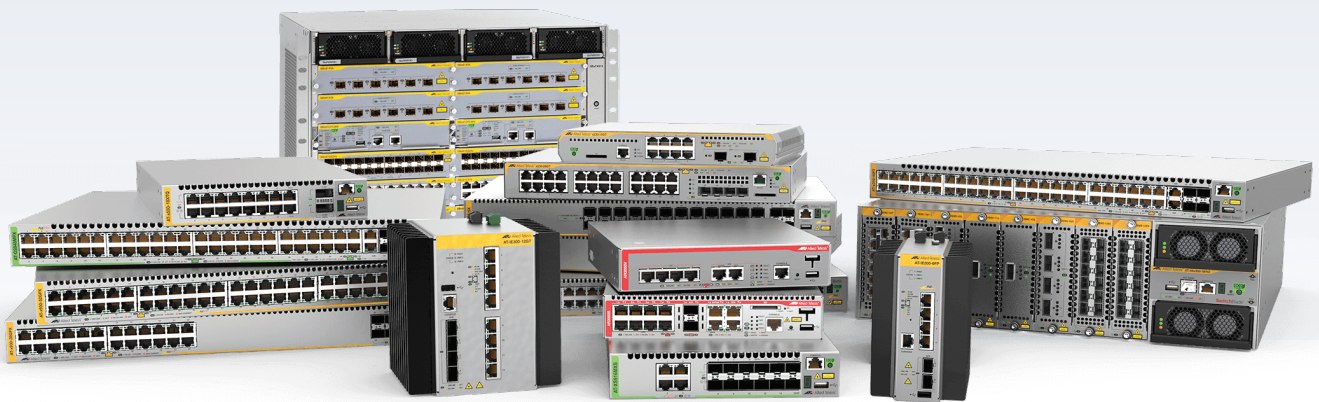


Release Note for AlliedWare Plus Software Version 5.4.9-1.x



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 » IE340 Series » IE300 Series » IE210L Series » IE200 Series
- » XS900MX Series » GS980M Series » GS970M Series
- » GS900MX/MPX Series » FS980M Series » AMF Cloud
- » AR4050S » AR3050S » AR2050V » AR2010V » AR1050V
- » 5.4.9-1.1 » 5.4.9-1.2 » 5.4.9-1.3 » 5.4.9-1.4 » 5.4.9-1.5 » 5.4.9-1.6 » 5.4.9-1.7

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

©2019 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 5.4.9-1.7	3
Introduction.....	3
New Features and Enhancements.....	6
Issues Resolved in Version 5.4.9-1.7	7
What's New in Version 5.4.9-1.6	10
Introduction.....	10
New Features and Enhancements.....	13
What's New in Version 5.4.9-1.5	14
Introduction.....	14
Issues Resolved in Version 5.4.9-1.5	17
What's New in Version 5.4.9-1.4	19
Introduction.....	19
Issues Resolved in Version 5.4.9-1.4	22
What's New in Version 5.4.9-1.3	24
Introduction.....	24
New Features and Enhancements.....	27
Issues Resolved in Version 5.4.9-1.3	28
What's New in Version 5.4.9-1.2	34
Introduction.....	34
Issues Resolved in Version 5.4.9-1.2	37
What's New in Version 5.4.9-1.1	38
Introduction.....	38
New Products.....	41
New Features and Enhancements.....	43
Important Considerations Before Upgrading	49
Obtaining User Documentation	55
Verifying the Release File	55
Licensing this Version on an SBx908 GEN2 Switch	56
Licensing this Version on an SBx8100 Series CFC960 Control Card	58
Installing this Software Version	60

Installing and Accessing the Web-based Device GUI 62

What's New in Version 5.4.9-1.7

Product families supported by this version:

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-1.7.

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.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 60](#).

For instructions on how to update the web-based GUI, see [“Installing and Accessing the Web-based Device GUI” on page 62](#). The GUI offers easy visual monitoring and configuration of your device.



Caution: Software version 5.4.9-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 versions. 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 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58](#).



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:

Models	Family	Date	Software File
AMF Cloud		11/2019	vaa-5.4.9-1.7.iso (VAA OS) vaa-5.4.9-1.7.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-1.7.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2019	SBx81CFC960-5.4.9-1.7.rel
SBx908 GEN2	SBx908 GEN2	11/2019	SBx908NG-5.4.9-1.7.rel
x950-28XSQ x950-28XTQm	x950	11/2019	x950-5.4.9-1.7.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2019	x930-5.4.9-1.7.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2019	x550-5.4.9-1.7.rel
x530-28GTXm x530-28GPXm x530L-52GPX	x530 and x530L	11/2019	x530-5.4.9-1.7.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	11/2019	x510-5.4.9-1.7.rel
IX5-28GPX	IX5	11/2019	IX5-5.4.9-1.7.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2019	x310-5.4.9-1.7.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2019	x230-5.4.9-1.7.rel

Models	Family	Date	Software File
x220-28GS x220-52GT x220-52GP	x220	11/2019	x220-5.4.9-1.7.rel
IE510-28GSX	IE510-28GSX	11/2019	IE510-5.4.9-1.7.rel
IE300-12GT IE300-12GP	IE300	11/2019	IE300-5.4.9-1.7.rel
IE340-20GP IE340L-18GP	IE340	11/2019	IE340-5.4.9-1.7.rel
IE210L-10GP IE210L-18GP	IE210L	11/2019	IE210-5.4.9-1.7.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2019	IE200-5.4.9-1.7.rel
XS916MXT XS916MXS	XS900MX	11/2019	XS900-5.4.9-1.7.rel
GS980M/52 GS980M/52PS	GS980M	11/2019	GS980M-5.4.9-1.7.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2019	GS970-5.4.9-1.7.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2019	GS900-5.4.9-1.7.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	11/2019	FS980-5.4.9-1.7.rel
AR4050S AR3050S	AR-series UTM firewalls	11/2019	AR4050S-5.4.9-1.7.rel AR3050S-5.4.9-1.7.rel
AR2050V AR2010V AR1050V	AR-series VPN firewalls	11/2019	AR2050V-5.4.9-1.7.rel AR2010V-5.4.9-1.7.rel AR1050V-5.4.9-1.7.rel

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

Please note, the 5.4.9-1.7 software version is ISSU incompatible with software version 5.4.9-1.6.

New Features and Enhancements

This AlliedWare Plus maintenance version includes the following enhancements:

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE30	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-3142	Switching	With this software update, the SBx81XLEM is now supported in platform silicon-profile profile1, with the SBx81GT40, SBx81XS16, SBx81XS6 and SBx81GS24a cards. The profile allows larger various table sizes.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-
ER-3174	AMF	With this software update, TQ access points can be replaced easily without having to worry about username and password configuration on the AMF guest node.	Y	Y	Y	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 5.4.9-1.7

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	DC2552XS/L3	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-65254	AMF	<p>Previously, isolated node recovery would be enabled for all devices where the only viable link to the core was via a virtual link.</p> <p>As a consequence, some configurations that were unsupported for Isolated Node Recovery would result in log messages and error messages when there was an alternate means of recovery available, such as via externally attached storage media.</p> <p>This has now been changed such that Isolated Node Recovery is not enabled when external media is present, as external media will always be used for recovery in preference to Isolated Node Recovery.</p> <p>Note that the mechanism that handles the presence of external media to update Isolated Node Recovery operates on a timer, and as a consequence if a backup runs within 6 minutes of an external media insertion event, a log message may still be generated. If a backup runs while external media is not available, viewing the backup will show an error message. This situation will persist until the next time a backup is run with external media inserted.</p> <p>This issue has been resolved.</p>	-	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-65781	AMF	<p>Previously, utilization of an AlliedWare Plus device as an AMF guest could fail because of an internal communication error between the AMF node and the guest.</p> <p>This issue has been resolved.</p>	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	DC2552XS/L3	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud		
CR-66091	Device Security SSH	With this software update, the "diffie-hellman-group1-sha1" has been removed as an SSH key exchange algorithm option in order to comply with the current ICSCA certification requirements.	Y	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-66037	Device Security SSH	With this software update, 3DES has been removed from the supported cypher set for SSH as it is no longer considered secure enough. This is required for ICSCA certification. Modern clients and servers can continue to interoperate using AES-based cyphers transparently.	Y	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-66003	DHCP Snooping	Previously, when DHCP snooping was enabled, some DHCP packets from the clients with particular IP header length values might be ignored. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-	-	
CR-65559	IGMP	With this software update, the IGMPv3 TO_EXCLUDE messages are no longer dropped when the host is operating in IGMPv1 compatibility mode in accordance with RFC3376.	Y	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-63720	IPv6	Previously, the 'ipv6 nd prefix lifetime' parameter was not added to the running configuration. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	-
CR-63898	OSPFv2	Previously, in OSPF networks where routers were performing inter-area routing and also had summary routes configured, when using the area X range command, if multiple routers within the network had the same summary routes configured, then in some circumstances where an OSPF boarder router generating such a summary route lost communication with its neighbor, it could fail to install backup routes for that same summary network via the other routers. This issue has been resolved.	-	-	Y	-	-	-	Y	-	Y	-	-	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	-	

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	DC2552XS/L3	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-65996	PIM-DM v4 Unicast Forwarding	Previously, a switch with PIM-DM configured might cause the switch CPU to operate at 100% utilization. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-	-
CR-66062	Tunnelling	Previously, when configuring tunnels on a device, use of an uncommon combination of command options, such as "tunnel df" and "tunnel ttl" could cause the device to restart unexpectedly if show running-config was subsequently executed. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	
CR-63682	Web API	Previously, it was possible for the error message below to be logged spuriously, particularly for a system under high load: <i>"CMMSG(286).tport.interface..tipc[01]: Receive timed out socket 97 nbytes was -1 last error Resource temporarily unavailable"</i> This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	-

What's New in Version 5.4.9-1.6

Product families supported by this version:

AR4050S	x220 Series
AR3050S	x230 Series
AR2050V	x230L Series
AR2010V	x310 Series
AR1050V	IX5-28GPX
FS980M Series	x510 Series
GS900MX/MPX Series	x510L Series
GS970M Series	x530 Series
GS980M Series	x530L Series
GS980MX Series	x550 Series
XS900MX Series	x930 Series
IE200 Series	x950 Series
IE210L Series	SwitchBlade x908 Generation 2
IE300 Series	SwitchBlade x8100: SBx81CFC960
IE510-28GSX Series	AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-1.6.

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.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 60](#).

For instructions on how to update the web-based GUI, see [“Installing and Accessing the Web-based Device GUI” on page 62](#). The GUI offers easy visual monitoring and configuration of your device.



Caution: Software version 5.4.9-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 versions. 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 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58](#).



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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	10/2019	FS980-5.4.9-1.6.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	10/2019	GS900-5.4.9-1.6.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2019	GS970-5.4.9-1.6.rel
GS980M/52 GS980M/52PS	GS980M/MX	10/2019	GS980M-5.4.9-1.6.rel
XS916MXT XS916MXS	XS900MX	10/2019	XS900-5.4.9-1.6.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	10/2019	IE200-5.4.9-1.6.rel
IE300-12GT IE300-12GP	IE300	10/2019	IE300-5.4.9-1.6.rel
IE210L-10GP IE210L-18GP	IE210L	10/2019	IE210-5.4.9-1.6.rel
IE510-28GSX	IE510-28GSX	10/2019	IE510-5.4.9-1.6.rel
x220-28GS x220-52GT x220-52GP	x220	10/2019	x220-5.4.9-1.6.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2019	x230-5.4.9-1.6.rel

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

Models	Family	Date	Software File
x310-26FT x310-50FT x310-26FP x310-50FP	x310	10/2019	x310-5.4.9-1.6.rel
IX5-28GPX	IX5	10/2019	IX5-5.4.9-1.6.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	10/2019	x510-5.4.9-1.6.rel
x530-28GTXm x530-28GPXm x530L-52GPX	x530 and x530L	10/2019	x530-5.4.9-1.6.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2019	x550-5.4.9-1.6.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	10/2019	x930-5.4.9-1.6.rel
x950-28XSQ x950-28XTQm	x950	10/2019	x950-5.4.9-1.6.rel
SBx908 GEN2	SBx908 GEN2	10/2019	SBx908NG-5.4.9-1.6.rel
SBx81CFC960	SBx8100	10/2019	SBx81CFC960-5.4.9-1.6.rel
AR4050S AR3050S	AR-series UTM firewalls	10/2019	AR4050S-5.4.9-1.6.rel AR3050S-5.4.9-1.6.rel
AR2050V AR2010V AR1050V	AR-series VPN firewalls	10/2019	AR2050V-5.4.9-1.6.rel AR2010V-5.4.9-1.6.rel AR1050V-5.4.9-1.6.rel
AMF Cloud		10/2019	vaa-5.4.9-1.6.iso (VAA OS) vaa-5.4.9-1.6.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-1.6.vhd (for Microsoft Azure)

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

Please note, the 5.4.9-1.6 software version is ISSU incompatible with software version 5.4.9-1.5.

New Features and Enhancements

This AlliedWare Plus maintenance version includes the following enhancement:

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x98Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
ER-3029	DHCP Relay	<p>With this software update DHCP snooping, VLAN stacking, and VLAN translation can now be supported on the same switchport. A new global configuration command:</p> <p>service dhcp-snooping per-vlan is implemented for this purpose.</p> <p>By default, when DHCP snooping is enabled without the per-vlan option, all DHCP packets are sent to the CPU for software processing. This conserves hardware ACL filter table space, and is appropriate and should continue to be used for most situations where DHCP snooping is required.</p> <p>You can use this new global configuration command instead to ensure DHCP snooped packets are selectively processed by CPU on a per-vlan basis. The result is DHCP traffic associated with VLANs that don't have DHCP snooping enabled is HW switched as normal, without being sent to the CPU for software processing unnecessarily.</p> <p>This can be useful where there is a need for DHCP traffic associated with selective VLANs to be processed by the CPU (for example, for insertion of DHCP snooping option-82 information for security purposes), whilst simultaneously allowing unrelated DHCP traffic associated with other VLANs to be hardware switched.</p> <p>This also means that DHCP packets received on switchports configured for VLAN translation/double-tagging can be hardware switched instead of being sent to the CPU when DHCP-snooping is enabled.</p>	-	-	Y	-	-	-	-	Y	Y	-	-	Y	Y	Y	-	-	Y	Y	-	Y	-	-	-	-	-	-

What's New in Version 5.4.9-1.5

Product families supported by this version:

AR4050S	x220 Series
AR3050S	x230 Series
AR2050V	x230L Series
AR2010V	x310 Series
AR1050V	IX5-28GPX
FS980M Series	x510 Series
GS900MX/MPX Series	x510L Series
GS970M Series	x530 Series
GS980M Series	x530L Series
GS980MX Series	x550 Series
XS900MX Series	x930 Series
IE200 Series	x950 Series
IE210L Series	SwitchBlade x908 Generation 2
IE300 Series	SwitchBlade x8100: SBx81CFC960
IE510-28GSX Series	AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-1.5.

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.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 60](#).

For instructions on how to update the web-based GUI, see [“Installing and Accessing the Web-based Device GUI” on page 62](#). The GUI offers easy visual monitoring and configuration of your device.



Caution: Software version 5.4.9-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 versions. 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 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58](#).



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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	10/2019	FS980-5.4.9-1.5.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	10/2019	GS900-5.4.9-1.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2019	GS970-5.4.9-1.5.rel
GS980M/52 GS980M/52PS	GS980M/MX	10/2019	GS980M-5.4.9-1.5.rel
XS916MXT XS916MXS	XS900MX	10/2019	XS900-5.4.9-1.5.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	10/2019	IE200-5.4.9-1.5.rel
IE300-12GT IE300-12GP	IE300	10/2019	IE300-5.4.9-1.5.rel
IE210L-10GP IE210L-18GP	IE210L	10/2019	IE210-5.4.9-1.5.rel
IE510-28GSX	IE510-28GSX	10/2019	IE510-5.4.9-1.5.rel
x220-28GS x220-52GT x220-52GP	x220	10/2019	x220-5.4.9-1.5.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2019	x230-5.4.9-1.5.rel

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

Models	Family	Date	Software File
x310-26FT x310-50FT x310-26FP x310-50FP	x310	10/2019	x310-5.4.9-1.5.rel
IX5-28GPX	IX5	10/2019	IX5-5.4.9-1.5.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	10/2019	x510-5.4.9-1.5.rel
x530-28GTXm x530-28GPXm x530L-52GPX	x530 and x530L	10/2019	x530-5.4.9-1.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2019	x550-5.4.9-1.5.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	10/2019	x930-5.4.9-1.5.rel
x950-28XSQ x950-28XTQm	x950	10/2019	x950-5.4.9-1.5.rel
SBx908 GEN2	SBx908 GEN2	10/2019	SBx908NG-5.4.9-1.5.rel
SBx81CFC960	SBx8100	10/2019	SBx81CFC960-5.4.9-1.5.rel
AR4050S AR3050S	AR-series UTM firewalls	10/2019	AR4050S-5.4.9-1.5.rel AR3050S-5.4.9-1.5.rel
AR2050V AR2010V AR1050V	AR-series VPN firewalls	10/2019	AR2050V-5.4.9-1.5.rel AR2010V-5.4.9-1.5.rel AR1050V-5.4.9-1.5.rel
AMF Cloud		10/2019	vaa-5.4.9-1.5.iso (VAA OS) vaa-5.4.9-1.5.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-1.5.vhd (for Microsoft Azure)

Issues Resolved in Version 5.4.9-1.5

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-65565	AMF	With this software update, the following deprecated ATMF application-proxy commands have been replaced: <ul style="list-style-type: none"> ■ show atmf ip-blocking was replaced with the command: show application-proxy threat-protection (all) ■ clear atmf application-proxy MAC and clear atmf application-proxy A.B.C.D were replaced with the command: clear application-proxy threat-protection (A.B.C.D MAC all) 	Y	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-65726	ICMP	Previously, if more than 32 ICMP based linkmon probes were configured with the same source address, some of the probes might continuously fail or fluctuate between failing and succeeding. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	
CR-65304	IGMP	Previously, in rare circumstances, it was possible for the device to fail to send or forward IGMP packets. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
CR-65178	L3 Multicast VCStack	Previously, a stack with VRF multicast could restart unexpectedly when the command clear ip mroute * was issued. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	Y	Y	Y	-	-	-	-	-	
CR-65611	Storm Control	Previously, when setting QoS storm-control on a switch with more than 24 ports, the settings would not be applied. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	-	Y	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-
CR-65703	Storm Control	Previously, the command vlandisable storm action was not working correctly. This issue has been resolved.	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-65743	Unicast Forwarding	Previously, on networks where many unicast destination lookup failures occurred, the unicast packets would be sent to the CPU and impact CPU performance. This issue has been resolved. With this software update, these packets will no longer go to CPU.	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-
CR-65350	VCStack	Previously, some VCS CLI commands and web APIs could fail on a SBx8100 CFC960 switch that had LIFs present. This could be seen in the log with the following log: <i>"CMMSG(45).tport.nsm.util/tmp/nsm_util: Failed to connect to remote host. Error:No such file or directory"</i> . This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-

What's New in Version 5.4.9-1.4

Product families supported by this version:

AR4050S	x220 Series
AR3050S	x230 Series
AR2050V	x230L Series
AR2010V	x310 Series
AR1050V	IX5-28GPX
FS980M Series	x510 Series
GS900MX/MPX Series	x510L Series
GS970M Series	x530 Series
GS980M Series	x530L Series
GS980MX Series	x550 Series
XS900MX Series	x930 Series
IE200 Series	x950 Series
IE210L Series	SwitchBlade x908 Generation 2
IE300 Series	SwitchBlade x8100: SBx81CFC960
IE510-28GSX Series	AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-1.4.

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.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 60](#).

For instructions on how to update the web-based GUI, see [“Installing and Accessing the Web-based Device GUI” on page 62](#). The GUI offers easy visual monitoring and configuration of your device.



Caution: Software version 5.4.9-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 versions. 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 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58](#).



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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	09/2019	FS980-5.4.9-1.4.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	09/2019	GS900-5.4.9-1.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	09/2019	GS970-5.4.9-1.4.rel
GS980M/52 GS980M/52PS	GS980M/MX	09/2019	GS980M-5.4.9-1.4.rel
XS916MXT XS916MXS	XS900MX	09/2019	XS900-5.4.9-1.4.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	09/2019	IE200-5.4.9-1.4.rel
IE300-12GT IE300-12GP	IE300	09/2019	IE300-5.4.9-1.4.rel
IE210L-10GP IE210L-18GP	IE210L	09/2019	IE210-5.4.9-1.4.rel
IE510-28GSX	IE510-28GSX	09/2019	IE510-5.4.9-1.4.rel
x220-28GS x220-52GT x220-52GP	x220	09/2019	x220-5.4.9-1.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	09/2019	x230-5.4.9-1.4.rel

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

Models	Family	Date	Software File
x310-26FT x310-50FT x310-26FP x310-50FP	x310	09/2019	x310-5.4.9-1.4.rel
IX5-28GPX	IX5	09/2019	IX5-5.4.9-1.4.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	09/2019	x510-5.4.9-1.4.rel
x530-28GTXm x530-28GPXm x530L-52GPX	x530 and x530L	09/2019	x530-5.4.9-1.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	09/2019	x550-5.4.9-1.4.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	09/2019	x930-5.4.9-1.4.rel
x950-28XSQ x950-28XTQm	x950	09/2019	x950-5.4.9-1.4.rel
SBx908 GEN2	SBx908 GEN2	09/2019	SBx908NG-5.4.9-1.4.rel
SBx81CFC960	SBx8100	09/2019	SBx81CFC960-5.4.9-1.4.rel
AR4050S AR3050S	AR-series UTM firewalls	09/2019	AR4050S-5.4.9-1.4.rel AR3050S-5.4.9-1.4.rel
AR2050V AR2010V AR1050V	AR-series VPN firewalls	09/2019	AR2050V-5.4.9-1.4.rel AR2010V-5.4.9-1.4.rel AR1050V-5.4.9-1.4.rel
AMF Cloud		09/2019	vaa-5.4.9-1.4.iso (VAA OS) vaa-5.4.9-1.4.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-1.4.vhd (for Microsoft Azure)

Issues Resolved in Version 5.4.9-1.4

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-65199	AMF Tunnelling	Previously, if an AMF virtual link configuration command specified a local interface that did not currently exist, the command would fail. However, this did not allow for some cases involving dynamic interfaces such as tunnels. This issue has been resolved, now, if the interface does not exist a warning message will be sent to the log. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	
CR-64706	DHCP Server	Previously, it was possible when entering the commands: show ip dhcp binding and show ip dhcp pool . that multiple DHCP pools for the clients were not shown. 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-65215	HW QoS Hotswap	Previously, if the CPU transmit rate limit was changed to a non-default rate, a hotswap of a XEM could set the rate back to default. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	-	-	-	-	-
CR-65293	Logging VCStack	Previously, it was possible for audit inconsistencies to occur on a stack if all port members of an aggregator were shut down in the stack, where the ports were spread over multiple stack nodes. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	Y	Y	Y	-	-	-	Y	-	-	Y	Y	Y	-	Y	Y	Y	Y	-	Y	-	-	-	-	-
CR-65321	Pluggable Transceivers	Previously, it was possible for a SFP detection to fail at bootup. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	-	-	-	-	-
CR-64986	Switching	Previously, on an x530 variant switch, the stack ports would not come up when Jumbo frames were enabled. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS900M/MPX	XS900MX	GS980M/MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-65172	System Web API	<p>Previously, leaving the device GUI dashboard open could cause the device to leak a small amount of memory each time the interface information was fetched.</p> <p>Previously, displaying the route table via the device GUI or the CLI could leak a small amount of memory.</p> <p>These issues have been resolved.</p> <p>ISSU: Effective when CFCs upgraded.</p>	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-65173	Web API	<p>Previously, using the device GUI with firewall enabled could cause a small amount of memory to leak each time that the firewall connections history was fetched.</p> <p>This issue has been resolved.</p>	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-

What's New in Version 5.4.9-1.3

Product families supported by this version:

AR4050S	x220 Series
AR3050S	x230 Series
AR2050V	x230L Series
AR2010V	x310 Series
AR1050V	IX5-28GPX
FS980M Series	x510 Series
GS900MX/MPX Series	x510L Series
GS970M Series	x530 Series
GS980M Series	x530L Series
GS980MX Series	x550 Series
XS900MX Series	x930 Series
IE200 Series	x950 Series
IE210L Series	SwitchBlade x908 Generation 2
IE300 Series	SwitchBlade x8100: SBx81CFC960
IE510-28GSX	AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-1.3.

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.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 60](#).

For instructions on how to update the web-based GUI, see [“Installing and Accessing the Web-based Device GUI” on page 62](#). The GUI offers easy visual monitoring and configuration of your device.



Caution: Software version 5.4.9-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 versions. 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 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58](#).



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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	09/2019	FS980-5.4.9-1.3.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	09/2019	GS900-5.4.9-1.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	09/2019	GS970-5.4.9-1.3.rel
GS980M/52 GS980M/52PS	GS980M/MX	09/2019	GS980M-5.4.9-1.3.rel
XS916MXT XS916MXS	XS900MX	09/2019	XS900-5.4.9-1.3.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	09/2019	IE200-5.4.9-1.3.rel
IE300-12GT IE300-12GP	IE300	09/2019	IE300-5.4.9-1.3.rel
IE210L-10GP IE210L-18GP	IE210L	09/2019	IE210-5.4.9-1.3.rel
IE510-28GSX	IE510-28GSX	09/2019	IE510-5.4.9-1.3.rel
x220-28GS x220-52GT x220-52GP	x220	09/2019	x220-5.4.9-1.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	09/2019	x230-5.4.9-1.3.rel

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

Models	Family	Date	Software File
x310-26FT x310-50FT x310-26FP x310-50FP	x310	09/2019	x310-5.4.9-1.3.rel
IX5-28GPX	IX5	09/2019	IX5-5.4.9-1.3.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	09/2019	x510-5.4.9-1.3.rel
x530-28GTXm x530-28GPXm x530L-52GPX	x530 and x530L	09/2019	x530-5.4.9-1.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	09/2019	x550-5.4.9-1.3.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	09/2019	x930-5.4.9-1.3.rel
x950-28XSQ x950-28XTQm	x950	09/2019	x950-5.4.9-1.3.rel
SBx908 GEN2	SBx908 GEN2	09/2019	SBx908NG-5.4.9-1.3.rel
SBx81CFC960	SBx8100	09/2019	SBx81CFC960-5.4.9-1.3.rel
AR4050S AR3050S	AR-series UTM firewalls	09/2019	AR4050S-5.4.9-1.3.rel AR3050S-5.4.9-1.3.rel
AR2050V AR2010V AR1050V	AR-series VPN firewalls	09/2019	AR2050V-5.4.9-1.3.rel AR2010V-5.4.9-1.3.rel AR1050V-5.4.9-1.3.rel
AMF Cloud		09/2019	vaa-5.4.9-1.3.iso (VAA OS) vaa-5.4.9-1.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-1.3.vhd (for Microsoft Azure)

New Features and Enhancements

This AlliedWare Plus maintenance version includes the following enhancements:

CR	Module	Description	FS980M	GS900MX/MPX	GS970M	GS980M	GS980MX	XS900MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, x510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud			
ER-2970	SD-WAN Triggers	<p>Previously, linkmon probe down triggers would not have activated at startup if the underlying source or egress-interface was down or when the probe was enabled and failed.</p> <p>This was because the probe was considered to be always down from initialization and therefore no state change had occurred to warrant a trigger activation.</p> <p>With this software update, the linkmon probe down triggers will activate after startup if the linkmon probe was down due to an underlying source or egress-interface being down or if the probe has no successful replies.</p> <p>Linkmon group members that do not have a probe will no longer cause the whole group to ignore the profile and rely on underlying link status.</p> <p>Instead, linkmon group members without a probe will be considered to be in an unknown state and cannot be used until a probe is configured. The other members of the group can be used as normal and abide by profile metric thresholds.</p>	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ER-889	Device Security	<p>This software update is to address the security issues described in "RFC7465 - Prohibiting RC4 Cipher Suites".</p> <p>The RFC requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections.</p> <p>This applies to all TLS versions. With this software update, an AlliedWare Plus device no longer uses the "RC4 cipher suite" by default for SSL.</p> <p>SSU: Effective when CFCs upgraded.</p>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
ER-3031	L3 Multicast	With this software update, a stack XS900 series switch will now allow L3 multicast traffic to pass without causing instability.	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Issues Resolved in Version 5.4.9-1.3

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

CR	Module	Description	FS980M	GS900MX/MPX	GS970M	GS980M	GS980MX	XS900MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-63626	AMF	Previously, it was possible for a switch to stop learning new MAC addresses after app proxy or clear mac address-table dynamic commands were used. This issue has been resolved.	-	-	-	-	-	Y	-	-	-	-	-	Y	-	-	Y	-	-	Y	-	-	-	-	-	-	-	-	-
CR-63942	CLI VCStack	Previously, under rare circumstances, it was possible for the command prompt to stop functioning after a stack failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	-	Y	Y	Y	-	-	-	Y	-	-	-	Y	Y	Y	-	Y	Y	Y	Y	-	-	-	-	-	-
CR-60591	EPSR	Previously, there was a potential delay processing the link down event upon topology changes on an EPSR ring, resulting in slower EPSR convergence. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	-	-	-	-	-	-
CR-64326	Hardware health monitoring	Previously, it was possible for the I2C driver on a SBx908 GEN2 or a x950 series switch to incorrectly manage communication with some of the sensor chips on the device when the CPU was under heavy load. This could result in spurious temperature sensor alarms and temperature sensor thresholds being changed in the chip. This issue has been resolved. ISSU: Effective when ISSU complete.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	-	-	-	-	-	-
CR-60405	Hotswap VCStack	Previously, a hotswap insertion quickly followed by a hotswap removal could potentially cause the XEM to be not initialised correctly. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-

CR	Module	Description	FS980M	GS900MX/MPX	GS970M	GS980M	GS980MX	XS900MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud		
CR-60253	HTTP Service	Previously, when a device 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	Y	Y	Y	Y	Y	Y	-
CR-64442	HTTP Device Security	Previously, the HTTP server on a router could allow the client to specify any ciphers that were implemented by openssl. With this software update, it only allows a reduced and more secure list for security improvement.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	-	
CR-64883	HW QoS	Previously, when egress rate-limiting was configured on a port, packets were being dropped unexpectedly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	Y	-	-	-	-	-	-	-	-
CR-61475	IDS/IPS	Previously, when using IPS or URL Filtering with NAT on routers with smaller amounts of RAM (AR2050V, AR2010V and AR1050) with very high volumes of HTTP traffic, it was possible for a low memory reboot to occur due to the amount of memory used by the Suricata application. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-	-	-	
CR-64264	IGMP OpenFlow	Previously, unresolved IGMP control packets would cause flooding on OpenFlow ports. This issue has been resolved.	-	Y	Y	Y	Y	Y	-	Y	Y	Y	-	Y	Y	Y	Y	-	-	Y	Y	-	Y	-	-	-	-	-	-	-
CR-64112	IGMP VRF-lite	Previously, disabling multicast routing would cause error logs if IGMP proxy service was still enabled. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	Y	Y	Y	-	Y	Y	Y	Y	-	

CR	Module	Description	FS980M	GS900MX/MPX	GS970M	GS980M	GS980MX	XS900MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud		
CR-65172	System	Previously, leaving the device GUI dashboard open could cause the device to leak a small amount of memory each time the interface information was fetched. Previously, displaying the route table via the device GUI or the CLI could leak a small amount of memory. These issues have been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-
CR-64138	Pluggable Transceivers VCStack	Previously, it was possible for an SFP+ port to stay linkup on a link even though the link went down due to a device restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	Y	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	-	-	-	-
CR-64262	PoE	Previously, the HANP timestamp for a port did not display correctly. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-
CR-51367	Port Authentication	Previously, after two supplicants were authenticated via WEB-AUTH and SSL on an x930 variant switch, it was possible for the switch to restart. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-
CR-64458	RADIUS	Previously, when attempting to change the password of an existing RADIUS user that was originally configured without a group on a switch, the switch might restart unexpectedly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	-
CR-64448	SD-WAN	Previously, when a linkmon profile was configured with consecutive probe loss as the preferred metric, the output of the show PBR rule command might print a blank line or nonsensical string. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-
CR-64544	SD-WAN	Previously, the "linkmon probe source" was incorrectly being indicated as an invalid interface when it actually was valid. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	

CR	Module	Description	FS980M	GS900MX/MPX	GS970M	GS980M	GS980MX	XS900MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-64817	SD-WAN Triggers	Previously, if an interface was down at startup that was associated with a linkmon probe source or egress interface, then a down trigger for that linkmon probe would not have run. This issue has been resolved, now the down trigger is run after startup once the probe detects the interface is down and considers itself to be invalid. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-
CR-65006	SD-WAN Triggers	Previously, if a linkmon probe was disabled but its underlying source or egress interface was invalid at startup, then it would activate associated unreachable triggers. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	-
CR-62372	VCStack	Previously, members of SBx908 GEN 2 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-63522	VCStack	Previously, if the VCS API or VCS commands (e.g. show stack) were used while a node was joining the stack, it was possible for the stack formation to fail and duplicate master event to occur. 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	-	-	-	-
CR-63936	VCStack	Previously, it was possible for the links on a x530 or x530L series switch to flap after a stack failover. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-
CR-64954	VCStack	Previously, under rare circumstances, it was possible for a SBx8100CFC960 switch to restart abnormally during stack failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-

CR	Module	Description	FS980M	GS900MX/MPX	GS970M	GS980M	GS980MX	XS900MX	IE200	IE210L	IE300	IE510	x220	x230, x230L	x310	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-64237	VRF-lite	<p>Previously, an incorrect source IP address was used in ICMP error packets when these packets were triggered by the VRF interface.</p> <p>This issue has been resolved.</p> <p>ISSU: Effective when ISSU complete.</p>	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	Y	Y	Y	Y	-	Y	Y	Y	-

What's New in Version 5.4.9-1.2

Product families supported by this version:

AR4050S	x220 Series
AR3050S	x230 Series
AR2050V	x230L Series
AR2010V	x310 Series
AR1050V	IX5-28GPX
FS980M Series	x510 Series
GS900MX/MPX Series	x510L Series
GS970M Series	x530 Series
GS980M Series	x530L Series
GS980MX Series	x550 Series
XS900MX Series	x930 Series
IE200 Series	x950 Series
IE210L Series	SwitchBlade x908 Generation 2
IE300 Series	SwitchBlade x8100: SBx81CFC960
IE510-28GSX Series	AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-1.2.

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.

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 60](#).

For instructions on how to update the web-based GUI, see [“Installing and Accessing the Web-based Device GUI” on page 62](#). The GUI offers easy visual monitoring and configuration of your device.



Caution: Software version 5.4.9-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 versions. 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 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58](#).



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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	08/2019	FS980-5.4.9-1.2.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2019	GS900-5.4.9-1.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2019	GS970-5.4.9-1.2.rel
GS980M/52 GS980M/52PS	GS980M/MX	08/2019	GS980M-5.4.9-1.2.rel
XS916MXT XS916MXS	XS900MX	08/2019	XS900-5.4.9-1.2.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2019	IE200-5.4.9-1.2.rel
IE300-12GT IE300-12GP	IE300	08/2019	IE300-5.4.9-1.2.rel
IE210L-10GP IE210L-18GP	IE210L	08/2019	IE210-5.4.9-1.2.rel
IE510-28GSX	IE510-28GSX	08/2019	IE510-5.4.9-1.2.rel
x220-28GS x220-52GT x220-52GP	x220	08/2019	x220-5.4.9-1.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2019	x230-5.4.9-1.2.rel

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

Models	Family	Date	Software File
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2019	x310-5.4.9-1.2.rel
IX5-28GPX	IX5	08/2019	IX5-5.4.9-1.2.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	08/2019	x510-5.4.9-1.2.rel
x530-28GTXm x530-28GPXm x530L-52GPX	x530	08/2019	x530-5.4.9-1.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2019	x550-5.4.9-1.2.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2019	x930-5.4.9-1.2.rel
x950-28XSQ x950-28XTQm	x950	08/2019	x950-5.4.9-1.2.rel
SBx908 GEN2	SBx908 GEN2	08/2019	SBx908NG-5.4.9-1.2.rel
SBx81CFC960	SBx8100	08/2019	SBx81CFC960-5.4.9-1.2.rel
AR4050S AR3050S	AR-series UTM firewalls	08/2019	AR4050S-5.4.9-1.2.rel AR3050S-5.4.9-1.2.rel
AR2050V AR2010V AR1050V	AR-series VPN firewalls	08/2019	AR2050V-5.4.9-1.2.rel AR2010V-5.4.9-1.2.rel AR1050V-5.4.9-1.2.rel
AMF Cloud		08/2019	vaa-5.4.9-1.2.iso (VAA OS) vaa-5.4.9-1.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-1.2.vhd (for Microsoft Azure)

Issues Resolved in Version 5.4.9-1.2

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	FS980M	GS900MX/MPX	GS970M	GS980M	GS980MX	XS900MX	IE200	IE300	IE210L	IE510	x220	x230	x310	IX5	x510, 510L	x530	x550	x930	x950	SBx8100 CFC400	SBx8100 CFC960	x908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
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	-	-	-	-	-

What's New in Version 5.4.9-1.1

Product families supported by this version:

AR4050S	x220 Series
AR3050S	x230 Series
AR2050V	x230L Series
AR2010V	x310 Series
AR1050V	IX5-28GPX
FS980M Series	x510 Series
GS900MX/MPX Series	x510L Series
GS970M Series	x530 Series
GS980M Series	x530L Series
GS980MX Series	x550 Series
XS900MX Series	x930 Series
IE200 Series	x950 Series
IE210L Series	SwitchBlade x908 Generation 2
IE300 Series	SwitchBlade x8100: SBx81CFC960
IE510-28GSX Series	AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-1.1.

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

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 60](#).

For instructions on how to update the web-based GUI, see [“Installing and Accessing the Web-based Device GUI” on page 62](#). The GUI offers easy visual monitoring and configuration of your device.



Caution: Software version 5.4.9-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 license certificate before you upgrade.

If an SBx908 GEN2 or SBx8100 switch already has a version 5.4.9 license installed, that license also covers all later 5.4.9 versions. 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 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58](#).



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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	07/2019	FS980-5.4.9-1.1.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	07/2019	GS900-5.4.9-1.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2019	GS970-5.4.9-1.1.rel
GS980M/52 GS980M/52PS	GS980M/MX	07/2019	GS980M-5.4.9-1.1.rel
XS916MXT XS916MXS	XS900MX	07/2019	XS900-5.4.9-1.1.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2019	IE200-5.4.9-1.1.rel
IE300-12GT IE300-12GP	IE300	07/2019	IE300-5.4.9-1.1.rel
IE210L-10GP IE210L-18GP	IE210L	07/2019	IE210-5.4.9-1.1.rel
IE510-28GSX	IE510-28GSX	07/2019	IE510-5.4.9-1.1.rel
x220-28GS x220-52GT x220-52GP	x220	07/2019	x220-5.4.9-1.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2019	x230-5.4.9-1.1.rel

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

Models	Family	Date	Software File
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2019	x310-5.4.9-1.1.rel
IX5-28GPX	IX5	07/2019	IX5-5.4.9-1.1.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	07/2019	x510-5.4.9-1.1.rel
x530-28GTXm x530-28GPXm x530L-52GPX	x530	07/2019	x530-5.4.9-1.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2019	x550-5.4.9-1.1.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2019	x930-5.4.9-1.1.rel
x950-28XSQ x950-28XTQm	x950	07/2019	x950-5.4.9-1.1.rel
SBx908 GEN2	SBx908 GEN2	07/2019	SBx908NG-5.4.9-1.1.rel
SBx81CFC960	SBx8100	07/2019	SBx81CFC960-5.4.9-1.1.rel
AR4050S AR3050S	AR-series UTM firewalls	07/2019	AR4050S-5.4.9-1.1.rel AR3050S-5.4.9-1.1.rel
AR2050V AR2010V AR1050V	AR-series VPN firewalls	07/2019	AR2050V-5.4.9-1.1.rel AR2010V-5.4.9-1.1.rel AR1050V-5.4.9-1.1.rel
AMF Cloud		07/2019	vaa-5.4.9-1.1.iso (VAA OS) vaa-5.4.9-1.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.4.9-1.1.vhd (for Microsoft Azure)

New Products

Version 5.4.9-1.1 supports the following recently-released products.

x530L-52GPX

Stackable Intelligent PoE+ Layer 3 Switch

Supported since 5.4.9-0.1

The x530L-52GPX stackable Gigabit Layer 3 switch features 48 x 100M/1G PoE+ ports, and 4 x 10G uplinks.

Key features:

- VCStack supports stacking up to four units locally or over distance to support resilient networking
- Ethernet Protection Switched Ring (EPSRing™) and G.8032 ERPS support high-speed resilient ring-based networks
- Autonomous Management Framework (AMF) for network automation
- Power over Ethernet Plus (PoE+) supplies up to 30 Watts to connect and power endpoints such as PTZ security cameras, POS terminals, and wireless access points.
- Dual fixed power supplies provide a PoE+ power budget of 740 Watts
- Continuous PoE ensures endpoint uptime, even during a switch firmware upgrade.

For more information, see the datasheet at www.alliedtelesis.com/documents/datasheet-x530l-52gpx.

x950-28XTQm

Expandable 10G/40G Stackable Layer 3 Switches

Supported since 5.4.9-0.4

The x950-28XTQm expandable 10G/40G stackable Layer 3 switch features 24 x 1/2.5/5/10G copper ports, 4 x 40G/100G uplink ports, and 1 x expansion bay.

Key features:

- VCStack supports stacking up to four units locally or over distance for a resilient network core
- Ethernet Protection Switched Ring (EPSRing™) and G.8032 ERPS support high-speed resilient ring-based networks
- Autonomous Management Framework (AMF) for network automation
- Large switching and routing tables support multiple services and connected devices
- 2.5/5G connectivity enables high-speed wireless, or maximum downlink speed using legacy Cat5e/6/6A cabling
- Active Fiber Monitoring for secure fiber backbone connections
- Market-leading SDN with industry certified OpenFlow v1.3
- 1.92 Terabit switch fabric and 1,190Mpps throughput for seamless data transfer capability.

For more information, see the datasheet at www.alliedtelesis.com/documents/datasheet-x950-series.

AR1050V

Secure Virtual Private Network (VPN) Routers

Supported since 5.4.9-0.1

The AR1050V secure Virtual Private Network (VPN) router is a secure business gateway, combining integrated firewall and VPN functionality with routing and switching.

Key features:

- An Intrusion Detection and Prevention System (IDS/IPS) provides monitoring, analysis and logging of suspicious events that occur on a network
- URL filtering enables HTTP or HTTPS access to particular websites to be allowed (whitelist) or blocked (blacklist) with user-defined lists
- IPSec VPNs enable secure connections between offices
- Easy-start wizards for easy Internet and VPN connectivity
- Autonomous Management Framework™ (AMF) compatibility automates device back-up for plug-and-play recovery.

For more information, see the datasheet at www.alliedtelesis.com/documents/datasheet-ar1050v.

New Features and Enhancements

This section summarizes the new features in 5.4.9-1.1:

- "180-node master licenses for Autonomous Management Framework (AMF) on SBx908 GEN2 and x950 Series switches" on page 44
- "RMON on tunnels" on page 44
- "ISAKMP Profile/PSK based on policy name" on page 44
- "DPI statistics per entity" on page 45
- "Change in time format for Dynamic DNS update method status" on page 45
- "VLAN double-tagging and VLAN ID translation on the same port" on page 45
- "The OpenFlow protocol on x530 Series switches for AMF Sec" on page 46
- "Global ACLs on x530 Series switches" on page 46
- "Alarm monitoring on stacked IE510-28GSX switches" on page 46
- "Resiliency link for VCStack Plus on SBx81CFC960" on page 46
- "IPv4 /31 bit subnetting" on page 47
- "Use IP address of the upstream interface as DHCP-Relay Source IP address" on page 47
- "Topology changes and optimizing EPSR rings with large numbers of VLANs" on page 48
- "Allow ARP security to ignore link-local ARP probes on a per-port basis" on page 48

To see how to find full documentation about all features on your product, see ["Obtaining User Documentation"](#) on page 55.

180-node master licenses for Autonomous Management Framework (AMF) on SBx908 GEN2 and x950 Series switches

From 5.4.9-1.1 onwards, a new license is available for enabling the SBx908 GEN2 and x950 Series switches to act as an AMF master for up to 180 nodes.

Note that a 300-node license was already previously available for SBx908 GEN2.

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](#).

RMON on tunnels

Available on AR-series devices

From 5.4.9-1.1 onwards, you can now enable Remote Network Monitoring (RMON) over tunnel interfaces.

RMON allows for useful collection of statistics, packet capturing and the monitoring of variables and generation of alarms on a particular interface. This functionality is now extended to tunnel interfaces.

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

ISAKMP Profile/PSK based on policy name

Available on AR-series devices

From 5.4.9-1.1 onwards, you can now specify for the ISAKMP Profile/Pre-Shared Key to use the local policy name. This means you do not need to rely on anything that other endpoints send.

To do this, specify the new parameter **policy <policy-name>** in the commands **crypto isakmp key** and **crypto isakmp peer**. For tunnel interfaces the policy name is the name of the tunnel (e.g. tunnel1).

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

DPI statistics per entity

Available on AR-series devices

From 5.4.9-1.1 onwards, your device can now display Deep Packet Inspection (DPI) statistics per entity. You can see transmit and receive counters of traffic that is transmitted and received by devices for each entity.

DPI statistics per entity allows for more fine grained reporting of application traffic, whether it be down to a Zone, Network, or an individual Host, and the ability to distinguish between different applications in an individual Zone, Network or Host.

To enable detailed DPI statistics per entity, use the command:

```
awplus(config-dpi)# counters detailed
```

These counters will require system resources and should be configured when required. To disable them, use the command:

```
awplus(config-dpi)# no counters detailed
```

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

Change in time format for Dynamic DNS update method status

Available on AR-series devices

From 5.4.9-1.1 onwards, the format of the last update times has been changed in the output of the command **show ddns-update-method status**. These times are now displayed in a human-readable format, in local time instead of UTC. For example: Jul 17, 2019 08:53:47.

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

VLAN double-tagging and VLAN ID translation on the same port

Available on SBx908 GEN2, x950, x930, x510, x510L, IE510-28GSX, and IE300 Series switches.

Version 5.4.9-1.1 supports VLAN double-tagging, VLAN ID translation or both on ports that support tagged packets, including switch ports in trunk mode, static channel groups, and dynamic (LACP) channel groups. VLAN double-tagging is also known as stacked VLANs, nested VLANs or Q-in-Q.

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

The OpenFlow protocol on x530 Series switches for AMF Sec

From 5.4.9-1.1 onwards, x530 and x530L Series switches support OpenFlow using the Allied Telesis AMF Sec Controller (previously SES Controller).

For important information about their support, see the [Openflow Feature Overview and Configuration Guide](#).

Global ACLs on x530 Series switches

From 5.4.9-1.1 onwards, on x530 Series switches you can attach hardware ACLs directly to all switchports using the **access-group** command. For example, to permit traffic from 192.168.1.x, but discard from 192.168.x.x:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.1.0/24 any
awplus(config)# access-list 3001 deny ip 192.168.0.0/24 any
awplus(config)# access-group 3000
awplus(config)# access-group 3001
```

Alarm monitoring on stacked IE510-28GSX switches

From 5.4.9-1.1 onwards, it is possible to configure separate alarms on VCStack backup members, as well as on the VCStack master switch. Different stack members can now be wired to separate sensors and/or relay outputs and have separate alarm conditions assigned to them.

This functionality is disabled by default. For information about how to configure it, see the [Alarm Monitoring Feature Overview and Configuration Guide](#).

Resiliency link for VCStack Plus on SBx81CFC960

From 5.4.9-1.1 onwards, resiliency links are supported on VCStack Plus.

When using Long Distant Stacking with VCStack Plus, if all of the long distance stacking fiber links take the same physical path between remote sites (e.g. via a multi-core OFC), it is possible that all stacking links could be severed. This could result in a "split brain" scenario where both chassis think they are VCS master, which could result in severe network issues requiring manual intervention.

To prevent this, 5.4.9-1.1 adds support for Ethernet VCS Resiliency link with Disabled Master Monitoring on SBx8100 VCStack Plus.

A Layer 2 Out-Of-Band-Management (OOBM) network connection is required at each site to connect to the ethernet ports of both CFCs on each chassis.

The out-of-band Ethernet port (eth0) is configured as a resiliency port with the command:

```
awplus(config)# stack resiliencylink eth0
```

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

IPv4 /31 bit subnetting

Available on all AlliedWare Plus switch, firewall and router devices that support Layer 3 interfaces

Version 5.4.9-1.1 expands support for IPv4 /31 bit subnetting. /31 bit subnetting is used when peering to ISP equipment where there is a strong need to conserve IPv4 address space. IPv4 /31 bit subnetting conserves address space because there is no concept of IP subnet and IP broadcast addresses associated with a /31 subnet. A /31 bit IPv4 subnet requires only two IPv4 addresses, each of which is allocated to a host.

From 5.4.9-1.1 onwards, you can configure /31 subnets on non-PPP/tunnel Layer 3 interfaces, such as VLAN, Ethernet, and Bridge. Prior to 5.4.9-1.1, this was only supported on PPP interfaces on AR-series firewalls and routers.

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

Use IP address of the upstream interface as DHCP-Relay Source IP address

Available on all AlliedWare Plus switch, firewall and router devices that support DHCP relay. Also supported from version 5.4.9-0.7.

When using DHCP-Relay, in most cases, there are filters placed between the DHCP relay and the DHCP server, to only allow DHCP packets from the client subnet to the server and back.

Version 5.4.9-1.1 supports a new command that allows you to configure DHCP-Relay to use the client-side interface (that is the interface receiving the DHCP client packets) IP address as the source address of the relayed DHCP packets.

The new command is:

```
awplus(config)# ip dhcp-relay use-client-side-address
```

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

Topology changes and optimizing EPSR rings with large numbers of VLANs

Available on SBx908 GEN2, x950, x930, x550, IX5, x510, x310, x230, IE510, IE300, IE210L, GS900MX, GS970M and GS900MX/MPX Series switches

From 5.4.9-1.1 onwards, you can use the new **epsr flush-type** command to specify how EPSR flushes Layer 2 entries when a topology change occurs. It can be configured to flush all Layer 2 entries on its EPSR interfaces or only flush the Layer 2 entries on its EPSR data VLANs.

Interface flushing is quicker and less granular than flushing Layer 2 entries on EPSR data VLANs as flushing on a data VLAN can incur a high overhead, reducing EPSR responsiveness to ring topology changes.

To flush all entries on the EPSR interface (including non-EPSR data VLANs) the **flush-type** command must be explicitly configured on the EPSR ring, using the **interface** parameter. For example:

```
awplus(config-epsr)# epsr red flush-type interface
```

For information about this feature, see the [EPSR Feature Overview and Configuration Guide](#).

Allow ARP security to ignore link-local ARP probes on a per-port basis

Available on all AlliedWare Plus switches

From 5.4.9-1.1 onwards, you can use the new **arp security drop link-local-arps** command to allow ARP security to ignore link-local ARP probes on a per-port basis. This means IPv4 link-local ARPs will be dropped without causing an ARP security violation when received.

Hosts that implement RFC 3927 may automatically assign themselves link-local IPv4 addresses in the subnet 169.254.0.0/16, if they are configured to learn their IP addresses via DHCP but are unable to contact a DHCP server. In an attempt to avoid IP address collision with other devices on the local network, the host will broadcast ARP probes for its randomly selected link-local IP address.

By default, ARP security will treat these ARP probes as violations and carry out the configured violation action on the port they are received on. If the violation action is configured as link-down, this will result in the host being disconnected from the network which will interrupt any DHCP IP address discovery that was in progress.

The new command allows you to configure ARP Security to drop these ARP probes, and any other ARPs that contain link-local IP addresses, without raising a violation on the affected port.

You can use the **show arp security statistics detail** command to see the status of ARPs dropped.

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

Important Considerations Before Upgrading

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

It describes the following changes:

- [Known issue when changing the password on a local radius user](#)
- [Detection of PoE legacy devices is now disabled by default](#)
- [Change in handling of RADIUS session-timeout attribute of zero](#)

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

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

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

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

Known issue when changing the password on a local radius user

Applies to all AlliedWare Plus switches that support local RADIUS

A known issue exists in this software version when changing the password on a local radius user. If a user exists and their password is changed, the process that controls the device's configuration restarts, incorrectly. Some configuration may be lost.

To work around this issue, do not change the password; instead, delete the user and re-add them with the new password.

This issue will be addressed in the next 5.4.9-1.x maintenance version.

Detection of PoE legacy devices is now disabled by default

Applies to all AlliedWare Plus PoE switches except FS980M Series

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

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

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

Change in handling of RADIUS session-timeout attribute of zero

Applies to all AlliedWare Plus devices

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

Software Release Licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.4.9 license on your switch if you are upgrading to 5.4.9-x.x on your SBx908 GEN2 or SBx8100 switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 56](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58.](#)

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

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

You cannot use ISSU to upgrade to 5.4.9-1.7 from any previous software version.

Upgrading a VCStack with reboot rolling

Applies to all stackable AlliedWare Plus switches

This version supports VCStack “reboot rolling” upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack. You can use the **reboot rolling** command to upgrade to 5.4.9-1.x from:

- 5.4.9-0.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 5.4.4-1.x

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

You cannot use rolling reboot to upgrade directly to 5.4.9-1.x from 5.4.4-0.x or earlier versions.

Forming or extending a VCStack with auto-synchronization

Applies to all stackable AlliedWare Plus switches

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up. Auto-synchronization is supported between 5.4.9-1.x and:

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

It is not supported between 5.4.9-1.x and 5.4.6-1.1 or **any** earlier releases.

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

If using an AMF controller

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

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

If using secure mode

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

If using Vista Manager EX

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

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

If using none of the above

If none of the above apply, then nodes running version 5.4.9-1.x are compatible with nodes running:

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

Upgrading all 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.

Changes to application list for the built-in deep packet inspection feature

Applies to AR4050S, AR3050S, AR2050V, AR2010V

The following applications have been **removed**:

- 1kxun
- AVI
- CiscoSkinny
- Citrix_Online -> under Citrix
- EPP
- Filetopia
- Flash
- GoogleHangout
- iQIYIMMSMove
- MPEG
- OggVorbis
- Quake
- QuickPlay
- QuickTime
- RealMedia
- SkyFile PostPaid
- SkyFile PrePaid
- SkyFile Rudics
- Socrates
- WebM
- WindowsMedia

The following applications have been **added**:

- AJP
- Amazon Video
- ApplePush
- Checkmk
- Diameter
- FBZero
- Generic
- GoogleDocs
- GooglePlus
- GoogleServices
- Hangout
- Memcached
- Messenger
- Mining
- Nest log sink
- NTOP
- Signal
- Skinny
- Skype call
- SMBv1
- SMBv23
- SomelP
- VidTO
- WhatsApp Files
- YouTube Upload

Obtaining User Documentation

For full AlliedWare Plus documentation, [click here to visit our online Resource Library](#).

For AlliedWare Plus products, the Library includes the following documents:

- **Feature Overview and Configuration Guides** - find these by searching for the feature name and then selecting Feature Guides in the right-hand menu.
- **Datasheets** - find these by searching for the product series and then selecting Datasheets in the right-hand menu.
- **Installation Guides** - find these by searching for the product series and then selecting Installation Guides in the right-hand menu.
- **Command References** - find these by searching for the product series and then selecting Manuals in the right-hand menu.

Verifying the Release File

On SBx908 GEN2, x950, x930, x550, x530, XS900MX, x220, and GS980M Series switches, to ensure that the release file has not been corrupted or interfered with during download, you can verify the release file. To do this, enter Global Configuration mode and use the command:

```
awplus(config)#crypto verify <filename> <hash-value>
```

where <hash-value> is the known correct checksum of the file.

This command compares the SHA256 checksum of the release file with the correct checksum for the file. The correct checksum is listed in the release's sha256sum file, which is available from the [Allied Telesis Download Center](#).

Caution



If the verification fails, the following error message will be generated:

“% Verification Failed”

In the case of verification failure, please delete the release file and contact Allied Telesis support.

All switch models of a particular series run the same release file and therefore have the same checksum. For example, all x930 Series switches have the same checksum.

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

Licensing this Version on an SBx908 GEN2 Switch

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a switch
- Obtain a release license for a switch
- Apply a release license on a switch
- Confirm release license application

1. Obtain the MAC address for a switch

A release license is tied to the MAC address of the switch.

Switches may have several MAC addresses. Use the **show system mac license** command to show the switch MAC address for release licensing:

```
awplus#show system mac license
MAC address for licensing:
eccd.6d9d.4eed
```

2. Obtain a release license for a switch

Contact your authorized Allied Telesis support center to obtain a release license.

3. Apply a release license on a switch

Use the **license certificate** command to apply a release license to your switch.

Note the license certificate file can be stored on internal flash memory, or an external SD card, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate 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   : 20-Mar-2019
Features included    : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                     EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                     L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                     RADIUS-100, RIP, VCStack, VRRP

Index                : 2
License name         : 5.4.9
Customer name        : ABC Consulting
Quantity of licenses : 1
Type of license      : Full
License issue date   : 20-Mar-2019
License expiry date  : N/A
Release              : 5.4.9
```

Licensing this Version on an SBx8100 Series CFC960 Control Card

Release licenses are applied with the **license certificate** command, then validated with the **show license** or **show license brief** commands. Follow these steps:

- Obtain the MAC address for a control card
- Obtain a release license for a control card
- Apply a release license on a control card
- Confirm release license application

If your CFC960 control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

1. Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license
MAC address for licensing:

Card                MAC Address
-----
1.5                 eccd.6d9e.3312
1.6                 eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

2. Obtain a release license for a control card

Contact your authorized Allied Telesis support center to obtain a release license.

3. Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

Entering a valid release license changes the console message displayed about licensing:

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate 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 chassis, use the commands **show license** or **show license brief** to confirm release license application.

On a stacked chassis, use the command **show license member** or **show license brief member** to confirm release license application.

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus#show license
OEM Territory : ATI USA
Software Licenses
-----
Index                : 1
License name         : Base License
Customer name        : ABC Consulting
Quantity of licenses : 1
Type of license      : Full
License issue date   : 20-Mar-2019
License expiry date  : N/A
Features included    : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                    : Virtual-MAC, VRRP

Index                : 2
License name         : 5.4.9
Customer name        : ABC Consulting
Quantity of licenses : -
Type of license      : Full
License issue date   : 20-Mar-2019
License expiry date  : N/A
Release              : 5.4.9
```

Installing this Software Version

Caution: Software version requires a release license for the SBx908 GEN2 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 56 and](#)
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 58.](#)

To install and enable this software version, use the following steps:

1. Copy the software version file (.rel) onto your TFTP server.
2. If necessary, delete or move files to create space in the switch’s Flash memory for the new file. To see the memory usage, use the command:

```
awplus# show file systems
```

To list files, use the command:

```
awplus# dir
```

To delete files, use the command:

```
awplus# del <filename>
```

You cannot delete the current boot file.

3. Copy the new release from your TFTP server onto the switch.

```
awplus# copy tftp flash
```

Follow the onscreen prompts to specify the server and file.

4. Move from Privileged Exec mode to Global Configuration mode, using:

```
awplus# configure terminal
```

Then set the switch to reboot with the new software version:

Product	Command
AR1050V	<code>awplus(config)# boot system AR1050V-5.4.9-1.7.rel</code>
AR2010V	<code>awplus(config)# boot system AR2010V-5.4.9-1.7.rel</code>
AR2050V	<code>awplus(config)# boot system AR2050V-5.4.9-1.7.rel</code>
AR3050S	<code>awplus(config)# boot system AR3050S-5.4.9-1.7.rel</code>
AR4050S	<code>awplus(config)# boot system AR4050S-5.4.9-1.7.rel</code>
FS980M series	<code>awplus(config)# boot system FS980-5.4.9-1.7.rel</code>
GS900MX/MPX series	<code>awplus(config)# boot system GS900-5.4.9-1.7.rel</code>
GS970M series	<code>awplus(config)# boot system GS970-5.4.9-1.7.rel</code>
GS980M/MX series	<code>awplus(config)# boot system GS980M-5.4.9-1.7.rel</code>
XS900MX series	<code>awplus(config)# boot system XS900-5.4.9-1.7.rel</code>
x220 series	<code>awplus(config)# boot system x220-5.4.9-1.7.rel</code>
x230 series	<code>awplus(config)# boot system x230-5.4.9-1.7.rel</code>

Product	Command
IE200 series	<code>awplus(config)# boot system IE200-5.4.9-1.7.rel</code>
IE210L series	<code>awplus(config)# boot system IE210-5.4.9-1.7.rel</code>
IE510L series	<code>awplus(config)# boot system IE510-5.4.9-1.7.rel</code>
x310 series	<code>awplus(config)# boot system x310-5.4.9-1.7.rel</code>
IE300 series	<code>awplus(config)# boot system IE300-5.4.9-1.7.rel</code>
IX5-28GPX	<code>awplus(config)# boot system IX5-5.4.9-1.7.rel</code>
x510 series	<code>awplus(config)# boot system x510-5.4.9-1.7.rel</code>
x530 series	<code>awplus(config)# boot system x530-5.4.9-1.7.rel</code>
IE510-28GSX	<code>awplus(config)# boot system IE510-5.4.9-1.7.rel</code>
x550 series	<code>awplus(config)# boot system x550-5.4.9-1.7.rel</code>
x930 series	<code>awplus(config)# boot system x930-5.4.9-1.7.rel</code>
x950 series	<code>awplus(config)# boot system x950-5.4.9-1.7.rel</code>
SBx908 GEN2	<code>awplus(config)# boot system SBx908NG-5.4.9-1.7.rel</code>
SBx8100 with CFC960	<code>awplus(config)# boot system SBx81CFC960-5.4.9-1.7.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
```

Installing and Accessing the Web-based Device GUI

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

The GUI is a convenient tool for monitoring your device's status and performing basic management tasks. Its dashboard provides at-a-glance monitoring of traffic and other key metrics.

On AR3050S and AR4050S firewalls, you can use the GUI to create an advanced application-aware firewall with features such as Application control and Web control. Alternatively, you can configure real-time threat protection with URL filtering, Intrusion Prevention and Malware protection.

On SBx908 GEN2 switches, x950 Series and most AR-Series devices, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

The steps for installing and accessing the GUI depend on whether the latest GUI has been pre-installed on your device in the factory, and if not, whether you are using a AR-Series device or a switch.

Check if the GUI is installed

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

Browse to the GUI

Perform the following steps to browse to the GUI.

Prerequisite on an AR-series device: If the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the “Configuring a Firewall Rule for Required External Services” section in the [Firewall and Network Address Translation \(NAT\) Feature Overview and Configuration Guide](#).

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

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

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

Device	Address
AR-Series	192.168.1.1
Switches	169.254.42.42

2. Open a web browser and browse to the IP address from step 1.
3. If you do not see a login page, you need to install the GUI, as described in “[Install the GUI if it is not installed](#)” on page 63. If you see a login page, log in. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the About page in the GUI and check the field called **GUI version**. The version to use with 5.4.9-1.1 is 2.4.0.

If you have an earlier version, update it as described in [“Update the GUI if it is not the latest version” on page 65](#).

Install the GUI if it is not installed

If you have an AR-series device and the GUI is not installed...

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

1. If the device’s firewall is enabled, create a firewall rule to permit traffic generated by the device that is destined for external services. See the “Configuring a Firewall Rule for Required External Services” section in the [Firewall and Network Address Translation \(NAT\) Feature Overview and Configuration Guide](#).
2. If you haven’t already, create one or more IP interfaces and assign them IP addresses, including configuring WAN connectivity. For information about configuring PPP, see the [PPP Feature Overview and Configuration Guide](#). For information about configuring IP, see the [IP Feature Overview and Configuration Guide](#).

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

```
awplus# update webgui now
```

4. Make sure the HTTP service is running:

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

5. Log into the GUI:

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

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

If you have a switch and the GUI is not installed...

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

1. Obtain the GUI file from our Software Download center. The file to use with 5.4.9-1.1 is `awplus-gui_549_13.gui`.

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

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

- « TFTP server
- « USB Flash drive
- « SD card

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

```
awplus>enable
awplus#copy usb awplus-gui_549_13.gui flash
```

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

```
awplus#dir
```

3. Delete any previous Java switch GUI files.

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

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

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

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

5. Make sure the HTTP service is running:

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

6. Log into the GUI:

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

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

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

Update the GUI if it is not the latest version

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

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

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

```
awplus# update webgui now
```

2. Stop and restart the HTTP service:

```
awplus# configure terminal
```

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

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

3. Log into the GUI:

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

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

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

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

1. Obtain the GUI file from our Software Download center. The file to use with 5.4.9-1.1 is `awplus-gui_549_13.gui`.

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

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

« TFTP server

« USB Flash drive

« SD card

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

```
awplus>enable
```

```
awplus#copy usb awplus-gui_549_13.gui flash
```

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

```
awplus#dir
```

3. Stop and restart the HTTP service:

```
awplus# configure terminal
```

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

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

4. Log into the GUI:

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

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

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