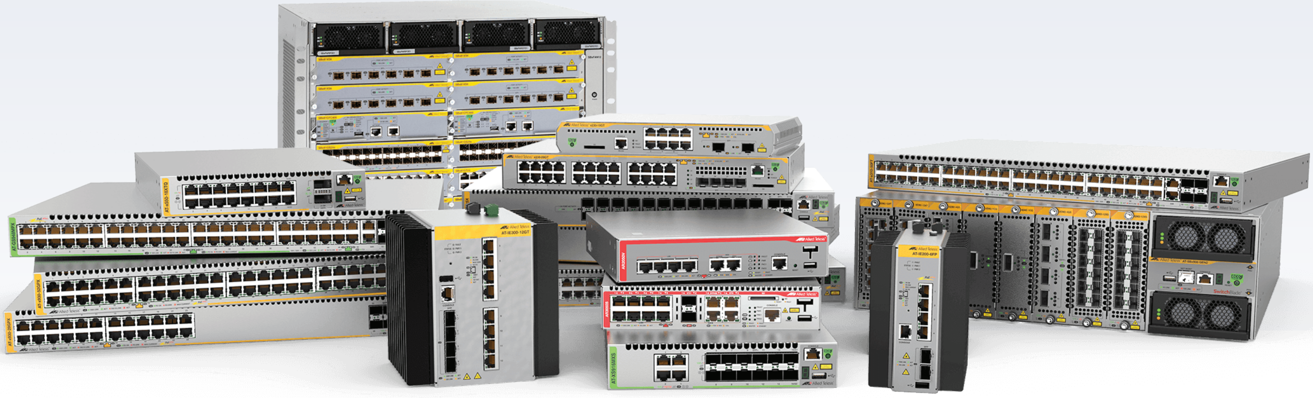
Allied Telesis™

# Release Note for AlliedWare Plus Software Version 5.4.9-2.x



**AlliedWare Plus**
**OPERATING SYSTEM**

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

» x550 Series » x530 Series » x510 Series » IX5 Series

» x320 Series » x310 Series » x230 Series » x220 Series » IE500 Series

» IE340 Series » IE300 Series » IE210L Series » IE200 Series

» XS900MX Series » GS980M Series » GS980EM Series » GS970M Series

» GS900MX/MPX Series » FS980M Series » AMF Cloud

» AR4050S » AR3050S » AR2050V » AR2010V » AR1050V

» 5.4.9-2.1 » 5.4.9-2.2 » 5.4.9-2.3 » 5.4.9-2.4 » 5.4.9-2.5 » 5.4.9-2.6 » 5.4.9-2.7

# Acknowledgments

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

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

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

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

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

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

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

## Getting the most from this Release Note

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

# Content

# What’s New in Version 5.4.9-2.7

Product families supported by this version:

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

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-2.7.

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

For instructions on how to upgrade to this version, see “Installing this Software Version” on page 94.

For instructions on how to update the web-based GUI, see “Installing and Accessing the Web-based GUI on AR-Series Devices” on page 99. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

| Models | Family | Date | Software File |
|---|---|---|---|
| AMF Cloud | | 09/2021 | vaa-5.4.9-2.7.iso (VAA OS)<br>vaa-5.4.9-2.7. vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.4.9-2.7.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 09/2021 | SBx81CFC960-5.4.9-2.7.rel |
| SBx908 GEN2 | SBx908 GEN2 | 09/2021 | SBx908NG-5.4.9-2.7.rel |
| x950-28XSQ<br>x950-28XTQm | x950 | 09/2021 | x950-5.4.9-2.7.rel |
| x930-28GTX<br>x930-28GPX<br>x930-52GTX<br>x930-52GPX<br>x930-28GSTX | x930 | 09/2021 | x930-5.4.9-2.7.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 09/2021 | x550-5.4.9-2.7.rel |
| x530-28GTXm<br>x530-28GPXm<br>x530L-52GPX | x530 and x530L | 02/2021 | x530-5.4.9-2.7.rel |
| x510-28GTX<br>x510-52GTX<br>x510-28GPX<br>x510-52GPX<br>x510-28GSX<br>x510-28GSX-80<br>x510DP-28GTX<br>x510DP-52GTX<br>x510L-28GT<br>x510L-28GP<br>x510L-52GT<br>x510L-52GP | x510 and x510L | 09/2021 | x510-5.4.9-2.7.rel |
| IX5-28GPX | IX5 | 09/2021 | IX5-5.4.9-2.7.rel |
| x320-10GH | x320 | 09/2021 | x320-5.4.9-2.7.rel |
| x310-26FT<br>x310-50FT<br>x310-26FP<br>x310-50FP | x310 | 09/2021 | x310-5.4.9-2.7.rel |
| x230-10GP<br>x230-10GT<br>x230-18GP<br>x230-18GT<br>x230-28GP<br>x230-28GT<br>x230L-17GT<br>x230L-26GT | x230 and x230L | 09/2021 | x230-5.4.9-2.7.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 09/2021 | x220-5.4.9-2.7.rel |
| IE510-28GSX | IE510-28GSX | 09/2021 | IE510-5.4.9-2.7.rel |
| IE340-20GP<br>IE340L-18GP | IE340 | 09/2021 | IE340-5.4.9-2.7.rel |
| IE300-12GT<br>IE300-12GP | IE300 | 09/2021 | IE300-5.4.9-2.7.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| IE210L-10GP<br>IE210L-18GP | IE210L | 09/2021 | IE210-5.4.9-2.7.rel |
| IE200-6FT<br>IE200-6FP<br>IE200-6GT<br>IE200-6GP | IE200 | 09/2021 | IE200-5.4.9-2.7.rel |
| XS916MXT<br>XS916MXS | XS900MX | 09/2021 | XS900-5.4.9-2.7.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 09/2021 | GS980M-5.4.9-2.7.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 09/2021 | GS980EM-5.4.9-2.7.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 09/2021 | GS970-5.4.9-2.7.rel |
| GS924MX<br>GS924MPX<br>GS948MX<br>GS948MPX | GS900MX/MPX | 09/2021 | GS900-5.4.9-2.7.rel |
| FS980M/9<br>FS980M/9PS<br>FS980M/18<br>FS980M/18PS<br>FS980M/28<br>FS980M/28PS<br>FS980M/52<br>FS980M/52PS<br>FS980M/28DP | FS980M | 09/2021 | FS980-5.4.9-2.7.rel |
| AR4050S<br>AR3050S | AR-series UTM firewalls | 09/2021 | AR4050S-5.4.9-2.7.rel<br>AR3050S-5.4.9-2.7.rel |
| AR2050V<br>AR2010V<br>AR1050V | AR-series VPN firewalls | 09/2021 | AR2050V-5.4.9-2.7.rel<br>AR2010V-5.4.9-2.7.rel<br>AR1050V-5.4.9-2.7.rel |

**Caution:** Software version 5.4.9-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 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 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

The 5.4.9-2.7 software version is ISSU compatible with 5.4.9-2.6.

# New Features and Enhancements

This section summarizes the enhancements in version 5.4.9-2.7

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | x330 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ER-4315** | **AMF** | This software version allows GS900 series switches to be replaced with either GS980M or x230-52 series switches using AMF automatic recovery. | – | – | – | – | Y | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **ER-3859** | **Multicast Forwarding**<br>**HW** | This software version provides a new multicast command: **ip igmp flood-group**<br>This command adds any source flooding entry into the switches multicast hardware table to flood multicast packets to all ports within the VLAN without mirroring the traffic to CPU. This significantly reduces the number of hardware entries consumed.<br>Configuration example:<br>To configure an IGMP flooding group to L2 ports only use the following commands..<br>`awplus(config)#`**`int vlan1`**<br>`awplus(config-if)#`**`ip igmp flood-group 239.255.255.250`**<br>This will flood any UDP packet to group 239.255.255.250 to all ports in vlan1 | – | – | – | – | Y | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – |

# Issues Resolved in Version 5.4.9-2.7

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

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-73387** | **802.1x** | Previously, unauthorizing supplicants could result in a memory leak.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-70236** | **AMF** | Previously, when a device connected via an AMF link, was moved from one upstream device to a different upstream device and both upstream devices had virtual uplinks, it was possible that Layer 3 communication might not resume for the device.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-71948** | **AMF** | Previously, after an AMF network topology change, it was possible in some situations for connectivity to some AMF nodes not to be restored.<br>This issue has been resolved, improvements have been made to the way AMF handles topology changes that involve changes to reachability between virtual and non-virtual links.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-72657** | **AMF** | Previously, removal of an AMF node could result in a bad entry in the AMF software table, causing disruption in an AMF network.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **CR-72841** | **AMF** | Previously, when a virtual AMF node was terminating one end of a virtual-link connecting to a physical AMF node, the link could fail to fully establish.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | Y | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-73984** | **AMF** | Previously, the log message '*received packet on xxx with own address as source address*' was generated at **info** log level.<br>The log message has been changed to **warning** level, to increase its visibility.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | Y | Y | – | – | Y | – | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | Y | Y | Y | Y | Y | Y | Y |
| **CR-71969** | **AWC-Lite** | This software update corrects the calculation method of BSSID for a Channel Blanket VAP. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | Y | Y | Y | – |
| **CR-72946** | **AWC-Lite** | Previously, a memory leak could occur when the **`administrative address`** command was entered.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-73261** | **AWC-Lite** | Previously, the **`no wireless`** command could cause a memory leak.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |
| **CR-73263** | **AWC-Lite** | Previously, the **`auto-config`** command could cause a memory leak.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |
| **CR-73264** | **AWC-Lite** | Previously, the **`show wireless auto-config`** command could cause a memory leak.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |
| **CR-73272** | **AWC-Lite** | Previously, the **`wireless download ap`** and **`wireless power-channel ap`** commands could cause a memory leak.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |
| **CR-73273** | **AWC-Lite** | Previously, the **`debug wireless`** and **`show debug wireless`** commands could cause a memory leak.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-73274** | **AWC-Lite** | With this software update, the following error log messages are added for different types of incorrect AP configuration:<br>""WDS SSID not found""<br>""VAP0 not found""<br>""Hwtype does not support CB""<br>""CB control VLAN not found""<br>""CB key not found""<br>""SC SSID not found""<br>""SC key not found""<br>""SC radio not found""<br>""SC channel not found""<br>""SC VAP not found""<br>""Passpoint security must be WPA Enterprise""" | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |
| **CR-73318** | **AWC-Lite** | Previously, incorrect log mesages were displayed with the following commands:<br>■ wireless power-channel ap"<br>■ wireless ap-configuration apply app"<br>■ wireless reset ap"<br>■ wireless download ap"<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |
| **CR-73328** | **AWC-Lite** | Previously, configuring the Channel Blanket eligible channel could cause a memory leak.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | – | Y | – | Y | Y | Y | – |
| **CR-70200** | **CLI** | Previously, the output displayed for the field 'Time since last change' for the command **`show interface`** could become abnormal if the system was up for over 497 days.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-72550** | **CLI**<br>**Tunnel** | Previously, recreating a tunnel interface immediately after it was deleted, could cause the device to restart unexpectedly.<br>This issue has been resolved. Now, when trying to create a tunnel interface immediately after it is deleted, the action is ejected with the following message:<br> "% IFNAME is currently being deleted, please try again". | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-70998** | **Device GUI, HTTP Service, Web API** | Previously, it was possible to download certain files from the device over HTTPS without authorization if the:<br>■ HTTP service was enabled<br>■ AlliedWare Plus Device GUI was not installed on the device.<br>This issue has been resolved. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | Y | Y | Y | Y | Y | Y | – |
| **CR-54492** | **DHCP Server** | This software update alters the DHCPv4 lease time calculation to avoid roll over errors on 64-bit OS systems when using -1(infinite) or large values for default DHCP lease time.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-68889** | **DHCP Server** | Previously, the commands **`show ip dhcp binding`** and **`show ip dhcp pools`** were unable to process DHCP bindings that included malformed HW addresses and would display"Malformed statement" instead.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-63798** | **Environmental Monitoring** | Previously, the temperature sensor on x950 series and x908 GEN2 could occasionally reported an abnormal condition.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-74358** | **IDS, IPS** | Previously, on devices with IPS enabled and "category http-events action deny" set, HTTP POST messages containing HTTP Multipart data (e.g. a form submission) might incorrectly be dropped.<br>If this occurred, then an info-level log message would be generated in the following form:<br>IPS[4455]: [Drop] IPS: http-events HTTP multipart generic error URL:http://...<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-72193** | **IPv4, IPv6** | Previously, if an IPv4 and IPv6 dual-stack enabled interface was brought down and then up, then IPv4 routing via the interface could fail.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-71830** | **IPv6, Multicast routing** | Previously, IPv6 static multicast would not work with an IPv6 PIM license.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | – | Y | Y | Y | Y | Y | Y | Y | – | Y | – | Y | Y | Y | – |
| **CR-72336** | **L2TP, VRF-Lite** | Previously, when a VRF interface was deleted, nexthop entries in other VRFs could still be left with the reference to that interface, resulting in traffic not being forwarded correctly.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | Y | Y | Y | – | Y | Y | Y | – |
| **CR-72606** | **System** | This software update addresses the security vulnerability as stated in CVE-2020-14305, preventing unauthenticated remote users to cause an unexpected reboot of the system on H323 over IPv6 connection tracking.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-71758** | **Logging, MAC Thrashing** | Previously, a "Thrash-limiting: Re-enabled learning" log message could be generated when one or more links on an aggregator went down, for instance when the link partner rebooted.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | Y | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-72144** | **Loop Protection**<br>**VCStack** | Previously, network ports were linking up before the configuration was applied.<br>This caused an internal system module on the different stacking nodes to go out of synchronisation, resulting in some CLI configuration failing to be executed.<br>This issue has been resolved. | – | – | – | – | Y | Y | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | – | – | – | – | – | – | – | – |
| **CR-70789** | **Multicast Routing** | Previously the error log "*No more free mll pairs*" could be generated frequently due to a slight mis-match between the software and hardware MLL table limit on some LIFs.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-71897** | **Multicasting Forwarding Hardware** | Previously, IP IGMP flooding groups were not forwarding the traffic correctly.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | – |
| **CR-73456** | **OpenFlow** | Previously, packets encapsulated with an 802.3 header (length instead of type) which were not using SNAP encapsulation could cause hardware flows to be added which would match all Ethernet types, thus adversely affecting OpenFlow switching.<br>This issue has been resolved. | – | Y | Y | Y | – | – | – | – | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | – | – | – | – | – |
| **CR-71828** | **PIM-SM**<br>**Tunnel** | Previously, if PIM-SM or IGMP was configured on a tunnel before it had a valid ifindex or address, the configured commands would fail, and it was not possible for the software to dynamically recover from this issue.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-72068** | **Pluggable Tranceivers** | Previously, PoE ports would not recover after the PoE ports was disabled after the voltage went below the minumum required value, even when the voltage returned to the stable state.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | Y | – | – | – | – | Y | – | – | – | – | – | – | – | – |
| **CR-70887** | **Pluggable Transceiver, VCStack** | Previously, the AlliedTelesis device could falsely report link events on a stack port when its link partner was still in the process of linking up, resulting in link flapping when stack ports were about to link up.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – |
| **CR-72440** | **Pluggable Transceivers** | Previously, pluggable ports sometimes would not linkup at startup due to configuration replay being run before the pluggables were configured.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | Y | – | – | – | – | Y | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-71115** | **PoE** | Previously, on IE300 and x320 series, some dual-signature PoE power devices would not draw the minimum DC current for a pair-set unless both pair-sets were powered up simultaneously, resulting in disconenction of the power devices.<br>This issue has been resolved with a new parameter added to the command:<br>**`power-inline disconnect-defer`**<br>&lt;disconnect-defer-timeout&gt;<br>This parameter causes the disconnect detection to be enabled 3 seconds after the default pair-set has been powered which gives the power devices enough time to draw power on both pair-sets. The disconnect detection timeout can also be configured longer than 3 seconds if requried.<br>The command "(no\|) **`power-inline disconnect-defer`**" defers the DC disconnect detection in hardware. It is disabled by default. Some 60W PDs take longer than the 802.3at standard time for drawing the mimimum DC current on an individual pair. By defering the enabling of the DC disconnect logic it allows both sets of pairs to power up and start drawing current.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-73123** | **PoE** | Previously, the SPF on x930 series switches was not reflecting the speed/duplex/medium-type settings correctly.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – |
| **CR-72948** | **PoE** | Previously, it was possible for some power-inline configuration to disappear from the running configuration when rebooting a stack-member.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | – | – | Y | – | – | – | – | – | – | – | Y | – | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-70785** | **Policy Based Routing (PBR)** | Previously when **`match tcp-flag`** was set in a class-map, any PBR nexthops within the same policy-map may not have been automatically resolved when matching traffic flows through the device.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-70923** | **Port Authentication** | Previously, application of a dynamic VLAN by port authentication would not work if that VLAN was preceded by a user named VLAN in the VLAN database.<br>This issue only occurred if the two VLANs had consecutive VIDs.<br>This issue has been resolved. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | Y | Y | – | – | – | – | – |
| **CR-72373** | **Port Authentication** | Previously, when using MAC authentication, after a supplicant was successfully authenticated, if the link went down and came up, the supplicant had a short window of time (less than 1 second) where traffic it transmitted could still be forwarded into the network prior to the authentication process starting, when this traffic should have been discarded.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | Y | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-73557** | **Port Authentication** | Previously, when dynamic VLANs were used in conjunction with MAC authentication, The MAC entry of the new supplicant could be incorrectly removed from the FDB table. The missing MAC may be detected by an auth audit and recovered along with a log message generated indicating the entry was missing.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-70388** | **Private VLAN MLD Snooping** | Previously an error message - for example: `"DBG:hsl_hw_impl_l2_add_fdb 1802: Could not add MC MAC. ifx 5002 3333.ff9d.e1cb vid 2"` could be generated when IPv6 multicast traffic was received on a member port of a private VLAN on which MLD snooping was enabled.<br>This issue has been resolved. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | – |
| **CR-70672** | **Routing** | Previously, if a connected route was down (for example due to the VLAN interface being shut down) and was replaced by a route from a routing protocol, then when the VLAN came back up the connected route could fail to be reinstated.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-71532** | **SMTP** | Previously, it was possible for the SMTP protocol to not process outgoing mail.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-73696** | **Switching** | Previously, configuring the command:<br>**Ingress-filter disable** on a switchport could cause traffic to unexpectedly be flooded to the configured port.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | – | Y | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-70914** | **System** | Previously, if an interface was configured with an IPv6 address derived from a prefix appended to the eui64 address of the interface, and the interface performed router advertisement for the same prefix, then the address would have decrementing lifetimes, and eventually the address would have lifetimes of zero.<br>As a result, the address would no longer be used for the interface, which caused the routing to cease on that interface.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-72108** | **System** | Previously, on rare occasions, the SBx908GEn2 and x950 variant switches could restart unexpectedly due to a logic error in the code in the handling of packets received by the switch.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | – | – | – | – |
| **CR-74221** | **System** | Previously, an internal error could occur in very rare cases that could deplete some of the switching system resources. Over time it was possible for this to eventually result in a VCStack separation.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-71715** | **Telnet** | Previously, the Telnet process could restart after receiving illegal Telnet packets.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-71468** | **Tunnel** | Previously, after changing the IP address on a tunnel, traffic was not being forwarded.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-72439** | **User Management** | This software update addresses a vulnerability as stated in CVE-2021-3156 where "sudo" may be exploited by local privileged users, resulting in heap-based buffer overflow.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | – |
| **CR-72369** | **VCStack** | Previously, if one of the stack members locked up, traffic from its ports could still cause learning events on the stack.<br>However, as this member was no longer part of the stack, learning was not the correct thing to do.<br>This issue has been resolved.. | – | Y | Y | Y | Y | – | Y | – | – | Y | Y | Y | – | – | Y | – | Y | Y | – | Y | Y | Y | – | Y | – | – | – | – | – |
| **CR-72470** | **VCStack** | Previously, configuration could be falsely detected as mismatched on a late-joining stack member.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – |
| **CR-72608** | **VCStack** | Previously, on rare occasions, a stack member might not join the stack correctly on a reboot or power cycle.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | – | – | Y | – | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | – | – |
| **CR-66144** | **VCStack** | Previously, when configuration commands were executed (either interactively or as part of an automated script) while a stack member was in the process of joining, the commands could fail to execute and take 5 minutes per command to timeout.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | – | – | Y | – | – | – | – | – | – | – | Y | – | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | – | – |
| **CR-68827** | **VLAN** | Previously, on x530 series and SBx8100 switches, If a VLAN classifier was applied on an interface, packets received matching that VLAN classifier on another interface could be incorrectly dropped.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | Y | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | GS980MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-70418** | **Web Control** | Previously, when using Web-Control or Antivirus in a high load network, it was possible for the proxy to not working properly.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – |

# What’s New in Version 5.4.9-2.6

Product families supported by this version:

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

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-2.6.

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

For instructions on how to upgrade to this version, see “Installing this Software Version” on page 94.

For instructions on how to update the web-based GUI, see “Installing and Accessing the Web-based GUI on AR-Series Devices” on page 99. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

| Models | Family | Date | Software File |
|---|---|---|---|
| AMF Cloud | | 02/2021 | vaa-5.4.9-2.6.iso (VAA OS)<br>vaa-5.4.9-2.6. vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.4.9-2.5.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 02/2021 | SBx81CFC960-5.4.9-2.6.rel |
| SBx908 GEN2 | SBx908 GEN2 | 02/2021 | SBx908NG-5.4.9-2.6.rel |
| x950-28XSQ<br>x950-28XTQm | x950 | 02/2021 | x950-5.4.9-2.6.rel |
| x930-28GTX<br>x930-28GPX<br>x930-52GTX<br>x930-52GPX<br>x930-28GSTX | x930 | 02/2021 | x930-5.4.9-2.6.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 02/2021 | x550-5.4.9-2.6.rel |
| x530-28GTXm<br>x530-28GPXm<br>x530L-52GPX | x530 and x530L | 02/2021 | x530-5.4.9-2.6.rel |
| x510-28GTX<br>x510-52GTX<br>x510-28GPX<br>x510-52GPX<br>x510-28GSX<br>x510-28GSX-80<br>x510DP-28GTX<br>x510DP-52GTX<br>x510L-28GT<br>x510L-28GP<br>x510L-52GT<br>x510L-52GP | x510 and x510L | 02/2021 | x510-5.4.9-2.6.rel |
| IX5-28GPX | IX5 | 02/2021 | IX5-5.4.9-2.6.rel |
| x320-10GH | x320 | 02/2021 | x320-5.4.9-2.6.rel |
| x310-26FT<br>x310-50FT<br>x310-26FP<br>x310-50FP | x310 | 02/2021 | x310-5.4.9-2.6.rel |
| x230-10GP<br>x230-10GT<br>x230-18GP<br>x230-18GT<br>x230-28GP<br>x230-28GT<br>x230L-17GT<br>x230L-26GT | x230 and x230L | 02/2021 | x230-5.4.9-2.6.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 02/2021 | x220-5.4.9-2.6.rel |
| IE510-28GSX | IE510-28GSX | 02/2021 | IE510-5.4.9-2.6.rel |
| IE340-20GP<br>IE340L-18GP | IE340 | 02/2021 | IE340-5.4.9-2.6.rel |
| IE300-12GT<br>IE300-12GP | IE300 | 02/2021 | IE300-5.4.9-2.6.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| IE210L-10GP<br>IE210L-18GP | IE210L | 02/2021 | IE210-5.4.9-2.6.rel |
| IE200-6FT<br>IE200-6FP<br>IE200-6GT<br>IE200-6GP | IE200 | 02/2021 | IE200-5.4.9-2.6.rel |
| XS916MXT<br>XS916MXS | XS900MX | 02/2021 | XS900-5.4.9-2.6.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 02/2021 | GS980M-5.4.9-2.6.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 02/2021 | GS980EM-5.4.9-2.6.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 02/2021 | GS970-5.4.9-2.6.rel |
| GS924MX<br>GS924MPX<br>GS948MX<br>GS948MPX | GS900MX/MPX | 02/2021 | GS900-5.4.9-2.6.rel |
| FS980M/9<br>FS980M/9PS<br>FS980M/18<br>FS980M/18PS<br>FS980M/28<br>FS980M/28PS<br>FS980M/52<br>FS980M/52PS<br>FS980M/28DP | FS980M | 02/2021 | FS980-5.4.9-2.6.rel |
| AR4050S<br>AR3050S | AR-series UTM firewalls | 02/2021 | AR4050S-5.4.9-2.6.rel<br>AR3050S-5.4.9-2.6.rel |
| AR2050V<br>AR2010V<br>AR1050V | AR-series VPN firewalls | 02/2021 | AR2050V-5.4.9-2.6.rel<br>AR2010V-5.4.9-2.6.rel<br>AR1050V-5.4.9-2.6.rel |

**Caution:** Software version 5.4.9-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 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 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

The 5.4.9-2.6 software version is ISSU compatible with 5.4.9-2.5.

# Issues Resolved in Version 5.4.9-2.6

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

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68760** | **802.1x** | Previously, the force-authorization option for port AUTH was failing if the port was configured for dot1x and eapol v2.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | – |
| **CR-67953** | **Aggregation-LACP**<br>**VCStack** | Previously, on a VCStack with a late joiner, occasionally if a port-channel went down, the log "Failed to complete post detach mux from aggregator po1 for port port5.0.52, error -1" was generated.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | Y | Y | Y | – | Y | – | – | – | – | – |
| **CR-69139** | **AMF** | Previously, a small memory leak could occurr when updating the AMF area info topology.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **CR-69722** | **AMF**<br>**LLDP** | Previously, an AMF guest node could be reset (i.e. leave and then re-join the AMF network) with every LLDP neighbour information update.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | Y | Y | – | – | Y | – | Y | – | Y | – | Y | Y | – | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-69767**<br>**CR-69962** | **AMF** | Previously, a very unusual combination of AMF provisioning commands left the file system pointing to a non-existent directory.<br>As a result, when AMF backup was performed, it became confused attempting to locate the non-existent directory.<br>The solution of this software update ensures that the AMF backups return to the home directory before initiating the backup.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **CR-69942** | **AMF** | Previously, a transition from an active amf-link to an amf-crosslink on active ports would not work.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **CR-69724** | **AMF** | Previously, the transitioning of an AMF node from AMF member to AMF master could lead to an inconsistent setting of the restricted login functionality across the network.<br>This setting is generally controlled and communicated to the network by the AMF master.<br>Due to the restricted login, functionality was being erroneously enabled on some devices.<br>User logins were delayed for 15 seconds as the AMF functionality attempted to contact neighbouring nodes, which eventually failed 15 seconds later.<br>This update ensures the consistency of the AMF restricted login functionality across the network.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-70236** | **AMF** | Previously, when a device connected via an AMF link, was moved from one upstream device to a different upstream device and both upstream devices had virtual uplinks, it was possible that Layer 3 communication might not resume for the device.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **CR-70488** | **AMF** | Previously, AMF provisioning in secure mode could fail.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **CR-70586** | **AMF** | Previously, when executing the **write config** command on an AMF node connected to another AMF node via a virtual-link, it could fail to distribute a recovery configuration file to all directly connected (downlink, crosslink) adjacent nodes.<br>It could also fail to store a recovery configuration file on any inserted media device (USB/SDCARD).<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| **CR-68139** | **AMF**<br>**Web API** | Previously, on AMF masters/controllers other than the SBx81CFC960, AMF nodes coming/going from the AMF network could result in API requests to AMF nodes via the controller/or master being lost.<br>This was due to the service responsible for proxying these requests being restarted each time a node came or went. With this software update, this service now reloads its configuration in a much more seamless way.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-69051** | **ARP** | Previously, reserved multicast traffic was being reflected out a NLB trunk port.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | – | Y | Y | Y | Y | Y | – | Y | – | – | – | – | – |
| **CR-69557** | **ARP**<br>**Neighbor Discovery** | Previously, multicast traffic with a TTL value of "1" could be incorrectly reflected out a trunk port configured for NLB.<br>This issue has been resolved. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | – | – | – | – | – |
| **CR-68555** | **Auto-negotiation** | Previously, it was possible for an x530 variant switch to not detect a port speed change when the link-partner renegotiated the link speed down to 100M (on 2.5G or 5G ports).<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-67884** | **Bridging** | Previously, if there were no physical interfaces in a running state attached to a bridge, then the host bridge interface would not be brought admin up and running.<br>This issue has been resolved. Now, the bridge interface will be automatically admin up even if there are no physical interfaces attached. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-70380** | **FAN** | With this software update, the fan profile on x530 PoE variants have been improved to allow for quieter operation. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68492** | **Firewall**<br>**PBR** | When a firewall is enabled it detects packets arriving with a source address that is not reachable via any of the routes in the main routing table. Those packets are logged as having a "Martian source" and are dropped.<br>When Firewall is disabled (after being enabled) this check should no longer be performed.<br>However, in some cases the check was still being performed. This could have been a problem in configurations involving Policy Based Routing, as they may have involved hosts that were only reachable via routes that were not in the main route table.<br>Note: This wasn't an issue if the device was booted without Firewall enabled.<br>This issue has now been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | – |
| **CR-69946** | **Flow Control** | Previously, ports connected to a SPTx pluggable could link up even if disabled.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | Y | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-68869** | **IGMP** | Previously, when Jumbo frames support was enabled on a switch, it was possible for the IGMP snooping to cause the switch to restart.<br>This issue has been resolved. | Y | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-67949** | **IGMP** | With this software update, known multicast packets will no longer be reflected out the source port if the source port is also configured as a trunk port for NLB. | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | – | Y | Y | – | Y | Y | Y | – | Y | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68345** | **IPSec** | Previously, when using IKEv1 Aggressive mode with NAT-T, the NAT-T information in the command **show ipsec peer** always showed as being off until the first rekey.<br>This was due to the ISAKMP SA being established and the information recorded before the NAT-T information was known.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-70378** | **IPv6** | With this software update, the preferred and valid lifetime values of IPv6 advertised in router advertisements will now be the lower of the valid and preferred lifetimes of:<br>■ the prefix in the configuration<br>■ any address that matches that prefix on the outgoing interface (i.e an address statically assigned to the interface with non default lifetimes) | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-69706** | **Layer 3 Switching** | Previously, the Layer 3 tables were not configured correctly and could report being full before they actually were.<br>This issue has been resolved. | – | – | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | – |
| **CR-68110** | **LLDP**<br>**PoE** | Previously, when an x320-10 variant switch was connected with a PD device that supported 802.3bt and LLDP, the switch did not send LLDP with the type 3 and 4 field.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-68287** | **LLDP**<br>**PoE** | Previously, with LLDP, sending power via MDI requests would not be processed.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68757** | **Logging**<br>**Hardware Health Monitoring** | Previously, on GS900MX and XS900 variant switches, there was a very small chance that a spurious voltage alarm could be raised.<br>This issue has been resolved.<br>Now, when an alarm is detected for voltage sensors, the value is rechecked before raising an alarm.<br>ISSU: Effective when ISSU complete. | – | – | Y | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-68224** | **Loop protection** | Previously, an error was sometimes shown when entering the command **loop protection action none** on an interface (with or without a timeout), despite the command completing successfully.<br>This issue has been resolved. | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | – |
| **CR-69373** | **MAC Thrashing** | Previously, MAC entries could randomly get deleted from some SBx8100 line cards running on the same chassis while traffic was flowing, resulting in unnecessary unicast traffic flooding.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-69506** | **MAC Thrashing**<br>**Trigger** | Previously, if thrash-limiting with action **`vlan-disable`** on aggregators as well as the **findme** trigger were both configured, port LEDs could sometimes continue to flash indefinitely if ports linked down while thrash-limiting was active.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | Y | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | Y | – | – | – | Y | – | – | – | – | – | – |
| **CR-68301** | **MLD**<br>**Multicast Routing** | Previously, a large number of IGMP or MLD traffic could cause an x930 variant switch to restart unexpectedly.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68374** | **Multicast forwarding hardware** | Previously, the command **show platform table ipmulti** could result in the PIM process to restart unexpectedly.<br>This issue has been resolved. | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | – |
| **CR-67405** | **NTP** | Previously, when NTP detected a time difference and changed the system clock internally, it was possible for this to affect some internal messaging within a switch, resulting in an internal communication failure error message to be logged.<br>This issue has been resolved.<br>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 | – |
| **CR-68229** | **PIM-SM** | Previously, it was possible for the PIM-SM process to restart when it was busy adding routes to the hardware table.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-66534** | **Port configuration** | Previously, an SFP+ port connected with DAC occasionally might not link up on x530L models.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – |
| **CR-67897** | **PPP** | Previously, when a static route was configured with the nexthop as a point-to-point interface (i.e."ip route 0.0.0.0/0 ppp0") and if the interface went down, it was possible for the routing table to make an incorrect decision, causing the route to no longer work as intended (traffic would be dropped).<br>This issue has been resolved. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68362** | **QoS storm protection** | Previously, if QoS Storm Protection was configured to shut down ports in conjunction with Loop Protection configured similarly, it could interfere with Loop Protection's action to shut the port down.<br>Depending on the configuration this could result in the port being brought up sooner than expected, or the port getting into an unexpected state where it displayed as 'err-disabled' but was still passing traffic and would not respond to either the **shutdown** or **no shutdown** commands.<br>This issue has been resolved.<br>Now when both protocols are in use together, QoS Storm Protection will not apply actions when Loop Protection (or any other protocol) has already shut the port down. | – | – | Y | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | – | – |
| **CR-70115** | **SNMP** | Previously, SNMP information was unable to be obtained by IPv6.<br>This issue has been resolved.<br>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-61186** | **SNMP** | Previously, net-snmp was vulnerable to DoS due to null pointer vulnerability stated in CVE-2018-18065 and CVE-2018-18066.<br>This software update addresses the vulnerability. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-69105** | **SSH** | With this software update, it is now possible to configure the SSH server to selectively allow only ciphers which are consistent with ciphers currently offered by OpenSSH by default, with CBC ciphers excluded<br>The new command as part of this implementation is:<br>**`(no)ssh server secure-ciphers`**<br>In addition, the **`show ssh server`** command output has also been modified to show the current ciphers in use.<br>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-69445** | **Storm Control** | With this software update, it is now possible to configure multiple storm-control types and rates on individual port for x220, GS980M and x230-52 variant switches. | – | – | – | – |  | Y | – | – | – | – | – | Y | Y | – |  | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-70387** | **VCStack** | Previously, on a SBx908GEN2, if there was an unexpected restart, then the SFP ports would not go link down until the unit rebooted.<br>This could result in a period of traffic disruption if one or more of the affected SFP ports was a member of a static or dynamic aggregator.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – |
| **CR-68318** | **VCStack** | Previously, interface state changes could sometimes cause audit inconsistencies on a stack.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | – | – |
| **CR-70026** | **VCStack** | Previously, there was a small chance that if a stack member left the stack and rebooted in less than a minute, then the re-booted stack member may not join the stack correctly.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-69703** | **Web API** | Previously, when using the Web API, it was possible for some data to become corrupted when doing SETs or POSTs.<br>This could cause invalid configuration or GETs to not work and could potentially cause the HTTP server to restart.<br>This issue has been resolved.<br>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-69760** | **Web API** | Previously, the CPU load value in the device GUI on AlliedWare+ devices could show a different value to the values shown on the CLI. This was due to a difference in the way that the values were calculated.<br>This issue has been resolved.<br>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-68107** | **Web API** | Previously, obtaining the eth0/eth1 speed via the VAA failed. A random value was returned resulting in a small memory leak in AppWeb.<br>Additionally, another small memory leak could occur when accessing port information via WebAPI on any platform.<br>Both issues have been resolved.<br>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 | – |

# What’s New in Version 5.4.9-2.5

Product families supported by this version:

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

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-2.5.

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

For instructions on how to upgrade to this version, see “Installing this Software Version” on page 94.

For instructions on how to update the web-based GUI, see “Installing and Accessing the Web-based GUI on AR-Series Devices” on page 99. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

| Models | Family | Date | Software File |
|---|---|---|---|
| AMF Cloud | | 05/2020 | vaa-5.4.9-2.5.iso (VAA OS)<br>vaa-5.4.9-2.5. vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.4.9-2.5.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 05/2020 | SBx81CFC960-5.4.9-2.5.rel |
| SBx908 GEN2 | SBx908 GEN2 | 05/2020 | SBx908NG-5.4.9-2.5.rel |
| x950-28XSQ<br>x950-28XTQm | x950 | 05/2020 | x950-5.4.9-2.5.rel |
| x930-28GTX<br>x930-28GPX<br>x930-52GTX<br>x930-52GPX<br>x930-28GSTX | x930 | 05/2020 | x930-5.4.9-2.5.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 05/2020 | x550-5.4.9-2.5.rel |
| x530-28GTXm<br>x530-28GPXm<br>x530L-52GPX | x530 and x530L | 05/2020 | x530-5.4.9-2.5.rel |
| x510-28GTX<br>x510-52GTX<br>x510-28GPX<br>x510-52GPX<br>x510-28GSX<br>x510-28GSX-80<br>x510DP-28GTX<br>x510DP-52GTX<br>x510L-28GT<br>x510L-28GP<br>x510L-52GT<br>x510L-52GP | x510 and x510L | 05/2020 | x510-5.4.9-2.5.rel |
| IX5-28GPX | IX5 | 05/2020 | IX5-5.4.9-2.5.rel |
| x320-10GH | x320 | 05/2020 | x320-5.4.9-2.5.rel |
| x310-26FT<br>x310-50FT<br>x310-26FP<br>x310-50FP | x310 | 05/2020 | x310-5.4.9-2.5.rel |
| x230-10GP<br>x230-10GT<br>x230-18GP<br>x230-18GT<br>x230-28GP<br>x230-28GT<br>x230L-17GT<br>x230L-26GT | x230 and x230L | 05/2020 | x230-5.4.9-2.5.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 05/2020 | x220-5.4.9-2.5.rel |
| IE510-28GSX | IE510-28GSX | 05/2020 | IE510-5.4.9-2.5.rel |
| IE340-20GP<br>IE340L-18GP | IE340 | 05/2020 | IE340-5.4.9-2.5.rel |
| IE300-12GT<br>IE300-12GP | IE300 | 05/2020 | IE300-5.4.9-2.5.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| IE210L-10GP<br>IE210L-18GP | IE210L | 05/2020 | IE210-5.4.9-2.5.rel |
| IE200-6FT<br>IE200-6FP<br>IE200-6GT<br>IE200-6GP | IE200 | 05/2020 | IE200-5.4.9-2.5.rel |
| XS916MXT<br>XS916MXS | XS900MX | 05/2020 | XS900-5.4.9-2.5.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 05/2020 | GS980M-5.4.9-2.5.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 05/2020 | GS980EM-5.4.9-2.5.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 05/2020 | GS970-5.4.9-2.5.rel |
| GS924MX<br>GS924MPX<br>GS948MX<br>GS948MPX | GS900MX/MPX | 05/2020 | GS900-5.4.9-2.5.rel |
| FS980M/9<br>FS980M/9PS<br>FS980M/18<br>FS980M/18PS<br>FS980M/28<br>FS980M/28PS<br>FS980M/52<br>FS980M/52PS<br>FS980M/28DP | FS980M | 05/2020 | FS980-5.4.9-2.5.rel |
| AR4050S<br>AR3050S | AR-series UTM firewalls | 05/2020 | AR4050S-5.4.9-2.5.rel<br>AR3050S-5.4.9-2.5.rel |
| AR2050V<br>AR2010V<br>AR1050V | AR-series VPN firewalls | 05/2020 | AR2050V-5.4.9-2.5.rel<br>AR2010V-5.4.9-2.5.rel<br>AR1050V-5.4.9-2.5.rel |

**Caution:** Software version 5.4.9-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 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 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

The 5.4.9-2.5 software version is ISSU compatible with 5.4.9-2.4.

# New Features and Enhancements

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ER-3282** | **OSPFv2** | With this software update, the existing **area range** command in OSPFv2 now has an additional optional **cost** parameter.<br>Normally when summary routes are generated the metric sent in the LSA is the largest of all possible paths that can be used to reach the destination network. When the cost parameter is specified, the metric sent in the LSA will be overridden by whatever value the user has specified.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | Y | – |
| **ER-3282** | **OSPFv2** | With this software update, OSPFv2 on AlliedWare Plus routers now support the **`distribute-list route-map NAME in`** command that was previously only available on AlliedWare Plus switches.<br>Also with this software update, in route-map configuration mode the command "**`no match interface NAME`**" no longer fails the initial system configuration load.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | Y | Y | Y | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | Y | – |

# Issues Resolved in Version 5.4.9-2.5

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

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66385** | **AMF** | Previously, under rare circumstances, the command shell could restart unexpectedly on an AMF member when a working-set was initiated.<br>This issue has been resolved.<br>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-66929** | **AMF** | Previously, it was not possible to specify a GS980EM switch as an AMF working set group.<br>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-67201** | **AMF** | Previously, the incorrect directory name was generated after executing the **`clone`** command.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | Y | Y |
| **CR-68336** | **AMF** | Previously on all x530L models, the AMF-Guest and AMF-Starter license were not included in the base license.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – |
| **CR-63778** | **Antivirus**<br>**Web Control** | Previously, when Web Control was enabled, a small amount of memory was lost each time a categorization request was made to the Digital Arts server.<br>Although the amount of memory was small, over time it could reduce the amount of free memory in the system, triggering the generation of low memory diagnostics. Eventually a system reboot could be triggered.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66550** | **API** | Previously, rebooting using the RESTful API did not log anything in the reboot history, resulting in an unexpected log being added to the reboot history.<br>This issue has been resolved.<br>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-67959** | **ARP Security** | With this software update, rate limiting will be applied to ARP security on GS900, x310, x510 and x550 series switches. | – | – | Y | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | Y | – | – | – | – | – | – | – | – | – | – |
| **CR-67246** | **AWC Lite** | Previously, the wireless controller function experienced a system reboot when the SSID of the AP could not be obtained.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | Y | – | – | Y | Y | Y | Y | Y | – |
| **CR-68016** | **AWC Lite** | Previously, the configured IP address was not being set as the management address of AWC-Lite after restarting the device.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | Y | – | – | Y | Y | Y | Y | Y | – |
| **CR-68122** | **AWC Lite** | With this software update, the MAC OUI for AP has been added to AWC lite. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | Y | – | – | Y | – | Y | Y | Y | – |
| **CR-66502** | **CLI** | Previously, the login banner was not being displayed.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-68208** | **Command Shell** | Previously, if an unexpected input character was entered before the ATMF shell handler had completed initialisation, this could result in an unexpected termination of the shell process.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66541** | **DPI**<br>**URL Filtering** | Previously, starting a stream feature such as DPI or IPS on a low memory device a period after the device had been processing packets, could result in the device not having enough free memory to start stream processing.<br>This issue has been resolved.<br>The device now tries to reclaim memory used by the system for performance caching to maximize the amount of available memory. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-66891** | **Environmental Monitoring** | Previously on x510-DP and x930 platforms, if a PSU fan quickly and completely stopped spinning (rather than a rotation rate just being below the threshold), before an alarm was triggered for the event, the alarm would not be triggered<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | Y | – | – | – | – | – | – | – | – | – |
| **CR-67588** | **Firewall** | Previously, on occasion, attempting to modify a firewall entity that was in use could result in an error, and the modification would fail.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-68159** | **LACP** | Previously, it was possible for user-configured LACP to be deleted when the LACP link went down.<br>This issue has been resolved.<br>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-66270** | **LACP Aggregation**<br>**Static Aggregation**<br>**VCStack** | Previously, when a stack member joined a Stack while initial configuration was being run, it could fail to apply the aggregator information correct in hardware.<br>This issue has been resolved. | – | – | Y | Y | Y | – | – | – | – | – | – | – | – | Y | – | Y | Y | – | Y | – | Y | – | – | Y | – | – | – | – | – |
| **CR-65941** | **Licensing** | Previously, a small memory leak could occur during a software license check.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-61985** | **Logging** | Previously, if multiple remote syslog destinations were configured with a specific source address, it was possible that all but one of the sources could continue to send with that source address, even if the source address configuration was changed.<br>This issue has been resolved. All log destinations will now be sent messages with the new source IP address.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – |
| **CR-66492** | **Logging** | Previously, if a **show tech** command was executed on a SBx908NG with a XEM2-12XS v1 installed, then it was possible for link down/ up events to be seen in the log.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – |
| **CR-66435** | **MACSec** | Previously, the MACsec counters could show incorrect values. Notably, "Pkts Late (Allowed)" and "Bytes Validated Only" could display as zero.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | – | Y | – | – | – | – | – |
| **CR-66538** | **MACSec** | Previously, the authd process could leak memory when issuing the command **`show macsec`** and periodically when hardware counters were gathered.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | – | Y | – | – | – | – | – |
| **CR-66937** | **MACSec** | Previously, there was a security vulnerability in MACSec whereby it was possible to bypass MACSec ingress frame checks.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | – | Y | – | – | – | – | – |
| **CR-67794** | **MACSec** | Previously, applying an MKA policy for the first time on a running port could result in the command failing.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | – | Y | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68340** | **Mirroring** | Previously, the command **`switchport remote-mirror-egress`** was missing in the running-configuration when configured on a provisioned port.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | Y | – |
| **CR-68100** | **MLD**<br>**PIMv6** | Previously, an incorrect source address size was being copied when PIMv6 was learning MLDv2 group records. This lead to addresses becoming corrupt and incorrect in PIMv6.<br>This issue has been resolved.<br>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-67730** | **Multicast Forwarding Hardware** | Previously, it was possible for a switch to learn multicast joins and unregistered multicast simultaneously. Adding both of these caused the switch to think that the multicast limit was already reached.<br>This was incorrect, as learning a multicast join shares the same hardware entry as the unregistered multicast entry meaning no extra hardware entries need to be consumed. This issue has been resolved.<br>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-68084** | **Multicast Forwarding Hardware** | Previously, switching multicast traffic at Layer 2 with frames larger than 1500 bytes was not supported.<br>With this software update, now, provided the ports have their MRU set to the appropriate size, jumbo frames can be correctly Layer 2 switched.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66812** | **Multicast Routing** | Previously, static multicast routing would not forward multicast traffic.<br>This issue has been resolved.<br>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-68229** | **PIM-SM** | Previously, it was possible for the PIM-SM process to restart when it was busy adding routes to the hardware table.<br>This issue has been resolved.<br>With this software update, it is now possible to configure how many internal updates PIM-SM, PIM-DM or PIM6-SM process at a time.<br>This can be configured by the command **`ip pim sparse-mode event-queue-length <num>`**.<br>■ Configuring a shorter event queue length allows PIM to allocate more CPU time to handling PIM packets and PIM timeout events.<br>■ Configuring a longer event queue length allows PIM to allocate more CPU time to updating hardware.<br>Previously, obtaining the eth0/eth1 speed via the VAA failed. A random value was returned resulting in a small memory leak in AppWeb.<br>Additionally, another small memory leak could occur when accessing port information via WebAPI on any platform.<br>Both issues have been resolved.<br>ISSU: Effective when CFCs upgraded.. | – | – | Y | – | – | – | – | – | Y | Y | Y | – | – | Y | Y | – | Y | Y | Y | Y | Y | – | Y | Y | – | – | Y | Y | Y |
| **CR-66162** | **Pluggable Transceivers** | Previously, it was possible for a hotswap of a AT-SP10T module to cause a system reboot on an x550-18XSQ V1 or V2 switch.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-68194** | **Pluggable Transceivers** | Previously, an unexpected system reboot could occur when a SP10T was inserted and removed too quickly.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | – | Y | – | – | – | – | – |
| **CR-66101** | **PoE** | Previously, if PoE power was shut down on a IE340 series switch due to the over temperature, the switch would stop providing PoE power.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-66344** | **PoE** | Previously on some PoE switches, the switch did not correctly apply a power value to a port. The value was supplied via LLDP-MED by the powered device.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | – | – | – | – |
| **CR-67281** | **PoE** | Previously, the SBx81GP24 line card would not power up a powered device that was close to its power limit.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-67397** | **PoE** | Previously, the x320 series switch PoE might become unresponsive when disabling or enabling PoE on some ports.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-66988** | **PoE**<br>**Port Configuration** | Previously, the AT-GS980MX series switch might start up with PoE reporting odd or even ports transposed.<br>This issue has been resolved. | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66532** | **PoE**<br>**VCStack** | Previously, on stacked PoE switches, it was possible for the **`no power-inline enable`** command to not be set on a backup stack member. If a failover occurred, then this configuration might have been lost.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | – | Y | – | Y | – | – | – | – | – | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | – | – | – | – | – | – |
| **CR-67586** | **Port Configuration** | Previously, GS980MX (or x530) and x550 series switches may not have linked up when connected using DAC pluggable.<br>This issue has been resolved. | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | – | – | – | – | – | – | – | – | – |
| **CR-67129** | **Port**<br>**Authentication** | Previously, dynamic port authentication data would not be synchronised across a stack.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – |
| **CR-68031** | **PPP** | With this software update, AlliedWare Plus routers are no longer vulnerable to EAP packet processing security issue stated in "CVE-2020-8597". | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-67008** | **QoS** | Previously It was not possible to set the DSCP field using a policy map.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | Y | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | Y | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-67752** | **QoS** | Previously on some switch models containing 2 switch chips, an ACL which changed a packet's user priority was also changing the CPU priority of the packet.<br>This could result in the CPU being starved of more important traffic breaking protocols such as OSPF.<br>This issue has been resolved. | – | – | Y | – | – | – | – | – | – | – | – | – | Y | Y | – | Y | Y | – | – | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-67995** | **SFlow** | Previously, if SFlow was configured using an interface range, the first port in that interface range would not be applied at startup.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | Y | – | – | – | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | – | – | – | – |
| **CR-66449** | **SNMP** | Previously if the SNMP process used too much memory, the wrong process was restarted meaning the memory was not freed.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – |
| **CR-67011** | **SNMP** | Previously, on the GS980EM/10H switch, an incorrect OID was returned when querying over SNMP.<br>This issue has been resolved. | – | – | – | – | Y | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-68157** | **Static Aggregation** | Previously, it was possible to see the error message when a channel-group was removed: "03:29:26 stk_a_1355_1001 HSL[963]: ERROR: Failed to remove ingress class on trunk port 03:29:26 stk_a_1355_1001 HSL[963]: ERROR: Failed to remove trunk source knockout FP entry for new trunk member"<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-67985** | **Triggers** | Previously, on devices with 32-bit processors, if a trigger was configured with a day-of-the-month condition (any day on any month, any year) it would not activate as expected.<br>This issue has been resolved. | Y | Y | Y | Y | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | – | – | – | – | – | – | – | – | – | – | – |
| **CR-50474** | **VCStack** | Previously, when a VCStack Plus stack had a large configuration, a failover could cause the re-joining stack to fail to load the configuration, resulting in a backplane fault being logged.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-65948** | **VCStack** | Previously on an x530 or SBxCFC960 stack, when multiple members were joining at the same time, some members could get stuck in the Initiation state and fail to join the stack.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-66297** | **VCStack** | Previously, VCStacking was not working using AT-SP10T modules on XEM2-8XSTm and XEM2-12XS.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – |  | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | – | – | – |
| **CR-66523** | **VCStack** | Previously, when ports were linked up using DAC, a number of link flapping scenarios could be observed.<br>This issue has been resolved. | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – |
| **CR-67851** | **VCStack** | Previously, on very rare occasions when VCStacking was interacting with a non AlliedWare Plus LACP active device with faster LACP packet transmission rate, the NSM process might restart on backup members if the LACP links were experiencing link-flapping.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | – | – | – | – | Y | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | – | – | – | – |
| **CR-68322** | **VCStack** | Previously, during a VCStacking failover on a x950 or x908Gen2 switch it was possible for SFP+ ports to take longer than expected to shut down, resulting in a longer failover time and traffic disruption.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | – | – | – |
| **CR-68323** | **VCStack** | Previously, on a x530 stack, stack port could fail to link up after removing and re-inserting a stackXS cable.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | GS980EM | IE200 | IE210L | IE300 | IE340 | IE510 | x220 | x230, x230L | x310 | x320 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx908 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66525** | **VCStack**<br>**Auto-negotiation** | Previously, if a port linked up at half duplex and late collisions occurred due to a duplex mis-match, it was possible for the port to stop forwarding traffic.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | Y | – | – | Y | – | – | – | – | – | – | – | – | – | – | – |
| **CR-64055** | **VLAN** | With this software update, it is now possible to add the same outer VLAN tag to multiple VLAN translation rules.<br>This means rules such as "switchport vlan translation vlan100 vlan 30 outer-vlan 10" and "switchport vlan translation vlan101 vlan 31 outer-vlan 10" are now possible.<br>DHCP Snooping also has a new command per VLAN to allow VLAN translation to be compatible.<br>Enabling **`ip dhcp snooping disable-l2-flooding`** on each vlan that is involved with VLAN translation stops duplicate DHCP packets from being flooded by the switch when DHCP Snooping is enabled.<br>This issue has been resolved. | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | – | Y | Y | – | Y | Y | Y | – | – | Y | – | – | – | – | – |
| **CR-67522** | **Web API** | Previously the **`show users`** command would report incorrect output for VTY lines that were in use by the WebAPI.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | – |
| **CR-68107** | **Web API** | Previously, obtaining the eth0/eth1 speed via the VAA failed. A random value was returned resulting in a small memory leak in AppWeb.<br>Additionally, another small memory leak could occur when accessing port information via WebAPI on any platform.<br>Both issues have been resolved.<br>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 |

# What’s New in Version 5.4.9-2.4

Product families supported by this version:

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

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-2.4.

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

For instructions on how to upgrade to this version, see “Installing this Software Version” on page 94.

For instructions on how to update the web-based GUI, see “Installing and Accessing the Web-based GUI on AR-Series Devices” on page 99. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

| Models | Family | Date | Software File |
|---|---|---|---|
| AMF Cloud | | 02/2020 | vaa-5.4.9-2.4.iso (VAA OS)<br>vaa-5.4.9-2.4. vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.4.9-2.4.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 02/2020 | SBx81CFC960-5.4.9-2.4.rel |
| SBx908 GEN2 | SBx908 GEN2 | 02/2020 | SBx908NG-5.4.9-2.4.rel |
| x950-28XSQ<br>x950-28XTQm | x950 | 01/2020 | x950-5.4.9-2.4.rel |
| x930-28GTX<br>x930-28GPX<br>x930-52GTX<br>x930-52GPX<br>x930-28GSTX | x930 | 02/2020 | x930-5.4.9-2.4.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 02/2020 | x550-5.4.9-2.4.rel |
| x530-28GTXm<br>x530-28GPXm<br>x530L-52GPX | x530 and x530L | 02/2020 | x530-5.4.9-2.4.rel |
| x510-28GTX<br>x510-52GTX<br>x510-28GPX<br>x510-52GPX<br>x510-28GSX<br>x510-28GSX-80<br>x510DP-28GTX<br>x510DP-52GTX<br>x510L-28GT<br>x510L-28GP<br>x510L-52GT<br>x510L-52GP | x510 and x510L | 02/2020 | x510-5.4.9-2.4.rel |
| IX5-28GPX | IX5 | 02/2020 | IX5-5.4.9-2.4.rel |
| x310-26FT<br>x310-50FT<br>x310-26FP<br>x310-50FP | x310 | 02/2020 | x310-5.4.9-2.4.rel |
| x230-10GP<br>x230-10GT<br>x230-18GP<br>x230-18GT<br>x230-28GP<br>x230-28GT<br>x230L-17GT<br>x230L-26GT | x230 and x230L | 02/2020 | x230-5.4.9-2.4.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 02/2020 | x220-5.4.9-2.4.rel |
| IE510-28GSX | IE510-28GSX | 02/2020 | IE510-5.4.9-2.4.rel |
| IE340-20GP<br>IE340L-18GP | IE340 | 02/2020 | IE340-5.4.9-2.4.rel |
| IE300-12GT<br>IE300-12GP | IE300 | 02/2020 | IE300-5.4.9-2.4.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 02/2020 | IE210-5.4.9-2.4.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| IE200-6FT<br>IE200-6FP<br>IE200-6GT<br>IE200-6GP | IE200 | 02/2020 | IE200-5.4.9-2.4.rel |
| XS916MXT<br>XS916MXS | XS900MX | 02/2020 | XS900-5.4.9-2.4.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 02/2020 | GS980M-5.4.9-2.4.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 02/2020 | GS970-5.4.9-2.4.rel |
| GS924MX<br>GS924MPX<br>GS948MX<br>GS948MPX | GS900MX/MPX | 02/2020 | GS900-5.4.9-2.4.rel |
| FS980M/9<br>FS980M/9PS<br>FS980M/18<br>FS980M/18PS<br>FS980M/28<br>FS980M/28PS<br>FS980M/52<br>FS980M/52PS<br>FS980M/28DP | FS980M | 02/2020 | FS980-5.4.9-2.4.rel |
| AR4050S<br>AR3050S | AR-series UTM firewalls | 02/2020 | AR4050S-5.4.9-2.4.rel<br>AR3050S-5.4.9-2.4.rel |
| AR2050V<br>AR2010V<br>AR1050V | AR-series VPN firewalls | 02/2020 | AR2050V-5.4.9-2.4.rel<br>AR2010V-5.4.9-2.4.rel<br>AR1050V-5.4.9-2.4.rel |

**Caution:** Software version 5.4.9-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 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 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

The 5.4.9-2.4 software version is ISSU compatible with 5.4.9-2.3.

# Issues Resolved in Version 5.4.9-2.4

This AlliedWare Plus maintenance version includes the following resolved issue:

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | IE200 | IE210L | IE300 | IE340/IE340L | IE510 | x210 | x220 | x230, x230L | x310 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **N/A** | **System** | Previously, on the IE340L Series, it was possible for the CPU to receive spurious i2c interrupts which could slow CPU performance. In rare cases, this could cause the device to restart at boot.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |

# What’s New in Version 5.4.9-2.3

Product families supported by this version:

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

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-2.3.

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

For instructions on how to upgrade to this version, see “Installing this Software Version” on page 94.

For instructions on how to update the web-based GUI, see “Installing and Accessing the Web-based GUI on AR-Series Devices” on page 99. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

| Models | Family | Date | Software File |
|---|---|---|---|
| AMF Cloud | | 01/2020 | vaa-5.4.9-2.3.iso (VAA OS)<br>vaa-5.4.9-2.3. vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.4.9-2.3.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 01/2020 | SBx81CFC960-5.4.9-2.3.rel |
| SBx908 GEN2 | SBx908 GEN2 | 01/2020 | SBx908NG-5.4.9-2.3.rel |
| x950-28XSQ<br>x950-28XTQm | x950 | 01/2020 | x950-5.4.9-2.3.rel |
| x930-28GTX<br>x930-28GPX<br>x930-52GTX<br>x930-52GPX<br>x930-28GSTX | x930 | 01/2020 | x930-5.4.9-2.3.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 01/2020 | x550-5.4.9-2.3.rel |
| x530-28GTXm<br>x530-28GPXm<br>x530L-52GPX | x530 and x530L | 01/2020 | x530-5.4.9-2.3.rel |
| x510-28GTX<br>x510-52GTX<br>x510-28GPX<br>x510-52GPX<br>x510-28GSX<br>x510-28GSX-80<br>x510DP-28GTX<br>x510DP-52GTX<br>x510L-28GT<br>x510L-28GP<br>x510L-52GT<br>x510L-52GP | x510 and x510L | 01/2020 | x510-5.4.9-2.3.rel |
| IX5-28GPX | IX5 | 01/2020 | IX5-5.4.9-2.3.rel |
| x310-26FT<br>x310-50FT<br>x310-26FP<br>x310-50FP | x310 | 01/2020 | x310-5.4.9-2.3.rel |
| x230-10GP<br>x230-10GT<br>x230-18GP<br>x230-18GT<br>x230-28GP<br>x230-28GT<br>x230L-17GT<br>x230L-26GT | x230 and x230L | 01/2020 | x230-5.4.9-2.3.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 01/2020 | x220-5.4.9-2.3.rel |
| IE510-28GSX | IE510-28GSX | 01/2020 | IE510-5.4.9-2.3.rel |
| IE340-20GP<br>IE340L-18GP | IE340 | 01/2020 | IE340-5.4.9-2.3.rel |
| IE300-12GT<br>IE300-12GP | IE300 | 01/2020 | IE300-5.4.9-2.3.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 01/2020 | IE210-5.4.9-2.3.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| IE200-6FT<br>IE200-6FP<br>IE200-6GT<br>IE200-6GP | IE200 | 01/2020 | IE200-5.4.9-2.3.rel |
| XS916MXT<br>XS916MXS | XS900MX | 01/2020 | XS900-5.4.9-2.3.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 01/2020 | GS980M-5.4.9-2.3.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 01/2020 | GS970-5.4.9-2.3.rel |
| GS924MX<br>GS924MPX<br>GS948MX<br>GS948MPX | GS900MX/MPX | 01/2020 | GS900-5.4.9-2.3.rel |
| FS980M/9<br>FS980M/9PS<br>FS980M/18<br>FS980M/18PS<br>FS980M/28<br>FS980M/28PS<br>FS980M/52<br>FS980M/52PS<br>FS980M/28DP | FS980M | 01/2020 | FS980-5.4.9-2.3.rel |
| AR4050S<br>AR3050S | AR-series UTM firewalls | 01/2020 | AR4050S-5.4.9-2.3.rel<br>AR3050S-5.4.9-2.3.rel |
| AR2050V<br>AR2010V<br>AR1050V | AR-series VPN firewalls | 01/2020 | AR2050V-5.4.9-2.3.rel<br>AR2010V-5.4.9-2.3.rel<br>AR1050V-5.4.9-2.3.rel |

**Caution:** Software version 5.4.9-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 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 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

The 5.4.9-2.3 software version is ISSU compatible with 5.4.9-2.2.

# New Features and Enhancements

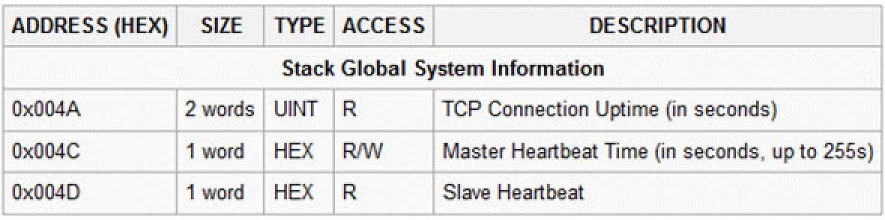
This section summarizes the new features in 5.4.9-2.3:

## New MODBUS heartbeat registers

*Available on IE300, IE340, x930, x950 devices*

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

They are as follows:



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

## 8-unit stacking support for x950 Series switches

*Available on x950 Series switches*

From 5.4.9-2.3 onwards, VCStack enables you to stack up to eight x950 series switches. The maximum number of VLANs supported is 2000, and the recommended number of VLANs is 1000.

# Issues Resolved in Version 5.4.9-2.3

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

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | IE200 | IE210L | IE300 | IE340 | IE510 | x210 | x220 | x230, x230L | x310 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66194** | **AMF** | Previously on the SBx81CFC960 v2, the maximum number of AMF virtual-links was 32.<br>This has been increased to 60, the same limit applied to the SBx81CFC960.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-66040** | **AMF Cloud Vista** | Previously, the AMF topology map may not have been correctly displayed on AMF Vista for areas using VAA container masters.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y |
| **CR-66303** | **AWC** | With this software version, the field: "Latest Calculated Time" seen in the output of the command: **`show wireless power-channel calculate`** is updated when the command **`wireless power-channel ap all calculate`** is used. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | – | Y | Y | Y | Y | Y | – |
| **CR-66273** | **Container Services** | Previously, ACS Instance log files grew without bound, which potentially caused memory shortages. Now they are bounded, and have rotated files.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-66094** | **Device Management** | Previously, keyboard input during the boot process could interrupt the bootup sequence.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-66189** | **Hardware Health Monitoring** | Previously, there was an issue causing the following false log event: *Platform: SENSOR Board Base - Voltage: 0.9V: Alarm asserted*.<br>This was because, when a voltage over-threshold event occurred and the alarm cleared, a driver issue could cause the alarm to constantly trigger.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | IE200 | IE210L | IE300 | IE340 | IE510 | x210 | x220 | x230, x230L | x310 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66172** | **HSL** | Previously, traffic through the device could result in the log message: *HSL[704]: hslnetlink-listen recvmsg overrun: No buffer space available.*<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – |
| **CR-65777** | **IGMP** | Previously, IGMP queries could fail to be sent resulting in incorrect timing out of multicast groups.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | Y | – | – | – | – | – |
| **CR-66061** | **LACP**<br>**ARP** | When using the arp-mac-disparity functionality it was possible for some unknown multicast packets to be reflected on ingress of a trunk port.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | Y | – | – | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | – | – | – | – | – |
| **CR-66341** | **Load Balancing**<br>**VCStack** | Previously, when using the flooding nexthop functionality for Microsoft NLB support, traffic flows could fail after a VCStack failover.<br>This issue has been resolved. | Y | – | Y | Y | Y | – | – | – | – | Y | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | – | – | – | – |
| **CR-66069** | **MACsec**<br>**Counters** | Previously, if MACsec was configured and allowed to run for some time, packet counters would be incremented.<br>If MACsec was de-configured and then re-configured, the counters would not be reset to 0 and would instead continue to count from the previous values.<br>This issue has been resolved, the counters now reset to 0 when MACsec is re-configured.<br>Also, the output from the command **`show macsec`** has been improved. Now the EAPOL packet counters are more accurate as they are read directly from hardware.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | Y | – | – | – | – | – |
| **CR-65719** | **Pluggable Transceivers** | Previously, some fiber pluggables on XLEM/XS8 cards had issues with linkup.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-66033** | **PoE** | Previously PoE could sometimes fail to startup correctly.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | IE200 | IE210L | IE300 | IE340 | IE510 | x210 | x220 | x230, x230L | x310 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66036** | **PoE** | Previously, PoE could fail to work after a DC power interruption.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-66279** | **PoE** | Previously, on an IE300 device, it was not possible to power up single-signature PoE devices.<br>This issue has been resolved. | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-64321** | **PoE**<br>**Logging** | Previously, an I2C error could sometimes get logged at startup.<br>This did not have any functional consequences.<br>This issue has been resolved. | – | Y | – | – | – | – | Y | – | – | – | – | Y | Y | Y | – | – | Y | – | – | – | – | – | – | – | – | – | – |
| **CR-66174** | **Port Authentication** | With this software version, Auth-web on routers no longer requires NAT to be enabled. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-61256** | **RADIUS** | Previously, if a client device failed to connect to a primary RADIUS server, it could result in the client device not sending further RADIUS requests.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | Y | Y | Y | Y | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – | Y | Y | Y | – |
| **CR-66366** | **Static Aggregation**<br>**HW QoS**<br>**VCStack** | Previously, multiple stack-member failovers could cause ACLs to fail when they were applied to aggregators.<br>This issue has been resolved. | – | – | 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 | x210 | x220 | x230, x230L | x310 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-63363** | **Suricata** | Previously, an issue existed where the Suricata process could consume excessive amounts of memory leading to the device rebooting. This could occur when any of IPS, URL Filtering or Malware Protection were enabled. It was particularly likely to occur when Web Control was enabled but was also possible in cases where the device was handling HTTP sessions containing multiple requests and responses.<br>Additionally, there was an issue where the memory management system would behave inefficiently, leaving large amounts of memory available exclusively to the Suricata process. In some cases this could lead to a low memory condition or even to the device rebooting. This issue could occur on devices with Malware Protection enabled and was particularly likely on the AR3050S, which has less RAM available.<br>These issues have been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-66131** | **System** | Previously when an AR1050V was restarted there was a very small possibility of an unexpected system reboot.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – |
| **CR-66352** | **VCStack** | Previously, 10G fiber did not link up on bootup.<br>This issue has been resolved. | – | – | Y | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-66237** | **VCStack**<br>**Web API** | Previously the GUI could show VCS configuration options on some devices that did not support VCS.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | Y | – | – | Y | Y | Y | Y | Y | – | – | Y | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-65007** | **VRF-Lite** | Previously, clearing multicast routes with the command: **`clear ip mroute`** could occasionally report an error message.<br>This issue has been resolved. | – | – | – | Y | – | – | – | – | – | – | – | – | – | Y | – | Y | Y | Y | Y | Y | – | – | – | – | – | – | – |

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M/MX | IE200 | IE210L | IE300 | IE340 | IE510 | x210 | x220 | x230, x230L | x310 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-64043** | **Web Control** | Previously, when using Web-Control, if the log message:<br>*"UTM[<pid>]: Web_Control: Digital Arts connectivity error (<reason>)"*<br>was seen, the c-icap process associated with Web-Control could lose memory. Over time this could cause excessive memory consumption, leading to a warning about low memory on the device and eventually to the device rebooting.<br>This issue has been resolved. The log message may still be seen but there is now no memory loss associated with it. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – |
| **CR-66042** | **Web Control** | Previously, Web Control configuration was not fully returned to defaults when the feature was disabled.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – |

# What’s New in Version 5.4.9-2.2

Product families supported by this version:

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

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-2.2.

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

For instructions on how to upgrade to this version, see “Installing this Software Version” on page 94.

For instructions on how to update the web-based GUI, see “Installing and Accessing the Web-based GUI on AR-Series Devices” on page 99. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

| Models | Family | Date | Software File |
|---|---|---|---|
| AMF Cloud | | 11/2019 | vaa-5.4.9-2.2.iso (VAA OS)<br>vaa-5.4.9-2.2. vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.4.9-2.2.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 11/2019 | SBx81CFC960-5.4.9-2.2.rel |
| SBx908 GEN2 | SBx908 GEN2 | 11/2019 | SBx908NG-5.4.9-2.2.rel |
| x950-28XSQ<br>x950-28XTQm | x950 | 11/2019 | x950-5.4.9-2.2.rel |
| x930-28GTX<br>x930-28GPX<br>x930-52GTX<br>x930-52GPX<br>x930-28GSTX | x930 | 11/2019 | x930-5.4.9-2.2.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 11/2019 | x550-5.4.9-2.2.rel |
| x530-28GTXm<br>x530-28GPXm<br>x530L-52GPX | x530 and x530L | 11/2019 | x530-5.4.9-2.2.rel |
| x510-28GTX<br>x510-52GTX<br>x510-28GPX<br>x510-52GPX<br>x510-28GSX<br>x510-28GSX-80<br>x510DP-28GTX<br>x510DP-52GTX<br>x510L-28GT<br>x510L-28GP<br>x510L-52GT<br>x510L-52GP | x510 and x510L | 11/2019 | x510-5.4.9-2.2.rel |
| IX5-28GPX | IX5 | 11/2019 | IX5-5.4.9-2.2.rel |
| x310-26FT<br>x310-50FT<br>x310-26FP<br>x310-50FP | x310 | 11/2019 | x310-5.4.9-2.2.rel |
| x230-10GP<br>x230-10GT<br>x230-18GP<br>x230-18GT<br>x230-28GP<br>x230-28GT<br>x230L-17GT<br>x230L-26GT | x230 and x230L | 11/2019 | x230-5.4.9-2.2.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 11/2019 | x220-5.4.9-2.2.rel |
| IE510-28GSX | IE510-28GSX | 11/2019 | IE510-5.4.9-2.2.rel |
| IE340-20GP<br>IE340L-18GP | IE340 | 11/2019 | IE340-5.4.9-2.2.rel |
| IE300-12GT<br>IE300-12GP | IE300 | 11/2019 | IE300-5.4.9-2.2.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 11/2019 | IE210-5.4.9-2.2.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| IE200-6FT<br>IE200-6FP<br>IE200-6GT<br>IE200-6GP | IE200 | 11/2019 | IE200-5.4.9-2.2.rel |
| XS916MXT<br>XS916MXS | XS900MX | 11/2019 | XS900-5.4.9-2.2.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 11/2019 | GS980M-5.4.9-2.2.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 11/2019 | GS970-5.4.9-2.2.rel |
| GS924MX<br>GS924MPX<br>GS948MX<br>GS948MPX | GS900MX/MPX | 11/2019 | GS900-5.4.9-2.2.rel |
| FS980M/9<br>FS980M/9PS<br>FS980M/18<br>FS980M/18PS<br>FS980M/28<br>FS980M/28PS<br>FS980M/52<br>FS980M/52PS<br>FS980M/28DP | FS980M | 11/2019 | FS980-5.4.9-2.2.rel |
| AR4050S<br>AR3050S | AR-series UTM firewalls | 11/2019 | AR4050S-5.4.9-2.2.rel<br>AR3050S-5.4.9-2.2.rel |
| AR2050V<br>AR2010V<br>AR1050V | AR-series VPN firewalls | 11/2019 | AR2050V-5.4.9-2.2.rel<br>AR2010V-5.4.9-2.2.rel<br>AR1050V-5.4.9-2.2.rel |

⚠ **Caution:** Software version 5.4.9-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 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 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

The 5.4.9-2.2 software version is ISSU compatible with 5.4.9-2.1.

# New Features and Enhancements

This section summarizes the new features in 5.4.9-2.2:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 89.

## IP Reputation whitelist

*Available on AR4050S and AR3050S UTM firewalls*

From 5.4.9-2.2 onwards, you can add IP addresses to an IP Reputation whitelist, so that IP Reputation will not alert or deny traffic to or from this address even if it is on an IP Reputation provider's lists.

For example, this may be useful in the following situations:

- A hosting site uses an IP address for a wide range of domains, some of which have been identified as 'bad', but most of which are acceptable. A user may wish to access the acceptable domains.
- An address may have been subject to some malicious activity and gained a bad reputation. Once the malicious activity has been resolved, a user may urgently need to regain access to the site before the address's reputation has been restored.

For more information about configuring and using the IP Reputation whitelist, see the Advanced Network Protection Feature Overview and Configuration Guide.

## Combined preference for SD-WAN

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

From 5.4.9-2.2 onwards, you can configure an SD-WAN linkmon profile to use the **combined** preference. The combined preference use a combination of latency, jitter, and packet loss when breaking ties to select the best links. This is a more sophisticated way of considering the quality of a link, and can result in more appropriate links being selected to send traffic over.

For more information about the combined preference, see the SD-WAN Feature Overview and Configuration Guide.

# 802.1X authentication on AR-series switch ports

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

From 5.4.9-2.2 onwards, 802.1X authentication is supported on the switch ports of the AR2050V, AR3050S, and AR4050S security appliances. This means the following authentication methods are supported on the following port types:

Table 2: AR2050V, AR3050S, and AR4050S port authentication support

| Port type | Authentication methods | Supported from version |
|---|---|---|
| Switch port | 802.1x authentication<br>MAC authentication | 5.4.9-2.2<br>5.4.8-2.1 |
| Ethernet port | Web authentication | 5.4.5-2.1 |

As both MAC and 802.1X authentication are supported on the device's switch ports, two-step authentication is also supported on these devices. When two-step authentication is enabled the sequence is MAC authentication first followed by 802.1X authentication.

The following limitations apply to these devices:

- 802.1X authentication is not supported on static channel-groups and dynamic (LACP) channel-groups.
- Dynamic VLAN assignment can only be configured per port and not per MAC address. This means that all supplicants on a port can only be dynamically assigned to the same VLAN. Different VLANS, however, can be assigned on different ports. (See the **auth dynamic-vlan-creation** command for more information on dynamic VLANs.)
- The maximum number of supplicants is 1024 per port and 1024 system-wide.

For more information on configuring port authentication, see the AAA and Port Authentication Feature Overview and Configuration Guide.

# Changeable context-id for USB modem

*Available on all AR-Series firewalls and VPN routers*

From 5.4.9-2.2 onwards, you can use the new command **cid** to set the PDP Context-ID (CID) instead of using a custom chat-script for 3G modems. The customer information in the CID is used to connect to a cellular network. This command is used in Interface Configuration (cellular) mode.

# Disabling rekeying of unused IPsec SAs

*Available on all AR-Series firewalls and VPN routers*

From 5.4.9-2.2 onwards, you can specify a rekey policy for an IPsec profile. This policy will be used to make a decision on whether the SA will rekey at its expiry.

The options are always, never, and on-demand. The on-demand option makes its decision based on whether the link has seen any traffic since the SA's last rekey. Note that the default behavior remains unchanged and is to always rekey.

The new options may be useful if you have a hub and spoke VPN topology and need to provision more than the maximum number of concurrent active VPNs supported by your AR-Series device. The new options age out unused VPNs more quickly, making more efficient use of the number of available VPNs. To specify the rekey policy, use the following new command in IPsec Profile Configuration mode:

```
rekey {always|never|on-demand}
```

For example, to only rekey when traffic is detected over the interface, in the profile named "myprofile", use the commands:

```
awplus(config)#crypto ipsec profile myprofile
awplus(config-ipsec-profile)#rekey on-demand
```

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

## Linkmon trigger enhancement

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

Previously, linkmon probe down triggers would not have activated at startup if an underlying source or egress-interface was down or when the probe was enabled and failed. 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.

From 5.4.9-2.2 (and also 5.4.9-1.3) onwards, 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.

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.

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.

For more information about linkmon probes, see the SD-WAN Feature Overview and Configuration Guide.

# Issues Resolved in Version 5.4.9-2.2

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

| CR | Module | Description | FS980M | GS970M | GS900MX/MPX | XS900MX | GS980M | IE200 | IE210L | IE300 | IE340 | IE510 | x210 | x220 | x230, x230L | x310 | IX5 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-66245** | **Update Manager** | With version 5.4.9-2.1, AR4050S firewalls did not receive updates from the Update Server.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – |

# What’s New in Version 5.4.9-2.1

Product families supported by this version:

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

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.9-2.1.

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

For instructions on how to upgrade to this version, see “Installing this Software Version” on page 94.

For instructions on how to update the web-based GUI, see “Installing and Accessing the Web-based GUI on AR-Series Devices” on page 99. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

| Models | Family | Date | Software File |
|---|---|---|---|
| AMF Cloud | | 11/2019 | vaa-5.4.9-2.1.iso (VAA OS)<br>vaa-5.4.9-2.1. vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.4.9-2.1.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 11/2019 | SBx81CFC960-5.4.9-2.1.rel |
| SBx908 GEN2 | SBx908 GEN2 | 11/2019 | SBx908NG-5.4.9-2.1.rel |
| x950-28XSQ<br>x950-28XTQm | x950 | 11/2019 | x950-5.4.9-2.1.rel |
| x930-28GTX<br>x930-28GPX<br>x930-52GTX<br>x930-52GPX<br>x930-28GSTX | x930 | 11/2019 | x930-5.4.9-2.1.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 11/2019 | x550-5.4.9-2.1.rel |
| x530-28GTXm<br>x530-28GPXm<br>x530L-52GPX | x530 and x530L | 11/2019 | x530-5.4.9-2.1.rel |
| x510-28GTX<br>x510-52GTX<br>x510-28GPX<br>x510-52GPX<br>x510-28GSX<br>x510-28GSX-80<br>x510DP-28GTX<br>x510DP-52GTX<br>x510L-28GT<br>x510L-28GP<br>x510L-52GT<br>x510L-52GP | x510 and x510L | 11/2019 | x510-5.4.9-2.1.rel |
| IX5-28GPX | IX5 | 11/2019 | IX5-5.4.9-2.1.rel |
| x310-26FT<br>x310-50FT<br>x310-26FP<br>x310-50FP | x310 | 11/2019 | x310-5.4.9-2.1.rel |
| x230-10GP<br>x230-10GT<br>x230-18GP<br>x230-18GT<br>x230-28GP<br>x230-28GT<br>x230L-17GT<br>x230L-26GT | x230 and x230L | 11/2019 | x230-5.4.9-2.1.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 11/2019 | x220-5.4.9-2.1.rel |
| IE510-28GSX | IE510-28GSX | 11/2019 | IE510-5.4.9-2.1.rel |
| IE340-20GP<br>IE340L-18GP | IE340 | 11/2019 | IE340-5.4.9-2.1.rel |
| IE300-12GT<br>IE300-12GP | IE300 | 11/2019 | IE300-5.4.9-2.1.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 11/2019 | IE210-5.4.9-2.1.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| IE200-6FT<br>IE200-6FP<br>IE200-6GT<br>IE200-6GP | IE200 | 11/2019 | IE200-5.4.9-2.1.rel |
| XS916MXT<br>XS916MXS | XS900MX | 11/2019 | XS900-5.4.9-2.1.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 11/2019 | GS980M-5.4.9-2.1.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 11/2019 | GS970-5.4.9-2.1.rel |
| GS924MX<br>GS924MPX<br>GS948MX<br>GS948MPX | GS900MX/MPX | 11/2019 | GS900-5.4.9-2.1.rel |
| FS980M/9<br>FS980M/9PS<br>FS980M/18<br>FS980M/18PS<br>FS980M/28<br>FS980M/28PS<br>FS980M/52<br>FS980M/52PS<br>FS980M/28DP | FS980M | 11/2019 | FS980-5.4.9-2.1.rel |

**Caution**: Software version 5.4.9-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.9 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 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

Please note, the 5.4.9-2.1 software version is ISSU incompatible with previous software versions.

# New Products

Version 5.4.9-2.1 supports the following upcoming and recently-released products.

## IE340-20GP and IE340L-18GP Industrial Ethernet Layer 3 Switches

Supported since IE340-20GP (5.4.9-1.1) and IE340L-18GP (5.4.9-1.4)

Allied Telesis ruggedized IE340 Industrial Ethernet switches are designed for harsh environments, such as those found in manufacturing, transportation and physical security. Key features include:

- Wide temperature range for harsh environments. IE340-20GP: -40°C to +75°C. IE340L-18GP: -40°C to +65°C
- Ethernet Protection Switched Ring (EPSRing™) and G.8032 ERPS support high-speed resilient ring-based networks
- Autonomous Management Framework (AMF) for network automation
- Routing capability (ECMP, OSPF, RIP, Static and BGP)
- Upstream Forwarding Only (UFO) for secure multi-user deployment
- Precise time synchronization with sub-microsecond resolution (IEEE 1588 PTP)
- 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.
- Continuous PoE ensures endpoint uptime, even during a switch firmware upgrade
- Active Fiber Monitoring prevents eavesdropping on fiber communications.

## FS980M/28DP Dual Power Supply Fast Ethernet Managed Access Switches

Supported since 5.4.9-1.1

The dual power supply model of the FS980M Series provides system and PoE redundancy to maximize network and end-point uptime. Key features include:

- Dual fixed PSUs to ensure System and PoE power redundancy, so critical powered devices remain online
- Autonomous Management Framework (AMF) for network automation
- Ethernet Protection Switched Ring (EPSRing™) and 4-unit VCStack, for high availability
- Static IPv4 routing and support for RIPv1 and RIPv2
- 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
- Edge security, including Multi Supplicant Authentication, IEEE 802.1x, RADIUS, TACACS+, Dynamic VLAN, Guest VLAN and ACLs.

# New Features and Enhancements

This section summarizes the new features in 5.4.9-2.1:

- "Autonomous Management Framework (AMF) Enhancements" on page 74
- "MACsec (Media Access Control Security)" on page 75
- "OSPF VRF-Lite capability" on page 76
- "SNMP Entity MIB enhancements" on page 76
- "Enabling the DHCP Snooping service on individual VLANs" on page 76
- "OpenFlow protocol v1.3 on x530 and x530L Series switches" on page 77
- "Stack up to eight units of x530 and x530L Series switches" on page 78
- "Storm control enhancements on x530 and x530L Series switches" on page 79
- "Keeping egress rate limiting at the same percentage of line rate as packet size changes" on page 79

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 89.

# Autonomous Management Framework (AMF) Enhancements

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

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

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

Version 5.4.9-2.1 includes the following AMF enhancements.

## AMF support for ONVIF Profile Q devices

From 5.4.9-2.1 onwards, AMF supports ONVIF (Open Network Video Interface Forum) Profile Q devices. This allows you to easily backup and restore ONVIF devices using the AMF backup system.

You configure an ONVIF device as an AMF guest node to allow AMF to manage it. The AMF node communicates with the device via HTTP, and only one device is allowed per port.

A new model type parameter **onvif** is available for setting the ONVIF guest node's guest-class. For example, to setup a guest-class for an ONVIF compliant camera with a static IP address, use the following commands:

```
awplus(config)# atmf guest-class camera
awplus(config-atmf-guest)# modeltype onvif
awplus(config-atmf-guest)# username admin password secret
awplus(config-atmf-guest)# http-enable
awplus(config-atmf-guest)# discovery static
```

ONVIF devices can also be configured with dynamic IP addresses using DHCP and DHCP snooping.

For more information on configuring ONVIF guest nodes, see the AMF Guestnode chapter in the AMF Feature Overview and Configuration Guide.

## AMF node recovery enhancements

From 5.4.9-2.1 onwards, automatic recovery will work for GS900MX/MPX series devices replaced with GS980MX series devices.

The full list of permitted substitutions are listed in the table below:

Table 2: Permitted device substitutions

| Original device type | Replacement device type | Supported from version* |
|---|---|---|
| x930 series | x950 series | 5.4.9-0.1 |
| x900 series | x930 series or<br>x950 series | 5.4.9-0.1 |
| x610 series | x530 series | 5.4.9-0.1 |
| x510 series | x530 series | 5.4.9-0.1 |
| IX5-28GPX | x530 series | 5.4.9-0.1 |
| x210 series | x230 series | 5.4.9-0.1 |
| GS900MX/MPX | GS980MX | 5.4.9-2.1 |

* The supported version needs to be running on the AMF master and the node's neighbor for the recovery to work.

## Copy command available in AMF provisioning mode

From 5.4.9-2.1 onwards, you can run the **copy** command from the AMF provisioning mode. The syntax is as follows:

```
awplus(atmf-provision)#copy <source-name> <destination-name>
```

For 5.4.9-x.x versions of AlliedWare Plus prior to 5.4.9-2.1 you need to use the **do** command to run the privilege exec **copy** command in AMF provisioning mode.

# MACsec (Media Access Control Security)

*Available on:*

- *x930 Series (front panel 1G ports)*
- *x950 (XEM2-12XS)*
- *SBx908GEN2 (XEM2-12XS)*

5.4.9-2.1 adds support for MACsec (Media Access Control Security) with preshared keys between 2 peers.

MACsec provides line-rate encryption and protection of traffic passing over a Layer 2 network or link. It protects all frames passing over the link, including Layer 2 protocols such as ARP. MACsec can provide the following services:

- Connectionless data integrity—ensures the frame has not been modified en route.
- Data origin authenticity—ensures the frame was sent by one of the MACsec peers.
- Confidentiality—encrypts the frame's EtherType and payload to ensure they cannot be read en route.
- Replay protection—ensures the same frame is not received more than once.

For more information about MACsec and how to configure it, see the MACsec Feature Overview and Configuration Guide.

## OSPF VRF-Lite capability

*Available on all AlliedWare Plus products that support VRF-Lite and OSPF*

OSPF instances configured inside VRF-Lite instances now operate as regular OSPF instances, without any VRF-specific behaviors such as the DN-bit or automatically operating as an ABR. This is because AW+ supports VRF-Lite rather than full VRF.

The new behavior is the equivalent of other vendors'"ospf capability vrf-lite" functionality, but in AlliedWare Plus you do not have to enter a command to enable the new behavior.

Also, the **domain-id** command has been removed from OSPF as it is not required for VRF-Lite.

For more information about VRF-Lite, see the VRF-Lite Feature Overview and Configuration Guide.

## SNMP Entity MIB enhancements

*Available on all AlliedWare Plus products*

From 5.4.9-2.1 onwards, the following public MIBs are supported:

- ENTITY-MIB (RFC 6933)

  Provides inventory information about the system as well as the physical ports that are present.
- ENTITY-SENSOR-MIB (RFC 3433)

  Provides information about the sensors that are present in the system and includes entries for all board and bay sensors in the system.
- ENTITY-STATE-MIB (RFC 4268)

  Provides information on the possible state attributes that could be tracked for a given entity.

For more information about MIBs, see the Support for Allied Telesis Enterprise MIBs in AlliedWare Plus Technical Guide and the SNMP Feature Overview and Configuration Guide.

## Enabling the DHCP Snooping service on individual VLANs

*Available on SBx908 GEN2, x950, x930, x510, x510L, IE510, IE340 and IE300 Series switches*

From 5.4.9-2.1 onwards, you can optionally enable the DHCP snooping service on a per-vlan basis, instead of enabling the DHCP snooping service globally.

## Enabling DHCP snooping globally

You can use the existing command **service dhcp-snooping** to enable the DHCP snooping service globally on your switch. When you enable it on the desired VLANs using the **ip dhcp snooping** command, your switch creates a global DHCP snooping Access Control List (ACL). This sends DHCP packets to the CPU for processing. Using this option, your switch forwards all DHCP traffic to the CPU, no matter what VLAN it belongs to.

## Enabling DHCP snooping per-vlan

You can use the new command service **dhcp-snooping per-vlan** instead of the command **service dhcp-snooping**. This option only creates an ACL for the VLANs that you configure with the **ip dhcp snooping** command. This limits the amount of DHCP traffic that is forwarded to the CPU. However, using this option creates an ACL for each VLAN that DHCP snooping is enabled on, so it is most suitable if you have a small number of VLANs. Use the **show platform classifier statistics utilization brief** command to see the number of ACLs available for your switch.

For more information about DHCP snooping, see the DHCP Snooping Feature Overview and Configuration Guide.

# OpenFlow protocol v1.3 on x530 and x530L Series switches

From 5.4.9-2.1 onwards, x530 and x530L Series switches support version 1.3 of the OpenFlow™ specification.

To ensure correct functionality, there are two platform commands to be aware of. The commands relate to Header modification and Flow entry consumption:

- platform sdn-route-ratio enhanced
- platform hwfilter-size ipv4-full-ipv6

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

## Header modification

On x530 and x530L Series switches, OpenFlow actions that carry out IP header alterations for IPv4 and IPv6 flows can consume two different hardware resources:

1. IP header alterations require Policy-based Routing functionality. By default, there are 127 Policy-based Routes available on the x530/x530L switch. We recommended you use the new platform command **platform sdn-route-ratio enhanced** to increase the limit to 1023 when using OpenFlow.

2. When modifying layer 3 or above headers, Header Alteration (HA) entries are required. There is a maximum of 1000 IPv4/v6 HA entries available for flows. These HA entries

are shared with ARPs, therefore if all shared resources are used by ARP it will no longer be possible for flows to use IP HA.

As well, OpenFlow may use Policy-based Routing entries to modify the MAC source address. For this, the switch uses a specialized table of 256 unique MAC addresses. You can use the command **show platform swtable siliconResource** to see how many of these MAC addresses are in use.

## Flow entry consumption

There are two factors that determine the number of flow entries consumed:

1. x530 Series switches convert ingress ACLs into IPv6 hardware entries and/or non-IPv6 hardware entries, depending on which fields the ACL matches:
   - For some ACLs, the switch can create only IPv6 or non-IPv6 hardware entries; it doesn't have to create both. For example, ACLs that match on IPv4 address result in non-IPv6 entries.
   - However, for some ACLs, the switch has to create both types of hardware entry, to make sure that all IPv6 and non-IPv6 traffic is matched. For example, ACLs that match on MAC address result in both types of entry.
2. If you need to match on source or destination IPv6 addresses, you must enter the command **platform hwfilter-size ipv4-full-ipv6** to enable this. When this command is enabled on an x530 or x530L Series switch, each IPv6 flow consumes twice the amount of hardware resource (i.e. twice the entry size) compared to an IPv4 flow.

Openflow has a default ingress ACL to trap packets to the CPU, which is translated into two hardware entries: an IPv6 entry and a non-IPv6 entry. With the default settings, these entries are both the same size. When you enable **platform hwfilter-size ipv4-full-ipv6**, the default Openflow rule will still be translated into two entries, but the IPv6 entry will be twice the size of the non-IPv6 entry and it will consume 3 hardware entries in total, rather than only 2 in the default mode.

## IPv6 forwarding

Note that IPv6 forwarding is disabled by default on all platforms. You need to enable IPv6 forwarding to allow Openflow to modify IPv6 flows properly, using the command **ipv6 forwarding**.

# Stack up to eight units of x530 and x530L Series switches

From 5.4.9-2.1 onwards, you can stack up to 8 units in a VCStack. With 40Gbps bandwidth for each unit, VCStack, in conjunction with link aggregation, provides a resilient highly available system where network resources are spread across stacked units.

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

## Storm control enhancements on x530 and x530L Series switches

From 5.4.9-2.1 (and also 5.4.9-1.3) onwards, you can set more than one storm control limit type at a time for x530 Series switches. For example, you can configure both broadcast and multicast levels on the same port at the same time.

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

## Keeping egress rate limiting at the same percentage of line rate as packet size changes

*Available on SBx908 GEN2 and x950 Series switches*

From 5.4.9-2.1 onwards, egress queue rate limiting can allow for the size of packet preamble and inter-packet gap (the "overhead"). This keeps the rate limit at the same percentage of line rate for all packet sizes. Otherwise, the percentage of line rate changes with packet size, because of the size of the overhead relative to smaller packets. This means smaller packets take up a larger percentage of the line rate.

To configure the new option, use the following new command in interface mode for the desired switch ports:

```
awplus(config-if)#egress-rate-limit overhead <bytes>
```

For standard ethernet packets, use a value of 20 bytes (8 bytes of preamble and a inter-packet gap of 12 bytes).

## Management-only VLANs

*Available on all AlliedWare Plus switches*

Management-only VLANs are VLANs that can only be used for managing the switch. They:

- have one and only one access port (no aggregators, trunk port etc.)
- do not route to/from other interfaces
- process packets in the CPU, rather than in hardware
- cannot be converted to a normal VLAN, nor can a normal VLAN be converted to a management-only VLAN. Delete and re-create the VLAN to convert a normal VLAN to/ from a management-only VLAN.

If you need to control ingress and egress traffic to and from management interfaces, you can use software-based ACLs to filter traffic to and from a management-only VLAN.

To create a management-only VLAN, use the command **vlan <vid> state management-only**. For example, to create VLAN100 as a management-only VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100 state management-only
```

# 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:

- TACACS+ and AAA commands that are unavailable in Secure Mode
- Change to when eth ports are treated as "up"
- DLF packets on IE200 Series switches
- Disabling PoE on a port on IE300 Series switches
- 3DES not longer supported for SSH
- Known issue in 5.4.9-1.1 and 5.4.9-1.2 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
- Changes in 5.4.9-1.1 to application list for the built-in deep packet inspection feature

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

- Software Release Licensing
- Upgrading a VCStack with reboot rolling
- Forming or extending a VCStack with auto-synchronization
- AMF software version compatibility
- Upgrading all devices in an AMF network

If you are upgrading from an earlier version than 5.4.9-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

## TACACS+ and AAA commands that are unavailable in Secure Mode

*Applies to all AlliedWare Plus switches that support Secure Mode*

In Secure Mode (the mode that is enabled with the command **crypto secure-mode**), TACACS+ is unavailable. This means the following commands are unavailable:

- the **group tacacs+** parameter of **aaa authentication login**
- **aaa authorization commands**
- **aaa authorization config-commands**
- **authorization commands**
- the **group tacacs+** parameter of **aaa accounting login**
- **aaa accounting commands**
- **aaa authentication enable default group tacacs+**
- **tacacs-server host**
- **tacacs-server key**
- **tacacs-server timeout**
- **ip tacacs source-interface**
- **show tacacs+**

## Change to when eth ports are treated as "up"

*Applies to AR-Series firewalls and routers*

Previously, ethernet (eth) interfaces would go into the "up" state early on in the bootup process. It was possible for them to reach the "running" state before the device's network configuration had finished applying.

This meant that during the start up process, ethernet interfaces could behave in a way that was different from the intended final device configuration. For example, if packets were sent by the device before the network configuration had finished applying, they would be dropped even though the Firewall configuration might intend them to be forwarded. One such packet type was IPv6 Router Solicitation packets, which might be dropped unintentionally.

This is no longer the case. From 5.4.9-2.2 onwards, ethernet interfaces are only put into the "up" state once the configuration has finished applying. This is the same as existing VLAN behaviour.

## DLF packets on IE200 Series switches

*Applies to IE200 Series switches only*

Previously, DLF (destination lookup failure) packets were flooded to the CPU on IE200 Series switches, which could impact CPU performance. From 5.4.9-1.5 onwards, these packets no longer go to the CPU.

## Disabling PoE on a port on IE300 Series switches

*Applies to IE300 Series switches only*

On an IE300 Series switch, you can use the command **no power-inline pair {data|spare} enable** to deactivate power on either the data or spare Ethernet pairs on ports 1.0.9-1.0.12. To completely disable PoE on this platform, you need to enter this command twice, specifying both the data and the spare pairs.

We do not recommend using the command **no power-inline enable** (without the pair, data or spare parameters) on these ports, because it will only disable the data pair, not both the data and spare pairs. However, from 5.4.9-2.1 onwards, if you do use the command **no power-inline enable**, that command will be saved in the configuration file.

## 3DES not longer supported for SSH

*Applies to all AlliedWare Plus devices*

Because 3DES is no longer considered secure, it has been removed from the supported cypher set for SSH. Modern clients and servers can continue to interoperate using AES-based cyphers transparently.

## Known issue in 5.4.9-1.1 and 5.4.9-1.2 when changing the password on a local radius user

*Applies to all AlliedWare Plus switches that support local RADIUS*

There is a known issue in software versions 5.4.9-1.1 and 5.4.9-1.2 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 was resolved in 5.4.9-1.3.

## 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.

# Changes in 5.4.9-1.1 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
- SomeIP
- VidTO
- WhatsApp Files
- YouTube Upload

## 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 90 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 92.

## 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 5.4.9-2.x from:

- 5.4.9-1.x
- 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 5.4.9-2.x from 5.4.4-0.x or earlier versions.

## Forming or extending a VCStack with auto-synchronization

*Applies to all stackable AlliedWare Plus switches*

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up. Auto-synchronization is supported between 5.4.9-2.x and:

- 5.4.9-1.x
- 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 5.4.9-2.x and 5.4.6-1.1 or **any** earlier releases.

## AMF software version compatibility

*Applies to all AlliedWare Plus devices*

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

### If using an AMF controller

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

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

### If using secure mode

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

### If using Vista Manager EX

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

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

### If using none of the above

If none of the above apply, then nodes running version 5.4.9-2.x are compatible with nodes running:

- 5.4.9-1.x
- 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 devices in an AMF network

*Applies to all AlliedWare Plus devices*

**This version supports upgrades across AMF networks.** There are two methods for upgrading firmware on an AMF network:

- Reboot-rolling, which upgrades and reboots each node in turn
- Distribute firmware, which upgrades each node, but does not reboot them. This lets you reboot the nodes at a minimally-disruptive time.

You can use either reboot-rolling or distribute firmware to upgrade to this software version, from 5.4.3-2.6 and later.

However, if you use reboot-rolling or distribute firmware to upgrade an AMF network, and any of the devices are running 5.4.7-1.1 or later, then you must initiate the upgrade from a device that is running 5.4.7-1.1 or later. Otherwise, the devices running 5.4.7-1.1 or later will not be upgraded.

If you are using rolling-reboot, we recommend limiting it to working-sets of 42 nodes or fewer.

In summary, the process for upgrading firmware on an AMF network is:

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
   a. create a working-set of the nodes you want to upgrade
   b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
   c. Check the console messages to make sure that all nodes are "release ready". If they are, follow the prompts to perform the upgrade.

# Obtaining User Documentation

For full AlliedWare Plus documentation, click here to visit our online Resource Library. For AlliedWare Plus products, the Library includes the following documents:

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

# Verifying the Release File

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

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

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

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

Caution

If the verification fails, the following error message will be generated:
**"% Verification Failed"**
**In the case of verification failure, please delete the release file and contact Allied Telesis support.**

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

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

# Licensing this Version on an SBx908 GEN2 Switch

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

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

### 1. Obtain the MAC address for a switch

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

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

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

### 2. Obtain a release license for a switch

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

### 3. Apply a release license on a switch

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

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

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

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

### 4. Confirm release license application

On a stand-alone switch, use the commands **show license** or **show license brief** to confirm release license application.

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

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches. The following example shows output on an SBx908 GEN2 switch:

```
awplus#show license

Board region: Global

Index                           : 1
License name                    : Base License
Customer name                   : Base License
Type of license                 : Full
License issue date              : 20-Mar-2019
Features included               : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                                  EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                                  L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                                  RADIUS-100, RIP, VCStack, VRRP

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

# Licensing this Version on an SBx8100 Series CFC960 Control Card

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

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

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

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

### 1. Obtain the MAC address for a control card

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

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

```
awplus#show system mac license

MAC address for licensing:


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

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

### 2. Obtain a release license for a control card

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

### 3. Apply a release license on a control card

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

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

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

```
11:04:56 awplus IMI[1696]: SFL: The current software is not licensed.
awplus#license certificate demo1.csv
A restart of affected modules may be required.
Would you like to continue? (y/n): y
11:58:14 awplus IMI[1696]: SFL: The current software is licensed. Exiting
unlicensed mode.

Stack member 1 installed 1 license

1 license installed.
```

**4. Confirm release license application**

On a stand-alone chassis, use the commands **show license** or **show license brief** to confirm release license application.

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

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

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

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

# Installing this Software Version

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 90 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 92.

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

1. Copy the software version file (.rel) onto your TFTP server.

2. If necessary, delete or move files to create space in the switch's Flash memory for the new file. To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

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

| Product | Command |
|---|---|
| SBx8100 with CFC960 | `awplus(config)# boot system SBx81CFC960-5.4.9-2.7.rel` |
| SBx908 GEN2 | `awplus(config)# boot system SBx908NG-5.4.9-2.7.rel` |
| x950 series | `awplus(config)# boot system x950-5.4.9-2.7.rel` |
| x930 series | `awplus(config)# boot system x930-5.4.9-2.7.rel` |
| x550 series | `awplus(config)# boot system x550-5.4.9-2.7.rel` |
| x530 series | `awplus(config)# boot system x530-5.4.9-2.7.rel` |
| x510 series | `awplus(config)# boot system x510-5.4.9-2.7.rel` |
| IX5-28GPX | `awplus(config)# boot system IX5-5.4.9-2.7.rel` |
| x320 series | `awplus(config)# boot system x320-5.4.9-2.7.rel` |
| x310 series | `awplus(config)# boot system x310-5.4.9-2.7.rel` |
| x230 series | `awplus(config)# boot system x230-5.4.9-2.7.rel` |
| x220 series | `awplus(config)# boot system x220-5.4.9-2.7.rel` |
| IE510-28GSX | `awplus(config)# boot system IE510-5.4.9-2.7.rel` |

| Product | Command |
|---|---|
| IE340 series | `awplus(config)# boot system IE340-5.4.9-2.7.rel` |
| IE300 series | `awplus(config)# boot system IE300-5.4.9-2.7.rel` |
| IE210L series | `awplus(config)# boot system IE210-5.4.9-2.7.rel` |
| IE200 series | `awplus(config)# boot system IE200-5.4.9-2.7.rel` |
| XS900MX series | `awplus(config)# boot system XS900-5.4.9-2.7.rel` |
| GS980EM series | `awplus(config)# boot system GS980EM-5.4.9-2.7.rel` |
| GS980M series | `awplus(config)# boot system GS980M-5.4.9-2.7.rel` |
| GS970M series | `awplus(config)# boot system GS970-5.4.9-2.7.rel` |
| GS900MX/ MPX series | `awplus(config)# boot system GS900-5.4.9-2.7.rel` |
| FS980M series | `awplus(config)# boot system FS980-5.4.9-2.7.rel` |
| AR4050S | `awplus(config)# boot system AR4050S-5.4.9-2.7.rel` |
| AR3050S | `awplus(config)# boot system AR3050S-5.4.9-2.7.rel` |
| AR2050V | `awplus(config)# boot system AR2050V-5.4.9-2.7.rel` |
| AR2010V | `awplus(config)# boot system AR2010V-5.4.9-2.7.rel` |
| AR1050V | `awplus(config)# boot system AR1050V-5.4.9-2.7.rel` |

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

```
awplus(config)# exit
awplus# show boot
```

6. Reboot using the new software version.

```
awplus# reload
```

# Installing and Accessing the Web-based GUI on Switches

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

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

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

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

## Check if the GUI is installed

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

### Browse to the GUI

Perform the following steps to browse to the GUI.

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

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

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

2. Open a web browser and browse to the IP address from step 1.

3. If you do not see a login page, you need to install the GUI, as described in "Install the GUI if it is not installed" on page 100. 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 5.4.9-2.7 is 2.7.1.

If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 100.

## Install the GUI if it is not installed

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

1. Obtain the GUI file from our Software Download center. The **file** to use with 5.4.9-2.7 is awplus-gui_549_22.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_22.gui flash
   ```

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

   ```
   awplus#dir
   ```

3. Delete any previous Java switch GUI files.

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

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

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

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

5. Make sure the HTTP service is running:

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

6. Log into the GUI:

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

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

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

## Update the GUI if it is not the latest version

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

1. Obtain the GUI file from our Software Download center. The file to use with 5.4.9-2.7 is awplus-gui_549_22.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_16.gui flash
   ```

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

   ```
   awplus#dir
   ```

3. Stop and restart the HTTP service:

   ```
   awplus# configure terminal
   ```

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

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

4. Log into the GUI:

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

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

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

# Installing and Accessing the Web-based GUI on AR-Series Devices

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

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

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

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

## Check if the GUI is installed

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

### Browse to the GUI

Perform the following steps to browse to the GUI.

**Prerequisite:** If the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

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

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

   Alternatively, you can use the default address on unconfigured devices, which is 192.168.1.1.

2. Open a web browser and browse to the IP address from step 1.

3. If you do not see a login page, you need to install the GUI, as described in "Install the GUI if it is not installed" on page 100. 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 5.4.9-2.7 is 2.7.1. If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 100.

## Install the GUI if it is not installed

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

1. If the device's firewall is enabled, create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

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

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

```
awplus# update webgui now
```

4. Make sure the HTTP service is running:

```
awplus# configure terminal

awplus(config)# service http
```

5. Log into the GUI:

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

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

## Update the GUI if it is not the latest version

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

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

```
awplus# update webgui now
```

2. Stop and restart the HTTP service:

```
awplus# configure terminal

awplus(config)# no service http

awplus(config)# service http
```

3. Log into the GUI:

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

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