-x.x and may affect your network behavior if you upgrade. Please read it carefully before upgrading.

It describes the following changes:

- Detection of PoE legacy devices is now disabled by default
- Change in handling of RADIUS session-timeout attribute of zero

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

- Software Release Licensing
- ISSU (In-Service Software Upgrade) on SBx8100 with CFC960
- Upgrading a VCStack with reboot rolling
- Forming or extending a VCStack with auto-synchronization
- AMF software version compatibility
- Upgrading all switches in an AMF network

If you are upgrading from an earlier version than 5.4.9-x.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.4.8-1.x version, please check the 5.4.8-2.x release note. Release notes are available from our website, including:

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

Detection of PoE legacy devices is now disabled by default

Applies to all AlliedWare Plus PoE switches except FS980M Series

From 5.4.9-0.1 onwards, detection of legacy PoE devices is disabled by default on all AlliedWare Plus PoE switches except FS980M Series.

If you need to enable detection of legacy devices, you can do so by using the following command:

```
awplus(config)#power-inline allow-legacy
```

Change in handling of RADIUS session-timeout attribute of zero

Applies to all AlliedWare Plus devices

From 5.4.9-0.1 onwards, if a RADIUS server sends an access-accept message that has a session-timeout of zero, the session-timeout is ignored and the supplicant is authorized and can connect. In 5.4.8-2.x, the supplicant would be unable to connect.

Software Release Licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.4.9 license on your switch if you are upgrading to 5.4.9-0.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 59 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 61.

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

ISSU is available on standalone SBx8100 Series switches with dual CFC960 control cards, and on switches using VCStack Plus™ to create a single virtual unit out of two chassis (where each chassis has a pair of CFC960 control cards). ISSU allows you to upgrade the software release running on the CFCs with no disruption to network traffic passing through the chassis.

You cannot use ISSU to upgrade to 5.4.9-0.1 from any previous software version.

Upgrading a VCStack with reboot rolling

Applies to all stackable AlliedWare Plus switches

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack. You can use the **reboot rolling** command to upgrade to 5.4.9-0.x from:

- 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 reboot rolling, first enter the **boot system** command, which will install the new release file on all stack members. Then enter the **reboot rolling** command. Note that reboot rolling is not supported on SBx8100.

You cannot use rolling reboot to upgrade directly to 5.4.9-0.x from 5.4.4-0.x or earlier versions.

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. Auto-synchronization is supported between 5.4.9-0.x and:

- 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 5.4.9-0.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 5.4.9-0.x are compatible with nodes running:

- 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 switches 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, XS900MX, x220, and GS980M 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                    : 5.4.9
Customer name                   : ABC Consulting
Quantity of licenses            : 1
Type of license                 : Full
License issue date              : 20-Mar-2019
License expiry date             : N/A
Release                         : 5.4.9
```

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                  : 5.4.9
Customer name                 : ABC Consulting
Quantity of licenses          : -
Type of license               : Full
License issue date            : 20-Mar-2019
License expiry date           : N/A
Release                       : 5.4.9
```

Installing this Software Version

Caution: 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 59 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 61.

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
AR1050V	`awplus(config)# boot system AR1050V-5.4.9-0.8.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.4.9-0.8.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.9-0.8.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.9-0.8.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.9-0.8.rel`
FS980M series	`awplus(config)# boot system FS980-5.4.9-0.8.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.4.9-0.8.rel`
GS970M series	`awplus(config)# boot system GS970-5.4.9-0.8.rel`
GS980M series	`awplus(config)# boot system GS980M-5.4.9-0.8.rel`
XS900MX series	`awplus(config)# boot system XS900-5.4.9-0.8.rel`
x220 series	`awplus(config)# boot system x220-5.4.9-0.8.rel`
x230 series	`awplus(config)# boot system x230-5.4.9-0.8.rel`

Product	Command
IE200 series	`awplus(config)# boot system IE200-5.4.9-0.8.rel`
IE210L series	`awplus(config)# boot system IE210-5.4.9-0.8.rel`
x310 series	`awplus(config)# boot system x310-5.4.9-0.8.rel`
IE300 series	`awplus(config)# boot system IE300-5.4.9-0.8.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.9-0.8.rel`
x510 series	`awplus(config)# boot system x510-5.4.9-0.8.rel`
x530 series	`awplus(config)# boot system x530-5.4.9-0.8.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.4.9-0.8.rel`
x550 series	`awplus(config)# boot system x550-5.4.9-0.8.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.9-0.8.rel`
x950 series	`awplus(config)# boot system x950-5.4.9-0.8.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.4.9-0.8.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.9-0.8.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 Device GUI

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 AR3050S and AR4050S 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 SBx908 GEN 2 switches and AR-Series 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, and if not, whether you are using a AR-Series device or a switch.

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 on an AR-series device: 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:

Device	Address
AR-Series	192.168.1.1
Switches	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 66. 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**.

If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 67.

Install the GUI if it is not installed

If you have an AR-series device and the GUI 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.

If you have a switch and the GUI 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 5.4.9-0.x is awplus-gui_549_11.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_549_11.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

If you have an AR-series device and you need to update the GUI...

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.

If you have a switch and you need to update the GUI...

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 5.4.9-0.x is awplus-gui_549_11.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_549_11.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.*