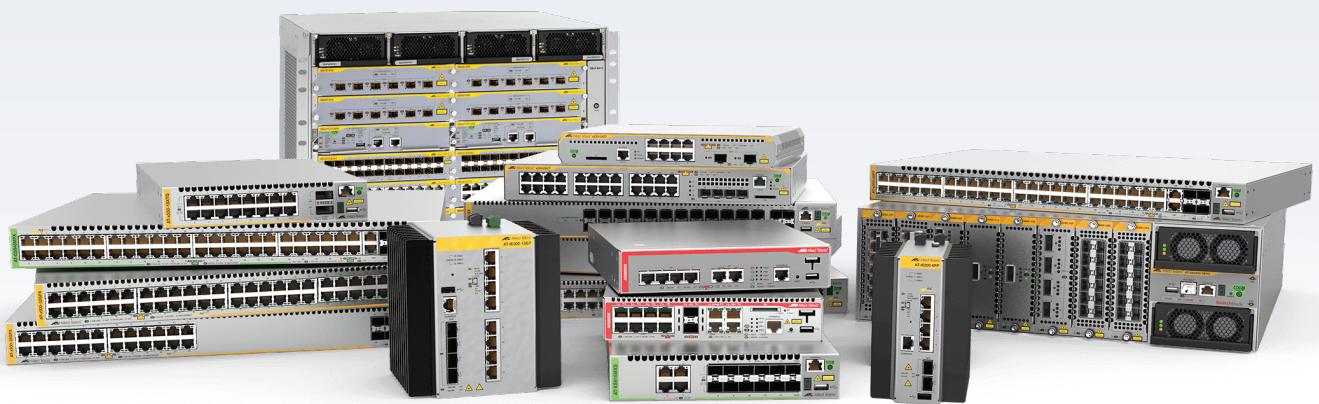


Release Note for AlliedWare Plus Software Version 5.4.8-2.x



AlliedWare Plus OPERATING SYSTEM

- » SBx8100 Series » SBx908 GEN2 » x950 Series
- » x930 Series » x550 Series » x530 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
- » 5.4.8-2.2 » 5.4.8-2.3 » 5.4.8-2.4 » 5.4.8-2.5 » 5.4.8-2.6 » 5.4.8-2.7 » 5.4.8-2.8 » 5.4.8-2.9
- » 5.4.8-2.10

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

©2009 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

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

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

Getting the most from this Release Note

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

Content

What's New in Version 5.4.8-2.10	3
Introduction	3
Issues Resolved in Version 5.4.8-2.10	6
What's New in Version 5.4.8-2.9	7
Introduction	7
Issues Resolved in Version 5.4.8-2.9	10
What's New in Version 5.4.8-2.8	15
Introduction	15
Enhancement in Version 5.4.8-2.8	18
What's New in Version 5.4.8-2.7	19
Introduction	19
Issues Resolved in Version 5.4.8-2.7	22
What's New in Version 5.4.8-2.6	23
Introduction	23
New Features and Enhancements	26
Issues Resolved in Version 5.4.8-2.6	27
What's New in Version 5.4.8-2.5	34
Introduction	34
Issues Resolved in Version 5.4.8-2.5	37
What's New in Version 5.4.8-2.4	39
Introduction	39
Issues Resolved in Version 5.4.8-2.4	42
What's New in Version 5.4.8-2.3	43
Introduction	43
New Features and Enhancements	46
Issues Resolved in Version 5.4.8-2.3	47
What's New in Version 5.4.8-2.2	53
Introduction	53
New Products	56
New Features and Enhancements	57
Important Considerations Before Upgrading	69
Obtaining User Documentation	77

Verifying the Release File	77
Licensing this Version on an SBx908 GEN2 Switch	78
Licensing this Version on an SBx8100 Series Switch Control Card	80
Installing this Software Version	82
Accessing the web-based device GUI.....	84

What's New in Version 5.4.8-2.10

Product families supported by this version:

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

x530 Series
x510 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.10.

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 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80](#).



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	FS980-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2019	GS900-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2019	GS970-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	08/2019	GS980M-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	08/2019	XS900-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2019	IE200-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	08/2019	IE300-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	08/2019	IE210-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	08/2019	IE510-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	08/2019	x220-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2019	x230-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2019	x310-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	08/2019	IX5-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84

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	x510-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	08/2019	x530-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2019	x550-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2019	x930-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	08/2019	x950-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	08/2019	SBx908NG-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	08/2019	SBx81CFC400-5.4.8-2.10.rel SBx81CFC960-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	08/2019	AR4050S-5.4.8-2.10.rel AR3050S-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	08/2019	AR2050V-5.4.8-2.10.rel AR2010V-5.4.8-2.10.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		08/2019	vaa-5.4.8-2.10.iso (VAA OS) vaa-5.4.8-2.10. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.10.vhd (for Microsoft Azure)	

Unsupported devices

Software version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

SBx81CFC960 version 2 support

Software version 5.4.8-2.10:

- Supports version 2 of the SBx81CFC960 control card

Issues Resolved in Version 5.4.8-2.10

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE210L	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60253	HTTP	Previously, when a switch was under heavy load, the web server could occasionally show an increased memory usage which was not subsequently returned to the free buffer pool when load returned to normal. 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-62372	VCStack	Previously, members of SBx908 GEN2 or x950 variant stacks could occasionally fail to inter-communicate properly and would show TIPC timeout messages. In the worst case this would lead to a duplicate master followed by one stack member rebooting. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	-	-	-	-
CR-63383	Web API	Previously, when multiple VTY shell sessions were opened with the device GUI or Vista manager and some were closed, it could cause other GUI or Vista Manager shell sessions to freeze and terminate. 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	-

What's New in Version 5.4.8-2.9

Product families supported by this version:

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

x530 Series
x510 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.9.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80](#).



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	FS980-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2019	GS900-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2019	GS970-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	08/2019	GS980M-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	08/2019	XS900-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2019	IE200-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	08/2019	IE300-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	08/2019	IE210-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	08/2019	IE510-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	08/2019	x220-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2019	x230-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2019	x310-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	08/2019	IX5-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84

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	x510-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	08/2019	x530-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2019	x550-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2019	x930-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	08/2019	x950-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	08/2019	SBx908NG-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	08/2019	SBx81CFC400-5.4.8-2.9.rel SBx81CFC960-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	08/2019	AR4050S-5.4.8-2.9.rel AR3050S-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	08/2019	AR2050V-5.4.8-2.9.rel AR2010V-5.4.8-2.9.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		08/2019	vaa-5.4.8-2.9.iso (VAA OS) vaa-5.4.8-2.9.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.9.vhd (for Microsoft Azure)	

Unsupported devices

Software version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

ISSU and SBx81CFC960 version 2 support

Software version 5.4.8-2.9:

- Supports version 2 of the SBx81CFC960 control card
- Is not ISSU compatible with previous software versions

Issues Resolved in Version 5.4.8-2.9

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61324	AMF	Previously, AMF NODE-IDs would be allocated in a nearly contiguous range up to a maximum of 308 nodes. The range of nodes is actually 1-4094. This update randomises the allocation of the NODE-IDs to take into account the entire range without restricting them to the lower NODE-ID values. This has the advantage of reducing clashes of duplicate NODE-IDs. 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-63137	AMF Antivirus	With this software update, the AMF backup is no longer backing up the Antivirus directory. This resource is downloaded when Antivirus is started and contains virus signatures that should not be part of an AMF backup. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	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 "squid" module could suffer a critical error and be restarted. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	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. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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.	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	-
CR-62664	IDS/IPS	Previously, when http-events of the IPS function were set to deny, access to the web site could be prevented. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	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	-
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.	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	-
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-63148	L2TPv3 Tunneling	Previously, after dynamically changing the configuration of an L2TPv3 tunnel interface, the tunnel interface could sometimes fail to come up. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-
CR-63176	LACP	Previously, port security error messages: "DBG:exfx_portsec_learnCountDecrement 626: Invalid interface ifIndex 0" would be logged when deleting dynamic aggregators. The error message was due to an incorrect validation logic. 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	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud																									
CR-62120	LLDP	LLDP supports configuration of a variety of location coordinates, such as latitude, longitude, and altitude of the device, street address, map datum, supported via LLDP-MED location TLV. With this software update, when configured, a negative (minus) altitude now correctly displays as negative when using the show location coord-location identifier command. For example: <pre>awplus(config)#location coord-location identifier 20 awplus(config-coord)#altitude -20 floors awplus#show location coord-location identifier 20</pre> <table><thead><tr><th>ID</th><th>Element</th><th>Type</th><th>Element Value</th></tr></thead><tbody><tr><td>20</td><td>Latitude</td><td>Resolution</td><td>[not configured]</td></tr><tr><td></td><td>Longitude</td><td>Resolution</td><td>[not configured]</td></tr><tr><td></td><td>Altitude</td><td>Resolution</td><td>[not configured]</td></tr><tr><td></td><td>Altitude</td><td></td><td>-20.00000000 floors</td></tr><tr><td></td><td>Map Datum</td><td></td><td>[not configured]</td></tr></tbody></table>	ID	Element	Type	Element Value	20	Latitude	Resolution	[not configured]		Longitude	Resolution	[not configured]		Altitude	Resolution	[not configured]		Altitude		-20.00000000 floors		Map Datum		[not configured]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	Y	-	-	Y	-
ID	Element	Type	Element Value																																															
20	Latitude	Resolution	[not configured]																																															
	Longitude	Resolution	[not configured]																																															
	Altitude	Resolution	[not configured]																																															
	Altitude		-20.00000000 floors																																															
	Map Datum		[not configured]																																															
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	-																								
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	-																								
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	-																								
CR-62287	Loop Protection	Previously, the show loop-protection command displayed ports out of order after a late stack member join. This issue has been resolved, now the ports are displayed in the correct order.	-	-	Y	Y	-	-	Y	-	-	Y	Y	Y	-	Y	-	Y	-	Y	-	-	-	-	-	-																								

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-63159	Pluggable Transceivers	With this software update, the 40G pluggable AT-QSFPSR4LC in AT-SBx81XLEM/Q2 is now supported.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	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	Y	-	-	-	-	-	-	-	
CR-63092	PoE	Occasionally the PoE function on x220 and x530 variant switches could fail to power up PoE devices. This issue has been resolved.	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	
CR-62285	Port Authentication	Previously, when the authd process reinitialized with already authenticated users attached, the new instance of the authd process could sometimes incorrectly initialize, thus preventing the users from logging in. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y	Y	-
CR-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	-
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.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	
CR-62847	System	Previously, under rare circumstances, x550 series switches could generate erroneous i2c errors at boot up. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	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	-	-	-	-	
CR-63398	VCStack	This software update supports configuring a static-channel group for VLAN stacking.	-	-	Y	Y	-	-	Y	-	-	Y	Y	Y	-	Y	-	-	-	-	Y	-	-	-	-	

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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 5.4.8-2.8

Product families supported by this version:

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

x530 Series
x510 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.8.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80](#).



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	FS980-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	05/2019	GS900-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2019	GS970-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	05/2019	GS980M-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	05/2019	XS900-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	05/2019	IE200-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	05/2019	IE300-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	05/2019	IE210-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	05/2019	IE510-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	05/2019	x220-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2019	x230-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	05/2019	x310-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	05/2019	IX5-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84

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	x510-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	05/2019	x530-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2019	x550-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	05/2019	x930-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	05/2019	x950-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	05/2019	SBx908NG-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	05/2019	SBx81CFC400-5.4.8-2.8.rel SBx81CFC960-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	05/2019	AR4050S-5.4.8-2.8.rel AR3050S-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	05/2019	AR2050V-5.4.8-2.8.rel AR2010V-5.4.8-2.8.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		05/2019	vaa-5.4.8-2.8.iso (VAA OS) vaa-5.4.8-2.8.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.8.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

Enhancement in Version 5.4.8-2.8

This AlliedWare Plus maintenance version includes the following enhancement:

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AME Cloud	
ER-2790	VCStack	This Software update now supports VCS Resiliency link with Disabled Master Monitoring on the SBx8100 VCStack Plus. VCStack Plus 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 interface (eth0) must be configured as a resiliency port with the command: <pre>awplus(config)#stack resiliencylink eth0</pre> Command information: ■ The global configuration command stack disabled-master-monitoring is supported on the SBx8100 CFC960. ■ The global configuration command stack resiliencylink <interface-name> is supported on the SBx8100 CFC960. Note, the only supported interface is “eth0”. ■ The show command show stack detail displays the resiliency link information on the SBx8100 CFC960. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-

What's New in Version 5.4.8-2.7

Product families supported by this version:

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

x530 Series
x510 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.7.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80](#).



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	FS980-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	05/2019	GS900-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2019	GS970-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	05/2019	GS980M-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	05/2019	XS900-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	05/2019	IE200-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	05/2019	IE300-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	05/2019	IE210-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	05/2019	IE510-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	05/2019	x220-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2019	x230-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	05/2019	x310-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	05/2019	IX5-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84

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	x510-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	05/2019	x530-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2019	x550-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	05/2019	x930-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	05/2019	x950-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	05/2019	SBx908NG-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	05/2019	SBx81CFC400-5.4.8-2.7.rel SBx81CFC960-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	05/2019	AR4050S-5.4.8-2.7.rel AR3050S-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	05/2019	AR2050V-5.4.8-2.7.rel AR2010V-5.4.8-2.7.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		05/2019	vaa-5.4.8-2.7.iso (VAA OS) vaa-5.4.8-2.7.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.7.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

Issues Resolved in Version 5.4.8-2.7

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	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-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 after many repeated attempts. - 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 other unrelated SFP links to flap. These issues have been resolved.	-	-	-	-	-	Y	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-

What's New in Version 5.4.8-2.6

Product families supported by this version:

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

x530 Series
x510 Series
x550 Series
x930 Series
x950 Series
SwitchBlade x908 GEN2
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.6.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80](#).



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	FS980-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	04/2019	GS900-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2019	GS970-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	04/2019	GS980M-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	04/2019	XS900-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	04/2019	IE200-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	04/2019	IE300-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	04/2019	IE210-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	04/2019	IE510-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	04/2019	x220-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2019	x230-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	04/2019	x310-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	04/2019	IX5-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84

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	x510-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	04/2019	x530-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2019	x550-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	04/2019	x930-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	04/2019	x950-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	04/2019	SBx908NG-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	04/2019	SBx81CFC400-5.4.8-2.6.rel SBx81CFC960-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	04/2019	AR4050S-5.4.8-2.6.rel AR3050S-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	04/2019	AR2050V-5.4.8-2.6.rel AR2010V-5.4.8-2.6.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		04/2019	vaa-5.4.8-2.6.iso (VAA OS) vaa-5.4.8-2.6.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.6.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

New Features and Enhancements

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

CR	Module	Description	FS980M	GS970M	GS980M	XS900MX	GS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-2231	AMF WEB API	With this software update, the HAproxy is now fully capable of performing graceful restart. As a result, an AMF node leaving or joining the network is no longer causing HTTP API requests from Vista Manager to other nodes in the network to be interrupted. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
ER-2194	PoE	With this software update, 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. ISSU: Effective when CFCs upgraded	Y	Y	Y	–	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
ER-2720	VRRP	With this software update, a new command: (no) vrrp icmp-ttl-exceeded-error-use-physical-address has been added to allow the physical IPv4 address of the VRRP interface to be used in the 'icmp time to live exceeded' error message generated by the VRRP router. By default, the physical IPv4 address of the VRRP interface is not used. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

Issues Resolved in Version 5.4.8-2.6

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-62164	AMF	Previously, when backing up a TQ guestnode, the AMF backup could not complete or timeout if the backup process was interrupted. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y
CR-62563	AMF	With this software update, the Japanese language is now supported on configuring TQ guest nodes. 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-60256	ARP Neighbour Discovery	Previously, stale entries in the ARP / IPv6 neighbour table could linger indefinitely if the table was not very full. As a result, it was possible for an entry to get stuck in a reachable state even though the neighbour was no longer reachable. 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-62410	ARP Neighbor Discovery	Previously, when using the arp-mac-disparity functionality, it was possible for some packets to be reflected on ingress of a trunk port. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–	–	–
CR-62618	ARP Neighbor Discovery	Previously, when using the arp-mac-disparity functionality, it was possible for the nexthop entry to be installed incorrectly. This could happen if the server sent an ARP request to the AW+ switch before the AW+ switch sent an ARP to the server. As a result, the traffic would not forward correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-62468	CLI	With this software update, the command: show radius local-server user will no longer show hashed user passwords. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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	Y	Y
CR-61474	Firewall	With this software update, the interaction between FTP data channel connection and NAT has been further improved. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-
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. Example syntax: To specify the DF bit 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	-
CR-62288	L3 Multicast	Previously, it was possible for memory leaks to occur during the processing on L3 multicasting. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-62972	L3 Multicast	Previously, AlliedWare Plus routers could restart unexpectedly when a multicast group entry was deleted. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-
CR-62308	Logging	Previously, it was possible for log rotation to be delayed for a long period, resulting in log buffer space exhaustion. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
CR-62256	Multicast Routing VRF-Lite	Previously, L3 multicast was not being forwarded within a VRF instance. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
CR-62333	Multicast Routing VRF-Lite	Previously, a VRF instance would fail to be added to a PIM interface, resulting in traffic not being forwarded. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
CR-60992	NAT	With this software update, the FTP data channel flow now complies with the IP tables rules.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-
CR-61877	PIM VCStack	Previously, if many multicast groups were configured on a stack, the stack failover could result in some lost information on those groups. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-
CR-62128	PIMv6	Previously, a master failover could generate unnecessary "CMSG overflows" GUI RESTful API error messages if many multicast groups with PIMv6 were configured on the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	Y	-	Y	-	-	Y	-	Y	Y	Y	Y	Y	-	-	Y	-	-	Y	-
CR-60550	Pluggable Transceivers	With this software update, the 40G AT-QSFPSR4-LC pluggable is now supported on AT-SBx81XLEM. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61930	Pluggable Transceivers	Previously, when hotswapping SFP/SFP+/QSFP modules on a x930 variant switch, the switch would sometimes fail to register the SFP removal or insertion event. As a result, the SFP ports could no longer be used. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-
CR-62266	Pluggable Transceivers	Previously, on x930 series switches, 1000BASE-T pluggables in the SFP+ slots were sometimes not detected. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-
CR-62296	PoE	Previously, PoE devices would not be powered up even when the PoE voltage was restored after a low voltage state. This issue has been resolved.	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-62293	Port Configuration	Previously, an SBx908 GEN2's AT-XEM2-12XTm port could fail to link up when the speed was configured as "5000M Auto" after a previous incorrect speed/duplex setting. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-62310	Port Security	With this software update, the following issues are resolved: On GS970M, GS900MX/MPX, XS900MX, GS980M, IE200, IE300, x210, x230, x310, IX5, x510, x510L, x550, x930, x950, SBx908 GEN2, platforms: - Previously, when port-security aging was configured, MAC station movements away from and back to the initial port would not operate correctly, preventing an FDB entry being re-learned into hardware on the initial port which prevented the MAC from communicating on that initial port until an internal 5 minute port-security timer had expired. - Previously, on a port with port-security aging, adding static MAC address entries or changing the port-security maximum setting would result in the FDB table for that port being prematurely flushed but without flushing the entries from port-security's database. This would prevent all of the previous FDB entries from being re-learned on that port until the 5 minute port-security timer had expired. - Previously, when using port security in combination with loop protection or thrash limiting on the same port, when loop protection or thrash limiting return the port back to a 'good' state this would override the setting of port-security if it was configured on that port but not in a locked state, resulting in port-security ceasing to function correctly until it was deconfigured and reconfigured on the port. ISSU: Effective when ISSU complete	-	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	-	Y	Y	Y	-	-	Y	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-62310 [cont...]	Port Security	With this software update, the following issues are resolved: On FS980M , x220 , x530 , and SBx8100 , platforms: - Previously, when port-security aging was configured, MAC station movements away from and back to the initial port would not operate correctly, the FDB entry would be removed from hardware on the initial port but would not be removed from port-security's software shadow table. If the MAC later moved back to the first port it would consume an additional entry in the shadow table. Moving between multiple ports in this way could quickly consume port-security's maximum limit on each port. - Previously, on a port with port-security aging, adding static MAC address entries on a port that had already learned that MAC address dynamically would not remove the dynamic entry from port security's shadow table. This means the MAC address would effectively consume 2 entries out of the port-security maximum configured for that port, instead of one, which could prematurely exhaust the port-security maximum configured for the port. ISSU: Effective when ISSU complete	Y	–	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	Y	Y	–	–	–	–	–
CR-61287	SSL	With this software update, OpenSSL has been upgraded to version 1.0.2q to address security vulnerability CVE-2018-0734. 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-61229	Static Aggregation VCStack	Previously, when a link aggregation was configured on a stack, L3 NLB packets were not forwarded if the ingress and egress ports were the same port. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	Y	Y	Y	–	Y	Y	Y	–	–	Y	–	–	–	–	
CR-62245	VCStack	Previously, it was possible for stack members to get stuck in the initialization state if there were multiple stack members joining the stack at the same time. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	
CR-61297	VCStack	Previously, it was possible for some stack members to be stuck in the "INIT" state 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	Y	Y	Y	–	–	–	–	

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX/MPX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-62365	VLAN	Previously, removing an existing IPv4 address from an interface and then assigning a new address to the same interface could result in the interface not being able to forward packets. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	—

What's New in Version 5.4.8-2.5

Product families supported by this version:

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.5.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80.](#)



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	01/2019	FS980-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	01/2019	GS900-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2019	GS970-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	01/2019	GS980M-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	01/2019	XS900-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	01/2019	IE200-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	01/2019	IE300-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	01/2019	IE210-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	01/2019	IE510-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	01/2019	x220-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2019	x230-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	01/2019	x310-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	01/2019	IX5-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84

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	01/2019	x510-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	01/2019	x530-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2019	x550-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	01/2019	x930-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	01/2019	x950-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	01/2019	SBx908NG-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	01/2019	SBx81CFC400-5.4.8-2.5.rel SBx81CFC960-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	01/2019	AR4050S-5.4.8-2.5.rel AR3050S-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	01/2019	AR2050V-5.4.8-2.5.rel AR2010V-5.4.8-2.5.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		01/2019	vaa-5.4.8-2.5.iso (VAA OS) vaa-5.4.8-2.5.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.5.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

Issues Resolved in Version 5.4.8-2.5

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

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200/IE210L	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-62068	CLI	Previously, the show interface command would display overflowed interface running time. This minor display 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-61398	Firewall	With this software update, ICMP rules will now match on unreachable messages being generated by the router. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	
CR-61939	IGMP, VRF	Previously, when IGMP snooping was disabled, it was possible that IGMP reports would not be correctly forwarded in the default VRF. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	–	
CR-62087	Layer 2 Multicast	Previously, L2 multicast traffic would not be forwarded between VLANs if L3 multicast was enabled. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–
CR-62062	Layer 3 Multicast	Previously, if multicast traffic needed to be sent to a port on multiple VLANs, and one of those VLANs was the same as the ingress VLAN, the traffic to the ingress VLAN would not be sent. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–
CR-62085	PIM-DM	Previously, if multicast traffic was traversing across a VLAN with ip pim dense-mode configured, removing the VLAN could cause the PIM process to terminate unexpectedly. This issue has been resolved. ISSU: Effective when ISSU complete	–	–	–	–	–	–	Y	Y	–	–	Y	–	Y	Y	Y	–	–	Y	Y	Y	–	–	–	–	

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200/IE210L	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61247	Pluggable Transceivers	Previously, removing a 1G copper pluggable from a port might cause the port to fail to link up for subsequent pluggables inserted in it. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	–	–	Y	–	–	–	–
CR-61229	Static Aggregation VCStack	Previously, when a link aggregation was configured on a stack, L3 NLB packets were not forwarded if the ingress and egress ports were the same port. This issue has been resolved.	–	–	Y	–	Y	–	–	–	–	–	Y	Y	Y	–	Y	Y	Y	–	–	Y	–	–	–	–

What's New in Version 5.4.8-2.4

Product families supported by this version:

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.4.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80.](#)



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	01/2019	FS980-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	01/2019	GS900-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2019	GS970-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	01/2019	GS980M-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	01/2019	XS900-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	01/2019	IE200-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	01/2019	IE300-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	01/2019	IE210-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	01/2019	IE510-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	01/2019	x220-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2019	x230-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	01/2019	x310-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	01/2019	IX5-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84

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	01/2019	x510-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	01/2019	x530-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2019	x550-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	01/2019	x930-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	01/2019	x950-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	01/2019	SBx908NG-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	01/2019	SBx81CFC400-5.4.8-2.4.rel SBx81CFC960-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	01/2019	AR4050S-5.4.8-2.4.rel AR3050S-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	01/2019	AR2050V-5.4.8-2.4.rel AR2010V-5.4.8-2.4.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		01/2019	vaa-5.4.8-2.4.iso (VAA OS) vaa-5.4.8-2.4.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.4.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

Issues Resolved in Version 5.4.8-2.4

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

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-61365	PoE	Previously, the colour display of the PoE LED status was incorrect for Denied and Fault status. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y	–	–	–	–
CR-61666	PIM-DM	Previously, the command no ip pim dense-mode , which disables PIM-DM operation from all downstream interfaces, could take a significant amount of time to be effective. This issue has been resolved. ISSU: Effective when ISSU complete	–	–	–	–	–	–	Y	Y	–	–	Y	–	Y	Y	Y	–	–	Y	Y	Y	–	–	–	–	

What's New in Version 5.4.8-2.3

Product families supported by this version:

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.3.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80.](#)



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	12/2018	FS980-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	12/2018	GS900-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	12/2018	GS970-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	12/2018	GS980M-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
XS916MXT XS916MXS	XS900MX	12/2018	XS900-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	12/2018	IE200-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	12/2018	IE300-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	12/2018	IE210-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	12/2018	IE510-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	12/2018	x220-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	12/2018	x230-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	12/2018	x310-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	12/2018	IX5-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84

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	12/2018	x510-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	12/2018	x530-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	12/2018	x550-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	12/2018	x930-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	12/2018	x950-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
SBx908 GEN2	SBx908 GEN2	12/2018	SBx908NG-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	12/2018	SBx81CFC400-5.4.8-2.3.rel SBx81CFC960-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	12/2018	AR4050S-5.4.8-2.3.rel AR3050S-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	12/2018	AR2050V-5.4.8-2.3.rel AR2010V-5.4.8-2.3.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		12/2018	vaa-5.4.8-2.3.iso (VAA OS) vaa-5.4.8-2.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.3.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

New Features and Enhancements

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, x510L	x530	x550	x610	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-2432	AWC	With this software update, the TQm5403 Wireless Access Point is now supported in the Vista Manager AWC plugin.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-
ER-2476	IPv4	With this software update, the handling of IPv4 routes within hardware and software tables has been improved so that when a port is shut down and then brought back up, the connected route can be handled more appropriately. 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	-

Issues Resolved in Version 5.4.8-2.3

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

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61151	AMF	Previously, a race condition between an AMF master and an AMF node during initialisation of the AMF master, resulted in nodes missing from AMF topology. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-60979	Antivirus	Previously the web-proxy would accept new connections even though the Antivirus process was not keeping up with the scanning of files transferred over the existing connections. This resulted in very high memory usage and could cause the device to restart if other processes were also using a large amount of memory. With this software change, the number of newly accepted http connections is now throttled to reduce the amount of memory the web-proxy uses when there is a very large number of concurrent client connections.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-
CR-61384	ARP VRRP	Previously, when a VRRP master was not the virtual IP owner and proxy ARP was configured on the VRRP interface, if an ARP for an address in the VRRP interface's subnet was received, the device would perform proxy ARP for that address. This was incorrect and was behaving like "local proxy ARP". The issue has been resolved. Now it only performs proxy ARP for addresses reachable over interfaces other than the VRRP interface (i.e. normal proxy ARP behaviour). ISSU: Effective when ISSU complete.	Y	-	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61414	ARP VRRP	Previously, in a VRRP configuration, if the VRRP interface on each router was also configured with Proxy ARP, the device(s) in the VRRP Backup state would give proxy ARP response with their real MAC address in addition to the proxy ARP replies sent by the Master with the Virtual MAC address. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-61630	AWC	Previously, Vista Manager incorrectly displayed an error for eligible AWC radio channels for some countries. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-60108	DNS	Previously if domain-specific DNS forwarding servers were configured (static or dynamic) and no general DNS servers were configured (static or dynamic), the servers could be used out of priority order. Also, in some dynamic configurations with domain-specific and general servers, the domain-specific servers might sometimes be used out of order around the time the dynamic servers were acquired. These issues have been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	Y	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61109	Environmental Monitoring	Previously on an IE510 switch, the output relays would be deactivated (closed) on power-on. Any alarm state would not be reflected until configuration was complete. This was an issue on backup stack members as the relays on backup members are expected to be open. This issue has been resolved. Now, (in conjunction with required bootloader version 2.0.31 or later), the output relays are activated (opened) within a few seconds of powering on the device and remain active until stack configuration is complete to ensure that the output relays reflect their configuration.	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-61270	Environmental Monitoring	Previously, alarm-monitoring alarms would not be triggered correctly if the snmp-server source-interface IFNAME command was used in the device configuration. This issue has been resolved.	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-61131	EPSR	With this software update, the x230 series switches are now faster at detecting link down on fibre ports, which improves EPSR failover time.	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-61295	EPSR	Previously, when disabling an EPSR instance on the primary or secondary ports that had the "Bidirectional Forwarding Detection" (BFD) disabled, the ports would be reported as disabled or discarding when they were actually forwarding in hardware, resulting in network loops. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-61315	IGMP	Previously, PIM Dense Mode Multicast routes could time out and be deleted even if traffic was still flowing if the source was not directly connected. This resulted in one or more packets being dropped while the route was re-learned. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	Y	Y	-	-	Y	-	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	
CR-61245	IGMP VCStack	Previously, high rates of IGMP leaves could cause a stack separation. This issue has been resolved.	-	-	Y	Y	Y	-	-	Y	-	-	Y	Y	Y	-	Y	Y	Y	Y	-	-	Y	-	-	-	-
CR-61446	IPSec	Previously, if an IPSec tunnel had a "dynamic" tunnel destination address, the remote peer was behind a NAT device and that NAT device was given a new IP address from the network, then the local router would detect the change in IP address and update the ISAKMP and IPSec NAT-T SA's, but would fail to update the "dynamic" tunnel interface address. This resulted in the received traffic being dropped even though the IP address was correctly detected. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
CR-61361	IPv6	Previously, IPv6 addresses might not be learnt correctly if there were many VLANs configured on a switch. For example, this could result in a failure to generate and apply IPv6 Link-local addresses on device startup. 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-60367	Multicast Routing	Previously, L3 multicast entries were not being registered to the L3 host table on certain devices. This issue has been resolved.	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61331	Multicast Routing	Previously, on an SBx908 GEN2 switch, multicast entries could be out of synchronisation across all stack members after a stack failover. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-
CR-61111	OSPF	Previously, if OSPF was configured with VRF-Lite, the OSPF in VRF-Lite domains would sometimes have the DN bit set in LSAs, resulting in other devices within the OSPF domain ignoring those LSAs when calculating the SPF. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-61667	PIM-SM	Previously, multicast traffic forwarded within a VRF interface could be lost during a stack master failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	Y	Y	-	-	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-
CR-61246	Pluggable Transceivers	Previously, the DAC cable in XEM2-12XS showed incorrectly as 'SR' rather than 'CR' for the interface mode. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	Y	-	-	-	-
CR-61300	Pluggable Transceivers	Previously, the AT-SPSX/I pluggable transceiver did not work correctly on GS900MPX and x310 series switches. This issue has been resolved.	-	-	-	Y	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-61719	Port Configuration	Previously, on a FS980M/9PS switch, executing the show platform command could cause the switch to restart unexpectedly. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-61329	RIPng	With this software update, the x230-10GP switch now supports a maximum number 256 RIPng interfaces. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS980M	GS900MX/MPX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, x510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	SBx908 GEN2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61307	Switch	Previously, it was possibility for an error message concerning a buffer overflow to be logged if there was a high number of VLANs configured on a SBx8100 switch. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	-	-	-	-	-
CR-61223	VCStack	Previously, stacking ports sometimes flapped when an AT-QSFP-SR4/LR4 was used. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-
CR-61297	VCStack	Previously, it was possible for some stack members to be stuck in the "INIT" state 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	Y	Y	Y	Y	-	-	-	-
CR-61069	Web Control	With this software update, web-proxy will now use less memory in an idle environment. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-

What's New in Version 5.4.8-2.2

Product families supported by this version:

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-2.2.

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



Caution: Software version 5.4.8-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80.](#)



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	12/2018	FS980-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	12/2018	GS900-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	12/2018	GS970-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
GS980M/52 GS980M/52PS	GS980M	12/2018	GS980M-5.4.8-2.2.rel	Coming soon
XS916MXT XS916MXS	XS900MX	12/2018	XS900-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	12/2018	IE200-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
IE300-12GT IE300-12GP	IE300	12/2018	IE300-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
IE210L-10GP IE210L-18GP	IE210L	12/2018	IE210-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
IE510-28GSX-80	IE500	12/2018	IE510-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
x220-28GS x220-52GT x220-52GP	x220	12/2018	x220-5.4.8-2.2.rel	x220-28GS: See "Accessing the web-based device GUI" on page 84 x220-52GT and x220-52GP: Coming soon
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	12/2018	x230-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
x310-26FT x310-50FT x310-26FP x310-50FP	x310	12/2018	x310-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
IX5-28GPX	IX5	12/2018	IX5-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84

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	12/2018	x510-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
x530-28GTXm x530-28GPXm	x530	12/2018	x550-5.4.8-2.2.rel	Coming soon
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	12/2018	x550-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	12/2018	x930-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
x950-28XSQ	x950	12/2018	x950-5.4.8-2.2.rel	Coming soon
SBx908 GEN2	SBx908 GEN2	12/2018	SBx908NG-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
SBx81CFC400 SBx81CFC960	SBx8100	12/2018	SBx81CFC400-5.4.8-2.2.rel SBx81CFC960-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
AR4050S AR3050S	AR-series UTM firewalls	12/2018	AR4050S-5.4.8-2.2.rel AR3050S-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
AR2050V AR2010V	AR-series VPN firewalls	12/2018	AR2050V-5.4.8-2.2.rel AR2010V-5.4.8-2.2.rel	See "Accessing the web-based device GUI" on page 84
AMF Cloud		12/2018	vaa-5.4.8-2.2.iso (VAA OS) vaa-5.4.8-2.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-2.2.vhd (for Microsoft Azure)	

Unsupported devices

Version 5.4.8-2.x does not support:

- SwitchBlade x908 switches (it does support SwitchBlade x908 GEN2 switches)
- DC2552XS/L3 switches.

New Products

Version 5.4.8-2.2 supports the following recently-released and upcoming products.

x950-28XSQ switches

High Capacity Stackable Layer 3+ Switches

The x950-28XSQ switches are designed as a powerful local or distributed core solution, in a 1RU form-factor. They have 24 x 1/10G SFP+ ports, 4 x 40G/100G uplink ports, and 1 expansion bay supporting further 10G, 40G or 100G ports.

For more information, see www.alliedtelesis.com/products/switches/x950-series/x950-28xsq.

x530-28GTXm and x530-28GPXm switches

Stackable Intelligent Layer 3 Switches

The x530-28GTXm and x530-28GPXm are versatile Gigabit distribution and network access switches. They have 24 x 100/1000T RJ-45 copper ports and 4x 1/10 Gigabit SFP+ uplinks. The x530-28GPXm offers 24 POE+ enabled ports.

Key features include Allied Telesis Autonomous Management Framework (AMF), Active Fiber Monitoring, EPSR and G.8032 high-speed ring connectivity, VCStack for resiliency, Layer 3 switching, including VRF lite, DHCP snooping, IEEE 802.1x/MAC/Web authentication support, IEEE 802.3at PoE+ sourcing (30W) and Continuous PoE.

x220-52GT and x220-52GP switches

Enterprise Gigabit Edge Switches

The x220-52GP and x220-52GT have 48 x 10/100/1000T RJ-45 copper ports and 4x 100/1000X SFP uplinks. The x220-52GP offers 48 POE+ enabled ports.

Key features include Allied Telesis Autonomous Management Framework (AMF), Active Fiber Monitoring, EPSR and G.8032 high-speed ring connectivity, Management stacking, static routing and RIP, DHCP snooping, IEEE 802.1x/MAC/Web authentication support, IEEE 802.3at PoE+ sourcing (30W) and Continuous PoE.

GS980M/52 and GS980M/52PS switches

Managed Gigabit Edge Switches

GS980M/52 and GS980M/52PS have 48 x 10/100/1000T RJ-45 copper ports and 4x 100/1000X SFP uplinks. The GS980M/52PS offers 48 POE+ enabled ports.

Key features include AMF Edge, EPSR ring connectivity, static routing and RIP, DHCP snooping, IEEE 802.1x/MAC/Web authentication support, IEEE 802.3at PoE+ sourcing (30W) and Continuous PoE.

New Features and Enhancements

This section summarizes the new features in 5.4.8-2.2 since 5.4.8-1.2:

- “Allied Telesis Autonomous Management Framework (AMF) enhancements” on page 58
- “MAC-authentications on AR-series devices” on page 58
- “Static suffix for RA auto-configuration” on page 59
- “Link Layer Discovery Protocol (LLDP) support on AR-series” on page 59
- “IPv6 Tunneling” on page 59
- “Receive Packet Scheduling” on page 60
- “MODBUS” on page 60
- “Day of the month trigger” on page 61
- “DHCP Framed IP Lease” on page 61
- “Short-term leases for IPv4 DHCP” on page 61
- “Improvements to “show” commands for multicasting” on page 62
- “Setting an alias name for a switch port for SNMP” on page 63
- “Improvements to QoS storm protection log messages” on page 63
- “PSU and fan module presence notification” on page 63
- “Bidirectional Forwarding Detection (BFD) on the SwitchBlade x8100 CFC960” on page 65
- “Upstream Forwarding Only (UFO) on the SwitchBlade x8100 CFC960” on page 65
- “Secure Mode on SBx908 GEN2 switches and x950 Series switches” on page 66
- “Virtual Chassis Stacking (VCStack) on x950 Series switches” on page 67
- “Specifying a name for OpenFlow controllers” on page 67
- “The OpenFlow protocol on x950 Series switches” on page 68
- “Forcing combo ports on x930-28GSTX switches to only accept either copper or fiber pluggables” on page 68
- “G.8032 on x220 Series switches” on page 68
- “Connectivity Fault Management (CFM) on x220, x230 and x230L Series switches” on page 68

To see how to find full documentation about all features on your product, see [“Obtaining User Documentation” on page 77](#).

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 5.4.8-2.2 includes the following AMF enhancements.

AMF Cloud support for 300 masters

From AlliedWare Plus version 5.4.8-2.2 onwards, AMF Cloud supports up to 300 masters with the AMF controller and multi-tenanted masters on a Virtual AMF Appliance (VAA). This VAA may be hosted on Amazon Web Service (AWS), Microsoft Azure, or a customer's private server.

AMF NETWORK SIZE	VCPUS	MEMORY
Multi-tenant VAA with up to 3000 nodes, 3000 virtual-links, 300 containers	8	32GB
Multi-tenant VAA with up to 10000 nodes, 10000 virtual-links, 300 containers	16	48GB
Multi-tenant VAA with up to 18000 nodes, 18000 virtual-links, 300 containers	24	48GB

clear atmf links commands

Occasionally certain events or topology changes can cause AMF links to become outdated. Version 5.4.8-2.2 introduces two new commands to clear these links. Clearing these links forces AMF to relearn the information from neighboring nodes and create a fresh, correct, view of the network.

```
clear atmf links [<interface-list>]
```

Use this command with no parameters to manually reset all the AMF links on a device. You can optionally specify an interface or range of interfaces to reset the links on.

```
clear atmf links virtual [<virtuallink-list>]
```

Use this command with no parameters to manually reset all the AMF virtual links on a device. You can optionally specify a comma separated list of virtual links to reset.

MAC-authentications on AR-series devices

Version 5.4.8-2.2 adds support for MAC-authentication to the switch ports on the following AR-series devices:

- « AR2050
- « AR3050
- « AR4050

MAC-authentication allows a device to authenticate to a network using its MAC address. This is useful for network devices such as printers and scanners that don't implement 802.1.x authentication or allow for user initiated web authentication.

AR-series devices support web authentication on Ethernet ports and MAC-authentication on switch ports, if the device has switch ports.

For more information on MAC-authentication, see the [AAA and Port Authentication Feature Overview and Configuration Guide](#).

Static suffix for RA auto-configuration

Available on all AlliedWare Plus devices

It is now possible to specify a static IPv6 suffix to use together with the prefix that is assigned to the interface. This is an alternative to using an automatically assigned suffix.

To set the static IPv6 suffix, use the new command:

```
awplus(config-if)#ipv6 address suffix <ip-address>
```

Use this command to configure the suffix to use when generating an address from prefix information. Any addresses that were created with the EUI-64 suffix will be removed, and new addresses will be added after the next Router Advertisement.

For more information about IPv6 addressing, see the [IPv6 Feature Overview and Configuration Guide](#).

Link Layer Discovery Protocol (LLDP) support on AR-series

Available on AR2050V, AR3050S and AR4050S

From version 5.4.8-2.2 onwards, LLDP is supported on the AR-series devices.

LLDP can transmit a lot of data about the network. Typically, the network information gathered using LLDP is transferred to a Network Management System by SNMP.

For security reasons, we recommend using SNMPv3 for this purpose (see the SNMP Feature Overview and Configuration Guide).

LLDP operates over switchports only (not eth or management ports). It can be configured on switchports that belong to static or dynamic channel groups, but not on the channel groups themselves.

For more information and configuration examples, see the [LLDP Feature Overview and Configuration Guide](#).

IPv6 Tunneling

Available on AR-series devices

From 5.4.8-2.2 onwards, IPv6 Tunneling is available as a mechanism for encapsulating IPv4 and IPv6 packets within a site-to-site IPv6 VPN. It is used to form a virtual point-to-point link between two IPv6 nodes. IPv6 Tunnels are stateless and have no knowledge of the configuration or even existence of the remote tunnel endpoint. Once an IPv6 Tunnel is configured, packets are encapsulated and forwarded regardless of whether the decapsulating device is present or not.

IPv6 Tunneling allows hosts in one private IP network to communicate with hosts in another private IP network by providing a tunnel between two routers across the Internet. The IPv6 tunnel connection endpoints are terminated via a Virtual Tunnel Interface (VTI) configured in each device.

For more information and a configuration example, see the [IPv6 Tunneling Feature Overview and Configuration Guide](#).

Receive Packet Scheduling

Available for AR2050V, AR3050S and AR4050S

AlliedWare Plus AR-series devices forward packets in software. They contain multi-core processors and hence require a mechanism for processing packets on all available cores. Receive Packet Scheduling is the mechanism used on these devices.

In almost all networks, the default setting for Receive Packet Scheduling setting is the most suitable. However, from 5.4.8-2.2 onwards, Allied Telesis supports a new command to select the scheduling method:

```
awplus(config)#receive-packet-scheduler {hash|balanced|split}
```

Allied Telesis now provides a Technical Guide on Receive Packet Scheduling and how to configure it, if this is necessary in your network. The guide includes a description of the different scheduling methods and the pros and cons for each. The guide concludes with some simple configuration examples and suggestions on how best to use the **receive-packet-scheduler** command options.

To download the guide, click here: [Receive Packet Scheduling Technical Guide](#).

MODBUS

Available on IE300 Series

Version 5.4.8-2.2 adds support for the MODBUS feature. MODBUS is a request-response protocol used in Supervisory Control and Data Acquisition (SCADA) systems for industrial automation devices. It provides a simple open and standardized method for devices to communicate using a client /server model

While initially deployed over RS232 interfaces, versions of the MODBUS protocol exist for serial lines (MODBUS RTU and MODBUS ASCII) and for Ethernet (MODBUS TCP).

AlliedWare Plus™ supports the variant intended for use over Ethernet and IP networks, MODBUS TCP.

The MODBUS feature allows AlliedWare Plus devices to be used for some SCADA processes, such as gathering sensor and alarm information and to control and monitor the state of ports and their PoE state.

For more information and a configuration example, see the [MODBUS Feature Overview and Configuration Guide](#).

Day of the month trigger

Available on all AlliedWare Plus devices

From 5.4.8-2.2 onwards, the **day** command has been expanded to allow you more control over your triggers. Using the **day** command, you can now specify that a trigger will run on a particular day of the month. This can be configured to run:

- On a specific day every month (for example, the 1st of the month)
- On a specific day in a specific month every year (for example, the 1st of January)
- On a specific day in a specific month in a specific year (for example, the 1st of January 2019).

In conjunction with the **type time** command, this gives you considerable customization and control of your triggers.

For more information and a configuration example, see the [Triggers Feature Overview and Configuration Guide](#).

DHCP Framed IP Lease

Available on all AlliedWare Plus devices that support DHCP server.

The DHCP Framed IP Lease feature allows you to automatically configure a DHCP IP lease when a network device is authenticated using 802.1x or MAC authentication. This makes it easier to manage multiple network devices using a central RADIUS server to assign IP addresses and other network settings.

This feature is useful when a network device (e.g. an IP camera) needs to be identified by its IP address. If the device needs replacing it is important that the replacement device has the same IP address and network configuration as the faulty one. DHCP Framed IP Lease allows you to store the DHCP configuration for the device, along with its username and password, on the RADIUS server. When the replacement is installed, the IP address and network configuration will be requested from the RADIUS server by the DHCP server and then applied to the supplicant.

DHCP Framed IP Lease is enabled on a port using the following command:

```
awplus(config-if)#auth dhcp-framed-ip-lease
```

For more information and configuration examples, see the [AAA and Port Authentication Feature Overview and Configuration Guide](#).

Short-term leases for IPv4 DHCP

Available on all AlliedWare Plus devices that support DHCP server.

From software version 5.4.8-2.2, AlliedWare Plus supports IPv4 DHCP short-term-leases with the command:

```
awplus(dhcp-config)#short-lease-threshold <hours> <minutes>
```

DHCP leases need to be backed up in NVS so that when the DHCP sever reboots or goes through a power cycle it won't lose all the knowledge of these leases.

Some networks have a high number of mobile devices repeatedly requesting DHCP leases every few seconds before their existing lease expires. This can happen, for example, when mobile devices move in and out of a WiFi zone or when WiFi signal strength changes. This means the same IP address can have multiple lease entries which can take up unnecessary backup file space.

The **short-lease-threshold** command allows you to configure the threshold for short leases, from 1 minute to 24 hours. Any lease shorter than the threshold is deemed to be a short lease and will not be backed up to NVS.

This is useful if you have:

- limited backup file space, and
- you don't need to restore leases after a device reboot or power cycle.

For more information about DHCP, see the [DHCP Feature Overview and Configuration Guide](#).

Improvements to "show" commands for multicasting

Available on all platforms that support PIM or IGMP

Version 5.4.8-2.2 includes new and updated **show** commands for multicasting.

New commands, available on all platforms that support PIM-SM or IGMP:

- **show ip pim sparse-mode mroute brief**
This command summarizes the number of PIM sparse-mode mroutes.
- **show ip igmp groups brief**
This command summarizes the number of IGMP groups.

New commands, available on IE510-28GSX-80, IX5-28GPX and SBx908 GEN2 switches and x310, IE300, x510, x510L, x550 and x930 Series switches:

- **show platform table ipmulti-brief**
This command summarizes the number of L3 entries in hardware.
- **show platform table ipmulti-count**
This command counts the number of L3 entries in hardware.

Commands with improved output, available on all platforms that support PIM-SM:

- **show ip pim sparse-mode mroute**
Previously, this command used dots to indicate the number of interfaces. Now it uses a count instead.
- **show ipv6 pim sparse-mode mroute**
Previously, this command used dots to indicate the number of interfaces. Now it uses a count instead.
- **show ipv6 pim sparse-mode interface**
This command now includes configured interfaces, and the maximum number of interfaces allowed.

For more information about PIM-SM, see the [PIM-SM Feature Overview and Configuration Guide](#).

For more information about IGMP, see the [IGMP/MLD Feature Overview and Configuration Guide](#).

Setting an alias name for a switch port for SNMP

Available on all AlliedWare Plus devices except AR2010V

Version 5.4.8-2.2 supports a new command for setting an alias name for a switch port, as returned by the SNMP ifMIB in OID 1.3.6.1.2.1.31.1.1.1.18.

The command syntax is:

```
awplus(config-if)#alias <ifAlias>
awplus(config-if)#no alias
```

The alias can be any printable character.

Third-party management systems often use standard MIBs to access device information. Network managers can specify an alias interface name to provide a non-volatile way to access the interface.

For more information about Allied Telesis MIB support, see [Support for Allied Telesis Enterprise MIBs in AlliedWare Plus](#) and the [SNMP Feature Overview and Configuration Guide](#).

Improvements to QoS storm protection log messages

Available on all AlliedWare Plus devices that support QoS storm protection

The log messages for QoS storm protection have been modified to include the words “QoS storm protection”.

For example, if QoS storm protection takes a link down, the log message now reads:

```
2018 Nov 05 08:30:05 user.info x930-6 NSM[962]: QSP: Interface port1.0.1 has been
disabled with action link-down by QoS storm protection
```

PSU and fan module presence notification

Available on SBx8100 Series, SBx908 GEN2 switches, x950 Series, x930 Series, x510DP Series, and IX5-28GPX switches

New SNMP trap

Version 5.4.8-2.2 includes improved SNMP notifications when a PSU or fan module is removed or inserted.

A new trap “atEnvMon2Notifications19” is generated when an insertion or removal event is detected on a power supply bay device. For more information about “atEnvMonv2Notifcations19” see [Support for Allied Telesis Enterprise MIBs in AlliedWare Plus](#).

Additionally, the power input/output alarm notifications that were previously sent after a PSU removal are no longer emitted. These notifications will still be sent when the power status changes.

New Format for Platform Log Messages

The format of platform sensor and hotswap messages has changed. This affects all log messages that were previously prefixed with "HPI:". The messages are now prefixed with "Platform:" and the format has changed to make it clearer which piece of hardware the message relates to. The stack member or card that the message applies to is now included on stackable and chassis systems. For state sensors, the triggering state is also included.

New format for Hotswap messages

Hotswap messages now have the format:

Platform: HOTSWAP <stack member> <bay_name>: <board_class> - <board_name>:
(inserted/removed)

For example:

Platform: HOTSWAP stack member 2 Bay2: Expansion - XEM-12Tv2:
inserted

Platform: HOTSWAP card 1.5 PSUB: PSU - AT-SBxPWRPOE1/AC:
removed

New format for Sensor messages

Sensor messages all begin with a common format and then have different endings depending on the type. The bay names are as shown in the **show system** command. The bay name for the system board is "Base".

The common section looks like:

Platform" SENSOR <stack member> (Bay|Board) <bay_name> - <sensor_name>:
<event_string>

Event_string	Description
Alarm asserted	The sensor alarm condition has been met
Alarm cleared	The sensor alarm condition has been cleared
State change	The sensor state has changed (but this is not necessarily cause for alarm)

Threshold sensor message suffix:

After the common section, threshold sensor messages end with:

Reading: <reading> Threshold: <threshold> (<units>)

For example:

Platform: SENSOR card 1.6 Board Base - Temp: Internal: Alarm asserted. Reading:51 Threshold:50 (Degrees C)

State sensor message suffix:

After the common section, state sensor messages end with:

<state_string>

The state_string can be either a state 1 string or a state 2 string, as show in the table below. For example:

Platform: SENSOR stack member 2 Board Base - Contact Input 1:
State change. Opened

Platform: SENSOR card 1.5 Bay PSUB – PSU Power Output: Alarm asserted. Unpowered

Sensor type	State 1 state_string	State 2 state_string
Module presence	Inserted	Removed
Contact input/Relay output	Opened	Closed
LED Output	On	Off
Power Supply	Powered	Unpowered
All other state sensor types	Yes	No

Bidirectional Forwarding Detection (BFD) on the SwitchBlade x8100 CFC960

AlliedWare Plus Bidirectional Forwarding Detection (BFD) is a network protocol. BFD is used to detect fast forwarding path failure for layer 2 redundancy protocols such as STP, RSTP, MSTP, EPSR and G.8032.

BFD operates directly over the Ethernet across all media types to detect link failures and speed up the convergence time of layer 2 protocols. Link failures can be a result of power failure, incorrect configuration, physical fault, or miswiring.

For more information and a configuration example, see the [Bidirectional Forwarding Detection \(BFD\) Feature Overview and Configuration Guide](#).

Upstream Forwarding Only (UFO) on the SwitchBlade x8100 CFC960

From 5.4.8-2.2 onwards, the Private VLAN feature UFO is available is on the SBx8100 Series with the SBx81CFC960 control card. UFO blocks the forwarding of Ethernet frames between certain ports of a UFO VLAN, while allowing forwarding of others.

For the SBx81CFC960, there are some limitations to be aware of:

- Private VLAN UFO is limited to 16 VLANs.
- UFO and VLAN translation are both implemented using Egress PCL rules, so only one of these features can be configured on a port to function properly. This means that if a port is configured as a UFO port, then VLAN translation should not be configured on this port and vice versa.
- RSPAN and Port Mirroring are not supported on a UFO VLAN port.

For more information and a UFO configuration example using Egress PCL rules, see the [UTM Offload Feature Overview and Configuration Guide](#).

For more information and a UFO configuration example using Egress PCL rules, see the [VLANs Feature Overview and Configuration Guide](#).

Secure Mode on SBx908 GEN2 switches and x950 Series switches

Now available on x950 Series and SBx908 GEN2 switches. Available in previous releases on a number of other switches

Version 5.4.8-2.2 supports Secure Mode on SBx908 GEN2 switches. When in Secure Mode, the following are disabled:

- Telnet
- SSHv1
- SNMPv1/v2
- All privilege levels except 1 and 15
- Algorithms that are not supported under FIPS, including MD5, RSA-1 and DSA
- The ability to store passwords in cleartext and to specify an **enable** password

In Secure Mode, the web server on the switch (used by the Device GUI) only accepts AES128-SHA ciphers.

Entering Secure Mode

1. Obtain the correct release file and its sha256sum file, for example by downloading them from the [Allied Telesis Download Center](#). Save the files on a trusted USB device and connect the USB device to the switch.
2. Before entering Secure Mode, erase the Flash. To do this, boot the device into the bootloader diagnostics menu, using Ctrl-D. Select option 7 'Bootup stage 2 diagnostics menu', and then select option 4 'Erase FLASH (Filesystem only)'.
3. Then select option 0 'Restart' to reboot the device. Enter the main bootloader menu by using Ctrl-B. Select option 1 'Perform one-off boot from alternate source' and then select the 'USB' option and the release you saved in step 1.
4. Once the switch has booted up, save the release file to Flash and verify it, as described in ["Verifying the Release File" on page 77](#).

5. Set the verified release as the boot release. For example, use the following commands:

```
awplus#configure terminal
awplus(config)#boot system x950-5.4.8-2.2.rel
```

6. Use the following commands to enter secure mode:

```
awplus(config)# crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

7. Use the following command to confirm that the switch is in secure mode:

```
awplus# show secure-mode
```

The following message should be displayed:

```
Secure mode is enabled
```

Leaving Secure Mode

1. If you wish to leave Secure Mode, you should delete all sensitive information first. This means deleting all trustpoints (one by one), by using the commands:

```
awplus# configure terminal
awplus(config)# no crypto pki trustpoint <name>
```

Also, delete all public/private key pairs, by using the commands:

```
awplus# crypto key zeroize all
```

2. Turn off Secure Mode, by using the commands:

```
awplus(config)# no crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

3. Reboot the switch. The switch **must** be rebooted after Secure Mode is turned off, and ideally Flash memory should be erased via the bootloader, as described above.

Virtual Chassis Stacking (VCStack) on x950 Series switches

Version 5.4.8-2.2 adds support for VCStack on x950 Series switches. Many other AlliedWare Plus switches already support VCStack.

VCStack provides a highly available system where network resources are spread out across stacked units, reducing the impact if one of the units fails. Aggregating switch ports on different units across the stack provides excellent network resiliency.

Long-distance stacking allows a VCStack to be created over fiber links to span longer distances, for resiliency within a distributed network environment.

Version 5.4.8-2.2 supports stacking of two x950 Series switches.

For detailed instructions about how to create a VCStack, see the [Installation Guide: AT-x950-28XSQ Switch and VCStack](#).

Specifying a name for OpenFlow controllers

Available on all AlliedWare Plus devices that support OpenFlow controllers

Version 5.4.8-2.2 enables you to name OpenFlow controllers.

To do this, use the new parameter `<controller-name>` with the command **openflow controller**.

The `<controller-name>` parameter:

- Simplifies the deletion of a controller because the deletion command is now simply:
no openflow controller <controller-name>
- Increases configuration comprehension by providing a descriptive name.

For more information about the OpenFlow protocol, see the [OpenFlow Feature Overview and Configuration Guide](#).

The OpenFlow protocol on x950 Series switches

From 5.4.8-2.2 onwards, AlliedWare Plus supports version 1.3 of the OpenFlow protocol on x950 Series switches. A number of other AlliedWare Plus switches already support the OpenFlow protocol.

These switches enable the OpenFlow protocol on a per-port basis, so you can choose which ports of the switch will be controlled by the OpenFlow protocol. Non-OpenFlow-enabled ports continue to support existing features of the device.

For more information and configuration details, see the [OpenFlow Feature Overview and Configuration Guide](#).

Forcing combo ports on x930-28GSTX switches to only accept either copper or fiber pluggables

x930-28GSTX switches include combo ports, which have an RJ45 copper side and an SFP fiber side. The switch automatically detects whether the copper or fiber side is used.

Version 5.4.8-2.2 enables you to only allow use of either the copper or fiber port for a given combo port pair, instead of automatically determining the medium type. To do this, use the new command:

```
awplus(config-if)#medium-type {auto|copper|fiber}
```

G.8032 on x220 Series switches

Version 5.4.8-2.2 adds support for G.8032 ring protection x220 Series switches. A number of other AlliedWare Plus switches already support G.8032.

G.8032 is an International Telecommunication Union (ITU) standard for Ethernet Ring Protection Switching (ERPS). It prevents loops on a per-VLAN basis with networks that are wired in a simple ring topology, and (with G.8032 Version 2) multiple ring and ladder topologies. G.8032 offers a rapid detection and recovery time if a link or node fails, in the order of 50 ms, depending on configuration.

For more information and configuration details, see the [G.8032 Feature Overview and Configuration Guide](#).

Connectivity Fault Management (CFM) on x220, x230 and x230L Series switches

Version 5.4.8-2.2 adds support for Connectivity Fault Management (CFM) on x220, x230 and x230L Series switches. A number of other AlliedWare Plus switches already support CFM.

CFM is an IEEE 802.1ag and ITU Y.1731 standard for managing connectivity at the Ethernet service level. The 802.1ag standard adds Fault management capabilities to Ethernet, while the ITU Y.1731 standard expands the capabilities to include Performance.

Ethernet CFM provides the network operator with a way to detect faults in the network, and to isolate the location of the fault at either the link level (i.e. port) or at the VLAN level. Y.1731 extends this, and also provides a way to manage Service Level Agreements (SLAs) at the link level, but more importantly at the VLAN level.

For more information and configuration details, see the [CFM Feature Overview and Configuration Guide](#).

Important Considerations Before Upgrading

This section describes changes that are new in 5.4.8-x.x and may affect your network behavior if you upgrade. Please read it carefully before upgrading.

It describes the following changes:

- [Change to format of LLDP and SNMP system description responses](#)
- [Using a 1G Fiber SFP in an SFP+ port on an x930 Series switch](#)
- [Reduction in number of RIP routes on x930 Series switches](#)
- [Spurious log message on failover or hotswap on SBx8100 Series switches](#)
- [Device GUI files synchronized across stack members](#)
- [Limits for AWC neighbor show commands](#)
- [Parameter name change for provisioning SwitchBlade x908 GEN2 switches](#)
- [Increase to rate at which multicast packets are sent to the CPU](#)
- [Delay at startup before connecting to remote log hosts](#)
- [x230 Series now support 118 ACLs](#)
- [Startup configuration errors when provisioning stackports on CFC960](#)
- [IPv6 traffic uses only the first available nexthop in a PBR rule](#)
- [Executing WRR queue commands interrupts traffic on SBx908 GEN2](#)
- [Changes to the recommended method of removing a switch from a VCStack](#)

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 5.4.8-x.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.4.7-1.x version, please check the 5.4.7-2.x release note. Release notes are available from our website, including:

- [5.4.7-x.x release notes](#)
- [5.4.6-x.x release notes](#)

Change to format of LLDP and SNMP system description responses

From 5.4.8-2.2 onwards, the format of LLDP and SNMP system description responses is "Allied Telesis router/switch, Software (AlliedWare Plus) Version <version>". Previously, the format was "Allied Telesis router/switch, AW+ v<version>".

The change improves the ability of some NMS software to parse this string for software and version information.

Using a 1G Fiber SFP in an SFP+ port on an x930 Series switch

From 5.4.8-2.2 onwards, if an x930 Series switch is connected to another x930 Series switch through a 1G fiber SFP in an SFP+ port, then the link may not link up or may not come back up after disconnecting and re-connecting.

To avoid this issue, use the **speed 1000** command to configure a fixed speed on the ports, instead of using autonegotiation.

Reduction in number of RIP routes on x930 Series switches

From 5.4.8-1.2 onwards, the maximum number of RIP routes on x930 Series switches is 10,000.

Spurious log message on failover or hotswap on SBx8100 Series switches

Applies to SBx8100 Series switches

From 5.4.8-1.2 onwards, on CFC failover or linecard hotswap, an error level message like the following will be logged on the (new) active CFC:

"CMSG(1061).platform.n.tipc[18]: Subscriber is not reachable after 10 tries and will be removed."

This message is expected and can be safely ignored.

Device GUI files synchronized across stack members

Applies to AlliedWare Plus switches that support VCStack

From 5.4.8-1.2 onwards, the Device GUI file is automatically synchronized to backup stack members, so they can use the GUI if the stack master reboots.

Limits for AWC neighbor show commands

Applies to AR-Series devices and SBx908 GEN2 switches

From 5.4.8-1.2 onwards, if the total number of Access Point (AP) neighbors in the system exceeds 12500, the following commands will only show the first 12500 neighbors:

- show wireless ap neighbors
- show wireless ap all neighbors

You can specify the AP ID to see all neighbors of each AP.

Parameter name change for provisioning SwitchBlade x908 GEN2 switches

Applies to SBx908 GEN2 switches

From 5.4.8-1.2 onwards, the command for provisioning an SBx908 GEN2 stack member has changed. It is now:

```
awplus(config)#switch <stack-ID> provision sbx908gen2
```

If you upgrade to 5.4.8-1.2 or later and your configuration file includes the previous syntax, AlliedWare Plus will automatically update it to the new syntax.

However, if you upgrade and then later downgrade to 5.4.8-0.x or earlier, your configuration file will keep the new syntax, which the switch will not recognize. After such a downgrade, provisioning also wouldn't be applied for any provisioned XEMs, because they depend on the switch provisioning, and configuration wouldn't be applied on provisioned interfaces. You would see error messages to warn you of this.

Increase to rate at which multicast packets are sent to the CPU

SBx8100, SBx908 GEN2 and x930 Series now send multicast packets to the CPU at a maximum rate of 100 packets per second by default, instead of the previous limit of 10 pps. If you want to reduce the CPU load on your switch, you can reduce this rate by using the following command:

```
awplus(config)#platform multicast-ratelimit <0-100>
```

Delay at startup before connecting to remote log hosts

Applies to all AlliedWare Plus devices

When the device boots up, there is a delay before it attempts to connect to remote log hosts. This is to allow time for the device to establish network connectivity to the remote host. During this period, the device buffers log messages and sends them once it has connected to the remote host.

From version 5.4.8-0.2 onwards, this delay is active by default and can't be turned off, and the default delay has been increased. The delay also now applies to event hosts.

The command to configure the delay is:

```
awplus(config)#log host startup-delay [delay <1-600>]  
[messages <1-5000>]
```

By default the system will buffer up to 2000 messages and wait 120s from when syslog starts before attempting to filter and transmit the buffered messages to remote hosts. If the default startup delay is not long enough for the boot and configuration process to complete and the links to come up, you may see logging failure messages on startup. In such cases, you can use the command to increase the startup delay.

x230 Series now support 118 ACLs

Applies to x230 Series switches

From 5.4.8-0.2 onwards, x230 Series switches support a maximum of 118 user-configurable ACLs. Previously, the maximum was 119.

Startup configuration errors when provisioning stackports on CFC960

Applies to SBx81CFC960

From 5.4.8-0.2 onwards, the stacking ports on provisioned switches and CFC960 control cards are displayed as stackports in the running configuration. Previously, they were displayed as access ports.

On a CFC960, this means that if you save the configuration on a previous release, and then you upgrade to 5.4.8-1.2 or later, the switch may report command errors on start-up. You can ignore these errors.

An example of such errors is:

WARNING: Failed to execute the following commands:

```
219: switchport -- % The command is not available for this interface
220: switchport mode access -- % The command is not available for
this interface
304: switchport -- % The command is not available for this interface
305: switchport mode access -- % The command is not available for
this interface
```

You are unlikely to see such errors on other switches. On other switches, if stackports are included in an interface range command with switchports, AlliedWare Plus removes the stackports from the range automatically. Therefore, the commands that generate the errors are not executed.

IPv6 traffic uses only the first available nexthop in a PBR rule

Applies to AR4050S and AR3050S firewalls and AR2050V and AR2010V routers

From 5.4.8-0.2 onwards, if a policy-based routing (PBR) rule contains multiple IPv6 nexthops, the device sends IPv6 traffic only via the first available nexthop in the list.

Previously, although most traffic would take the first available nexthop, a small amount of the traffic would be spread over the remaining nexthops. This meant that some traffic did not take the expected path.

Executing WRR queue commands interrupts traffic on SBx908 GEN2

Applies to SBx908 GEN2 switches

From 5.4.8-0.2 onwards, executing the following commands on an SBx908 GEN2 interrupts traffic flow:

```
wrr-queue weight  
no wrr-queue
```

The interruption lasts for less than a second and resolves automatically.

When you enter either of the above commands, the switch displays a message to warn you about the traffic interruption and allow you to abort the command.

Changes to the recommended method of removing a switch from a VCSStack

Applies to all switches that support VCSStack

Previously, it was possible to enter the **no stack <stack-id> enable** command to remove a switch from a stack while the switch was still an active member of the stack.

From 5.4.8-0.2 onwards, this is no longer possible. Instead, use the following steps to remove a switch from a stack:

1. Shut down all stacking links to the switch you wish to remove from the stack. This is optional but recommended, especially if someone other than you will do the step of physically uncabling the switch.
2. Remove all of the cabling used for stacking links.
3. Re-cable the remaining stack members together correctly.
4. Log into the disconnected device and run the command **no stack <stack-id> enable**.
5. If you want to use the switch as a standalone switch, reset its stack ID to 1. Use the command **stack <old-id> renumber 1**

Software Release Licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.4.8 license on your switch if you are upgrading to 5.4.8-2.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 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80](#).

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 5.4.8-2.2 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 5.4.8-2.x from:

- 5.4.8-1.x
- 5.4.8-0.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 5.4.8-2.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 5.4.8-2.x and:

- 5.4.8-1.x
- 5.4.8-0.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 5.4.8-2.x and 5.4.6-1.1 or **any** earlier releases.

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

If using an AMF controller

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

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

If using secure mode

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

If using Vista Manager EX

If you are using Vista Manager EX, 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 5.4.8-2.x are compatible with nodes running:

- 5.4.8-1.x
- 5.4.8-0.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 Guides in the right-hand menu.

Verifying the Release File

On SBx908 GEN2, x950, x930, x550, XS900MX and x220 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 enter 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.

Verifying the release on subsequent boot-ups

Once the switch has successfully verified the release file, it adds the **crypto verify** command to the running configuration.

If the switch is in secure mode, it will verify the release file every time it boots up. To do this, it runs the **crypto verify** command while booting. Therefore, you need to copy the **crypto verify** command to the startup configuration, by using the command:

```
awplus#copy running-config startup-config
```

If the **crypto verify** command is not in the startup configuration, the switch will report a verification error at bootup.

If there is a verification error at bootup, the switch produces an error message and finishes booting up. If this happens, run the **crypto verify** command after bootup finishes, to verify the running release file. If verification of the running release file fails, delete the release file and contact Allied Telesis support.

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 demol.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 : 30-Mar-2018
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    : 5.4.8
Customer name   : ABC Consulting
Quantity of licenses : 1
Type of license : Full
License issue date : 30-Mar-2018
License expiry date : N/A
Release         : 5.4.8
```

Licensing this Version on an SBx8100 Series Switch 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 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-2018
License expiry date : N/A
Features included : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                  Virtual-MAC, VRRP

Index          : 2
License name    : 5.4.8
Customer name   : ABC Consulting
Quantity of licenses : -
Type of license : Full
License issue date : 20-Mar-2018
License expiry date : N/A
Release        : 5.4.8
```

Installing this Software Version

Caution: Software version 5.4.8-2.x 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 78](#) and
- [“Licensing this Version on an SBx8100 Series Switch Control Card” on page 80.](#)

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
FS980M series	<code>awplus(config)# boot system FS980-5.4.8-2.10.rel</code>
GS900MX/MPX series	<code>awplus(config)# boot system GS900-5.4.8-2.10.rel</code>
GS970M series	<code>awplus(config)# boot system GS970-5.4.8-2.10.rel</code>
GS980M series	<code>awplus(config)# boot system GS980M-5.4.8-2.10.rel</code>
XS900MX series	<code>awplus(config)# boot system XS900-5.4.8-2.10.rel</code>
x220 series	<code>awplus(config)# boot system x220-5.4.8-2.10.rel</code>
x230 series	<code>awplus(config)# boot system x230-5.4.8-2.10.rel</code>
IE200 series	<code>awplus(config)# boot system IE200-5.4.8-2.10.rel</code>
IE210L series	<code>awplus(config)# boot system IE210-5.4.8-2.10.rel</code>
x310 series	<code>awplus(config)# boot system x310-5.4.8-2.10.rel</code>
IE300 series	<code>awplus(config)# boot system IE300-5.4.8-2.10.rel</code>

Product	Command
IX5-28GPX	<code>awplus(config)# boot system IX5-5.4.8-2.10.rel</code>
x510 series	<code>awplus(config)# boot system x510-5.4.8-2.10.rel</code>
x550 series	<code>awplus(config)# boot system x550-5.4.8-2.10.rel</code>
IE510-28GSX	<code>awplus(config)# boot system IE510-5.4.8-2.10.rel</code>
x550 series	<code>awplus(config)# boot system x550-5.4.8-2.10.rel</code>
x930 series	<code>awplus(config)# boot system SBx930-5.4.8-2.10.rel</code>
x950 series	<code>awplus(config)# boot system x950-5.4.8-2.10.rel</code>
SBx908 GEN2	<code>awplus(config)# boot system SBx908NG-5.4.8-2.10.rel</code>
SBx8100 with CFC400	<code>awplus(config)# boot system SBx81CFC400-5.4.8-2.10.rel</code>
SBx8100 with CFC960	<code>awplus(config)# boot system SBx81CFC960-5.4.8-2.10.rel</code>
AR2010V	<code>awplus(config)# boot system AR2010V-5.4.8-2.10.rel</code>
AR2050V	<code>awplus(config)# boot system AR2050V-5.4.8-2.10.rel</code>
AR3050S	<code>awplus(config)# boot system AR3050S-5.4.8-2.10.rel</code>
AR4050S	<code>awplus(config)# boot system AR4050S-5.4.8-2.10.rel</code>

- Return to Privileged Exec mode and check the boot settings, using:

```
awplus(config)# exit
```

```
awplus# show boot
```

- Reboot using the new software version.

```
awplus# reload
```

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 accessing the GUI depend on whether the 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. See:

- [All devices: GUI pre-installed at factory](#)
- [AR-Series devices: GUI not pre-installed or updating the GUI](#)
- [Switches: GUI not pre-installed or updating the GUI](#)

All devices: GUI pre-installed at factory

Perform the following steps to browse to the GUI if your device came with the GUI pre-installed.

If the firewall is enabled on an AR-series device, 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. Connect to any of the LAN switch ports.
2. Open a web browser and browse to the default IP address for VLAN1. The default address is:

Device	Address
AR-Series	192.168.1.1
Switches	169.254.42.42

Alternatively, give VLAN1 an IP address of your choice and browse to that address.

3. Log in with the default username of *manager* and the default password of *friend*.

AR-Series devices: GUI not pre-installed or updating the GUI

Perform the following steps through the command-line interface if:

- your AR-series device did not come with the GUI pre-installed, or
 - you have been running an earlier version of the GUI and need to update it (steps 3 onwards).
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. 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. If you are updating the GUI, stop and restart the HTTP service:

```
awplus# configure terminal
awplus(config)# no service http
awplus(config)# service http
```
 5. If you are installing the GUI for the first time, 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.

Switches: GUI not pre-installed or updating the GUI

Perform the following steps through the command-line interface if:

- your AlliedWare Plus switch did not come with the GUI pre-installed, or
 - 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 5.4.8-2.2 is `awplus-gui_548_09.tar.gz`.

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_548_09.tar.gz 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, it is advisable to 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. 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. If you are updating the GUI, stop and restart the HTTP service:

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

6. If you are installing the GUI for the first time, make sure the HTTP service is running:

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

7. 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*.