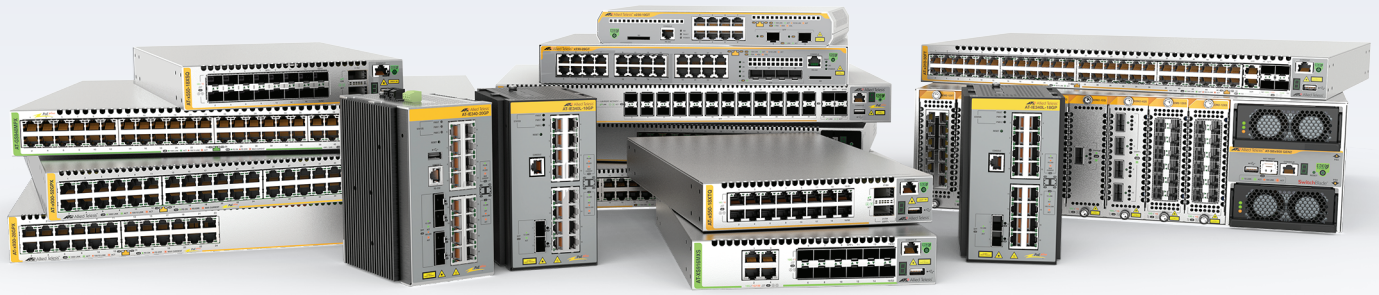
# Release Note for AlliedWare Plus Software Version 5.5.2-1.x



AlliedWare Plus OPERATING SYSTEM

AMF Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330-10GTX
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX/10
GS970M Series
10G Virtual UTM Firewall
AR4050S-5G
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

» 5.5.2-1.1 » 5.5.2-1.2 » 5.5.2-1.3 » 5.5.2-1.4 » 5.5.2-1.5

# 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/**


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

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

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

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by emailing **gpl@alliedtelesis.co.nz**.



## 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/**

# Contents


What's New in Version 5.5.2-1.5 ..... 1

Introduction ..... 1

Issues Resolved in Version 5.5.2-1.5 ..... 5

What's New in Version 5.5.2-1.4 ..... 9

Introduction ..... 9

New Features and Enhancements ..... 13

Issues Resolved in Version 5.5.2-1.4 ..... 16

What's New in Version 5.5.2-1.3 ..... 20

Introduction ..... 20

Issues Resolved in Version 5.5.2-1.3 ..... 24

What's New in Version 5.5.2-1.2 ..... 26

Introduction ..... 26

New Features and Enhancements ..... 29

Issues Resolved in Version 5.5.2-1.2 ..... 31

What's New in Version 5.5.2-1.1 ..... 34

Introduction ..... 34

New Features and Enhancements ..... 37

Important Considerations Before Upgrading ..... 46

Obtaining User Documentation ..... 54

Verifying the Release File ..... 54

Licensing this Version on an SBx908 GEN2 Switch ..... 55

Licensing this Version on an SBx8100 Series CFC960 Control Card ..... 57

Installing this Software Version ..... 59

Accessing and Updating the Web-based GUI ..... 61

# What's New in Version 5.5.2-1.5

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
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE Virtual UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-1.5.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 59.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 61. 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 | | 01/2023 | vaa-5.5.2-1.5.iso (VAA OS)<br>vaa-5.5.2-1.5.vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.5.2-1.5.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 01/2023 | SBx81CFC960-5.5.2-1.5.rel |
| SBx908 GEN2 | SBx908 GEN2 | 01/2023 | SBx908NG-5.5.2-1.5.rel |
| x950-28XSQ<br>x950-28XTQm<br>x950-52XSQ<br>x950-52XTQm | x950 | 01/2023 | x950-5.5.2-1.5.rel |
| x930-28GTX<br>x930-28GPX<br>x930-28GSTX<br>x930-52GTX<br>x930-52GPX | x930 | 01/2023 | x930-5.5.2-1.5.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 01/2023 | x550-5.5.2-1.5.rel |
| x530-10GHXm<br>x530-18GHXm<br>x530-28GTXm<br>x530-28GPXm<br>x530-52GTXm<br>x530-52GPXm<br>x530DP-28GHXm<br>x530DP-52GHXm<br>x530L-10GHXm<br>x530L-18GHXm<br>x530L-28GTX<br>x530L-28GPX<br>x530L-52GTX<br>x530L-52GPX | x530 and x530L | 01/2023 | x530-5.5.2-1.5.rel |
| x330-10GTX<br>x330-20GTX<br>x330-28GTX | x330 | 01/2023 | x330-5.5.2-1.5.rel |
| x320-10GH<br>x320-11GPT | x320 | 01/2023 | x320-5.5.2-1.5.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 | 01/2023 | x230-5.5.2-1.5.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 01/2023 | x220-5.5.2-1.5.rel |
| IE340-12GT<br>IE340-12GP<br>IE340-20GP<br>IE340L-18GP | IE340 | 01/2023 | IE340-5.5.2-1.5.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 01/2023 | IE210-5.5.2-1.5.rel |
| XS916MXT<br>XS916MXS | XS900MX | 01/2023 | XS900-5.5.2-1.5.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| GS980MX/10HSm<br>GS980MX/18HSm<br>GS980MX/28<br>GS980MX/28PSm<br>GS980MX/52<br>GS980MX/52PSm | GS980MX | 01/2023 | GS980MX-5.5.2-1.5.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 01/2023 | GS980EM-5.5.2-1.5.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 01/2023 | GS980M-5.5.2-1.5.rel |
| GS970EMX/10<br>GS970EMX/20<br>GS970EMX/28 | GS970EMX | 01/2023 | GS970EMX-5.5.2-1.5.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 01/2023 | GS970-5.5.2-1.5.rel |
| 10GbE Virtual UTM Firewall | vFW | 01/2023 | ATVSTAPL-1.7.1.iso and<br>vfw-x86_64-5.5.2-1.5.app |
| AR4050S<br>AR4050S-5G<br>AR3050S | AR-series UTM firewalls | 01/2023 | AR4050S-5.5.2-1.5.rel<br>AR3050S-5.5.2-1.5.rel |
| AR2050V<br>AR2010V<br>AR1050 V | AR-series VPN routers | 01/2023 | AR2050V-5.5.2-1.5.rel<br>AR2010V-5.5.2-1.5.rel<br>AR1050V-5.5.2-1.5.rel |

**Caution**: Software version 5.5.2-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-1.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 55 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 57.

# Unsupported devices

Version 5.5.2-1.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-1.5 software version is ISSU compatible with previous software versions.

# Issues Resolved in Version 5.5.2-1.5

This AlliedWare Plus maintenance version includes the following resolved issues:

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | SBx908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR4050-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77887** | **ACL** | Previously, adding a list of hardware ACLs on a switch could sometimes cause the switch to restart unexpectedly.<br>This issue has been resolved. | Y | Y | – | – | – | Y | Y | – | Y | – | Y | – | Y | Y | – | – | Y | – | – | – | – | – | – |
| **CR-77839** | **ACL** | Previously, ACLs could be installed incorrectly at startup in some cases leading to unexpected behaviour.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | – | – | Y | – | Y | – | – | Y | – | Y | – | – | – | – | – | Y | – | – | – | – | – | – | – |
| **CR-76935** | **AMF** | Previously, it was possible for AMF automatic node recovery to occasionally 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 | – |
| **CR-77837** | **DHCP Server** | This software update addresses the DHCP server vulnerability issues as stated in CVE-2022-2928 and CVE-2022-2929.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | Y | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-77626** | **ECMP Routing** | Previously, ECMP routing did not work correctly with the non-point-to-point interfaces as nexthop.<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-77459** | **Environmental Monitoring** | Previously, when creating an environment sensor trigger, an invalid node ID could lead to a strange error message.<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 | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | SBx908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR4050-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77630** | **Findme** | Previously, with **`findme trigger`** configured (or using findme as a CLI command), under some circumstances it was possible for the device to unexpectedly reboot.<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-77783** | **IGMP** | Previously, multicast routes were not correctly removed from the hardware table upon reception of an IGMP or MLD group leave message.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | Y | Y | Y | – | – | Y | – | Y | – | Y | – | – | – | Y | – | – | – | – | – | – | – |
| **CR-77844** | **MAC Thrashing** | Previously, when MAC thrash action was set to "port disable", the port would not show that MAC thrashing had been detected in the output of the **`show interface`** command.<br>This issue has been resolved. | Y | Y | – | – | – | Y | Y | – | Y | Y | Y | – | Y | Y | Y | – | Y | – | – | – | – | – | – |
| **CR-77777** | **Multicast Fowarding HW** | With this software update, an issue impacting the CPU performance associated with sending multicast packets has been resolved. | Y | Y | – | – | – | Y | Y | – | Y | – | Y | – | Y | Y | Y | – | Y | – | – | – | – | – | – |
| **CR-77725** | **PBR** | Previously, when deleting Policy-based Rules, an error message occured.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | – |
| **CR-78157** | **Pluggable Transceivers** | Previously, on insertion of a DAC cable, the link could flap before settling into the correct 'up' state.<br>This issue has been resolved. | Y | Y | – | – | – | – | – | – | Y | – | Y | – | Y | Y | Y | – | Y | – | – | – | – | – | – |
| **CR-75781** | **QoS** | Previously, the command **`set dscp`** entered within a QoS class-map was accepted but not added to the running-configuration.<br>This meant that if the configuration was saved this command would not be preserved over a reboot.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | – | – | Y | – | – | – | Y | – | Y | – | Y | – | – | – | Y | – | – | – | – | – | – | – |

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | SBx908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR4050-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-74574** | **QoS hardware** | Previously, the commands **`remark-map to new-dscp <num>`** and **`remark-map to new-bandwidth-class <class>`** would silently fail.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | Y | – | – | – | Y | Y | – | Y | – | Y | – | Y | Y | Y | Y | Y | – | – | – | – | – | – |
| **CR-77793** | **SSH** | Previously, known SSH hosts could not be saved properly, resulting in requiring typing in "yes" for accepting connection to hosts that were previously connected.<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 | – |
| **CR-77872** | **SSH** | Previously, to negate the command: **`ssh server secure-kex exclude-nist-curves`**, to the default setting, you would need to unset the NIST-curve exclusion by using the command: **`ssh server secure-kex`**, then execute the command: **`no ssh server secure-kex`**.<br>With this software update, it is now possisle to return the SSH server key exchange to the default value, by using the command: **`no ssh server secure-kex`**.<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 | – |

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | SBx908 GEN2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR4050-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ER-5172** | **SSH** | With this software update, there are new commands to allow you to enable SSH-RSA for connecting to legacy devices.<br>The new commands are:<br>■ **`(no) ssh server allow-legacy-ssh-rsa`**<br>Use this command to enable/disable the legacy SSH-RSA scheme for AW+ SSH server.<br>■ **`(no) ssh client allow-legacy-ssh-rsa`**<br>Use this command to enable/disable the legacy SSH-RSA scheme for AW+ SSH client.<br>The use of SSH-RSA scheme is disabled by default for both server and client.<br>**Note**: We don't recommend enabling SSH-RSA, because it reduces security. | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-77548** | **VCStack** | Previously, when two stack masters were joined, a duplicate master event should occur and one stack member would reboot.<br>In rare circumstances, the other master would also unnecessarily reboot.<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-77682** | **VCStack** | Previously, late joining stack members would sometimes reboot unexpectedly.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | Y | Y | – | – | – | – | Y | – | Y | – | – | – | Y | – | – | – | – | – | – | – |
| **CR-77852** | **VCStack** | Previously, when a VCS+ duplicate master event occurred, the two VCS+ chassis could struggle to correctly rejoin or recover.<br>This issue has been resolved.<br>ISSU: Effective when ISSU complete. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – |

# What's New in Version 5.5.2-1.4

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
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE Virtual UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-1.4.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 59.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 61. 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 | | 11/2022 | vaa-5.5.2-1.4.iso (VAA OS)<br>vaa-5.5.2-1.4.vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.5.2-1.4.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 11/2022 | SBx81CFC960-5.5.2-1.4.rel |
| SBx908 GEN2 | SBx908 GEN2 | 11/2022 | SBx908NG-5.5.2-1.4.rel |
| x950-28XSQ<br>x950-28XTQm<br>x950-52XSQ<br>x950-52XTQm | x950 | 11/2022 | x950-5.5.2-1.4.rel |
| x930-28GTX<br>x930-28GPX<br>x930-28GSTX<br>x930-52GTX<br>x930-52GPX | x930 | 11/2022 | x930-5.5.2-1.4.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 11/2022 | x550-5.5.2-1.4.rel |
| x530-10GHXm<br>x530-18GHXm<br>x530-28GTXm<br>x530-28GPXm<br>x530-52GTXm<br>x530-52GPXm<br>x530DP-28GHXm<br>x530DP-52GHXm<br>x530L-10GHXm<br>x530L-18GHXm<br>x530L-28GTX<br>x530L-28GPX<br>x530L-52GTX<br>x530L-52GPX | x530 and x530L | 11/2022 | x530-5.5.2-1.4.rel |
| x330-10GTX<br>x330-20GTX<br>x330-28GTX | x330 | 11/2022 | x330-5.5.2-1.4.rel |
| x320-10GH<br>x320-11GPT | x320 | 11/2022 | x320-5.5.2-1.4.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 | 11/2022 | x230-5.5.2-1.4.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 11/2022 | x220-5.5.2-1.4.rel |
| IE340-12GT<br>IE340-12GP<br>IE340-20GP<br>IE340L-18GP | IE340 | 11/2022 | IE340-5.5.2-1.4.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 11/2022 | IE210-5.5.2-1.4.rel |
| XS916MXT<br>XS916MXS | XS900MX | 11/2022 | XS900-5.5.2-1.4.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| GS980MX/10HSm<br>GS980MX/18HSm<br>GS980MX/28<br>GS980MX/28PSm<br>GS980MX/52<br>GS980MX/52PSm | GS980MX | 11/2022 | GS980MX-5.5.2-1.4.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 11/2022 | GS980EM-5.5.2-1.4.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 11/2022 | GS980M-5.5.2-1.4.rel |
| GS970EMX/10<br>GS970EMX/20<br>GS970EMX/28 | GS970EMX | 11/2022 | GS970EMX-5.5.2-1.4.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 11/2022 | GS970-5.5.2-1.4.rel |
| 10GbE Virtual UTM Firewall | vFW | 11/2022 | ATVSTAPL-1.7.1.iso and<br>vfw-x86_64-5.5.2-1.4.app |
| AR4050S<br>AR4050S-5G<br>AR3050S | AR-series UTM firewalls | 11/2022 | AR4050S-5.5.2-1.4.rel<br>AR3050S-5.5.2-1.4.rel |
| AR2050V<br>AR2010V<br>AR1050 V | AR-series VPN routers | 11/2022 | AR2050V-5.5.2-1.4.rel<br>AR2010V-5.5.2-1.4.rel<br>AR1050V-5.5.2-1.4.rel |

**Caution**: Software version 5.5.2-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-1.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 55 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 57.

## Unsupported devices

Version 5.5.2-1.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-1.4 software version is ISSU compatible with previous software versions.

# New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.2-1.4:

## Stricter process control

*Available on all AlliedWare Plus device*

**CR-77554** This software update provides a new feature where **edit**, **activate** and several other associated commands have more strict process control. Shell scripts are now prevented from accessing certain sensitive system files, and the **edit** command is also prevented from accessing sensitive system files.

File and directory manipulation commands, show file commands, copy, move, delete file commands, show command redirections, and trigger scripting may also be put under strict user process control.

The affected commands and command types are:

- activate <*script-name*>
- copy [force] <*source-name*> <*destination-name*>
- copy FILE zmodem
- copy FILE startup-config
- copy current-software FILE
- copy running-config FILE
- copy startup-config FILE
- copy buffered-log FILE
- copy permanent-log FILE
- delete FILE
- edit (FILE|)
- move <*source-name*> <*destination-name*>
- mkdir FILE
- rmdir FILE
- show file FILE
- show commands with output redirection
- trigger running shell scripts

**New command** In order to maintain backward compatibility, the functionality is disabled by default and enabled using a new command. This command prompts for a new password before it takes effect. This password is then required in order to disable the functionality. Privileged system managers will not be able to access sensitive system files without access to this password.

The new command is:

```
awplus(config)# (no) strict-user-process-control
```

**Command usage**

When the  command is configured to enable the feature it will prompt for a password and a password confirmation. A new password, separate from any existing privileged management passwords, should be entered. This password should be stored carefully and securely as it will be required to disable the feature using the 'no' form of the command. This command must be entered from a physical console. Adding/deleting the 'strict-user-process-control' command to/from saved configuration file will not affect the running status of the feature.  For additional security, entering the command from a remote login session is not allowed.

Use the command **show running-config** to confirm the status of the feature. If the feature is running, the output will contain the command **strict-user-procdess-control**.

ISSU: Effective when CFCs upgraded.

# VRF improvements

*Available on all AlliedWare Plus devices that support VRF-lite*

From software version 5.5.2-1.4 onwards, the following services are supported within VRF instances:

- SNMP server
- NTP server and client
- sFlow agent
- SSH client

Prior to this release, these service were supported within the Global VRF domain only.

## Examples

To configure an SNMP server to only respond to requests from SNMP managers residing within VRF 'red':

```
awplus(config)# snmp-server vrf red
```

To configure NTP to communicate with an NTP server residing within VRF 'red':

```
awplus(config)# ntp server 10.0.0.1 vrf red
```

To configure the sFlow Agent to send samples to an sFlow Collector residing within VRF 'red':

```
awplus(config)# sflow collector id 1 ip 10.0.0.1 vrf red
```

Alongside the existing Privileged Exec mode SSH client commands, a new Global Configuration mode SSH client command has been added.

```
awplus(config)# ssh client vrf <vrf-name>
```

To configure the SSH client to use VRF 'red' for SSH clients:

```
awplus#(config)# ssh client vrf red
```

For more information about:

- **SSH** - see the SSH Feature Overview and Configuration Guide
- **NTP** - see the NTP Feature Overview and Configuration Guide
- **sFlow** - see the sFlow Feature Overview and Configuration Guide
- **SNMP** - see the SNMP Feature Overview and Configuration Guide
- **VRF-lite** - see the VRF-lite Feature Overview and Configuration Guide

# Issues Resolved in Version 5.5.2-1.4

This AlliedWare Plus maintenance version includes the following resolved issues:

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR3040S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77632** | **ARP / Neighbor Discovery, EPSR, MAC Thrashing, VCStack** | Previously, it was possible for EPSR blocking to be defeated for ARP packets (request and reply) ingressing a port on a VCS stack if the ingress port was on the backup member.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded | Y | – | – | – | – | – | Y | – | – | – | Y | – | Y | Y | Y | – | Y | – | – | – | – | – | – |
| **CR-77601** | **DHCP Relay** | Previously, if DHCP-Relay received a BOOTREQUEST packet from an upstream relay interface, it might result in temporary lost of DHCP-Relay service.<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-77680** | **IPv4** | Previously, when IP directed-broadcast was enabled on an interface, Layer 3 broadcast packets were duplicated to the local 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 | – |
| **CR-72122** | **IPv4** | Previously, directed broadcast packets were dropped on an interface even though the **`ip directed-broadcast`** command was configured on the 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 | – |
| **CR-77845** | **LLDP** | Previously, packets that were not LLDP and were sent to multicast addresses: 01:80:c2:00:00:0e, 01:80:c2:00:00:03, 01:80:c2:00:00:00 , would cause the following log message:<br>'Unrecognised ethernet type'.<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 | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR3040S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77620** | **OSPF** | Previously, on rarely occassions in large OSPF networks, when the SPF calculation was performed periodically, it could cause a device to restart.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | Y | Y | Y | Y | Y | – |
| **CR-77739** | **Pluggable Transceivers** | Previously, under rare circumstances, a fiber SFP in the combo port of a x930-GSTX would not come up at startup.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – |
| **CR-75846** | **Pluggable Transceivers** | Previously, on the x950 series and SBx908 GEN2, on rare occasions, entering the **`show platform port`** command could cause a 10G copper port to go down then back up.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | Y | – | – | – | – | – | – |
| **CR-77423** | **Port Authentication** | Previously, sometimes with MAC-based Port Authentication, a supplicant could become unauthenticated immediately after being authenticated.<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 | – |
| **CR-77500** | **QoS** | Previously, disabling MLS QoS might cause a line card on a SBx8100 to reboot.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – |
| **CR-77732** | **sFlow** | Previously, in a VCStack environment where sFLow was configured, a stack master failover might cause the backup member 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 | – | – | – | – | – | – |
| **CR-77740** | **SSH** | With this software update, the default VTY limit has been raised from 5 to 8 to ensure SSH access is still possible when a GUI session is in heavy 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 | – |

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR3040S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77416** | **SSH, TACACS+** | Previously, TACACS+ user login via SSH was only successful at every second attempt. The first login attempt would 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 | – |
| **CR-77450** | **TACACS+** | Previously, if a TACACS+ key contained the character hash '#', the communication between the AlliedWare Plus device and the TACACS+ server could fail.<br>This issue has been resolved by not allowing '#' in a TACACS+ key.<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 | – |
| **CR-77619** | **VCStack** | Previously, during a rolling reboot , a "*stack not formed after rolling reboot*" message could be output during a normal reboot.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – |
| **CR-77251** | **VCStack** | Previously, on x330/GS970EMX VCStack devices using the 10G Copper Ports as static aggregator ports to an upstream device, it was possible for a link flap to occur on the 10G Copper Ports used as part of the aggregator when a stack member rejoined the stack.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | Y | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-77593** | **VCStack** | Previously, when a stack had been up for between approx 100 and 200 days, a rebooted stack member would not be able to rejoin the stack unless the entire stack was rebooted.<br>This issue has been resolved. | Y | Y | – | Y | Y | – | – | – | – | Y | Y | Y | Y | Y | – | Y | – | – | – | – | – | – | – |

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR3040S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77597** | **VRRP, VCStack** | Previously, a late joining card or stack member could have ACLs previously configured on aggregators applied globally to the card/member instead.<br>Also, previously, on a x530 stack, ACLs configured on aggregators with member ports on a late joining member could have those ACLs incorrectly applied, especially if different ACLs were applied to different aggregators.<br>These issues have been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | Y | Y | – | – | – | – | Y | – | Y | – | – | – | Y | – | – | – | – | – | – | – |

# What's New in Version 5.5.2-1.3

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
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE Virtual UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-1.3.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 59.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 61. 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 | | 09/2022 | vaa-5.5.2-1.3.iso (VAA OS)<br>vaa-5.5.2-1.3.vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.5.2-1.3.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 09/2022 | SBx81CFC960-5.5.2-1.3.rel |
| SBx908 GEN2 | SBx908 GEN2 | 09/2022 | SBx908NG-5.5.2-1.3.rel |
| x950-28XSQ<br>x950-28XTQm<br>x950-52XSQ<br>x950-52XTQm | x950 | 09/2022 | x950-5.5.2-1.3.rel |
| x930-28GTX<br>x930-28GPX<br>x930-28GSTX<br>x930-52GTX<br>x930-52GPX | x930 | 09/2022 | x930-5.5.2-1.3.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 09/2022 | x550-5.5.2-1.3.rel |
| x530-10GHXm<br>x530-18GHXm<br>x530-28GTXm<br>x530-28GPXm<br>x530-52GTXm<br>x530-52GPXm<br>x530DP-28GHXm<br>x530DP-52GHXm<br>x530L-10GHXm<br>x530L-18GHXm<br>x530L-28GTX<br>x530L-28GPX<br>x530L-52GTX<br>x530L-52GPX | x530 and x530L | 09/2022 | x530-5.5.2-1.3.rel |
| x330-10GTX<br>x330-20GTX<br>x330-28GTX | x330 | 09/2022 | x330-5.5.2-1.3.rel |
| x320-10GH<br>x320-11GPT | x320 | 09/2022 | x320-5.5.2-1.3.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 | 09/2022 | x230-5.5.2-1.3.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 09/2022 | x220-5.5.2-1.3.rel |
| IE340-12GT<br>IE340-12GP<br>IE340-20GP<br>IE340L-18GP | IE340 | 09/2022 | IE340-5.5.2-1.3.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 09/2022 | IE210-5.5.2-1.3.rel |
| XS916MXT<br>XS916MXS | XS900MX | 09/2022 | XS900-5.5.2-1.3.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| GS980MX/10HSm<br>GS980MX/18HSm<br>GS980MX/28<br>GS980MX/28PSm<br>GS980MX/52<br>GS980MX/52PSm | GS980MX | 09/2022 | GS980MX-5.5.2-1.3.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 09/2022 | GS980EM-5.5.2-1.3.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 09/2022 | GS980M-5.5.2-1.3.rel |
| GS970EMX/10<br>GS970EMX/20<br>GS970EMX/28 | GS970EMX | 09/2022 | GS970EMX-5.5.2-1.3.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 09/2022 | GS970-5.5.2-1.3.rel |
| 10GbE Virtual UTM Firewall | vFW | 09/2022 | ATVSTAPL-1.7.1.iso and<br>vfw-x86_64-5.5.2-1.3.app |
| AR4050S<br>AR4050S-5G<br>AR3050S | AR-series UTM firewalls | 09/2022 | AR4050S-5.5.2-1.3.rel<br>AR3050S-5.5.2-1.3.rel |
| AR2050V<br>AR2010V<br>AR1050 V | AR-series VPN routers | 09/2022 | AR2050V-5.5.2-1.3.rel<br>AR2010V-5.5.2-1.3.rel<br>AR1050V-5.5.2-1.3.rel |

**Caution**: Software version 5.5.2-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-1.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 55 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 57.

# Unsupported devices

Version 5.5.2-1.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-1.3 software version is ISSU compatible with previous software versions.

# Issues Resolved in Version 5.5.2-1.3

This AlliedWare Plus maintenance version includes the following resolved issues:

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR3040S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-75715** | **ARP Neighborhood Discovery** | Previously, the entries created by **`arp-mac-disparity unicast`** were not VLAN aware and could affect traffic on other VLANs.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | – | Y | – | – | – | – | – | – |
| **CR-77424** | **DHCP Server VRF-lite** | Previously, the output for the command: **`show ip dhcp binding vrf <vrf-name>`** would show the global VRF static entries in addition to dynamic entries for the specified VRF.<br>This issue has been resolved.<br>ISSU: Effective when CFCs upgraded. | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | Y | Y | Y | – | Y | Y | Y | Y | – |
| **CR-77413** | **Environmental Monitoring PoE** | Previously, when the PoE load caused the fans to be running at a high speed and the ambient temperature crossed a threshold, the fan speed could unexpectedly be reduced.<br>This issue has been resolved so that the fan speed remains high as long as there is a high PoE load. | Y | – | Y | Y | Y | – | – | Y | Y | Y | Y | Y | Y | – | – | – | – | – | – | – | – | – | – |
| **CR-77502** | **Firewall GUI** | Previously, statistics monitoring was not operating correctly for the firewall history.<br>This issue is now resolved and the firewall history is correctly monitored. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | Y | Y | Y | Y | – |
| **CR-76101** | **PoE** | Previously, a PD could request more power than was allowed for its class.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – |
| **CR-77060** | **Switching** | Previously, using the SP10TM module at 2.5Gbps could result in a small amount of frame loss.<br>This issue has been resolved. | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | – | – | – | – | – |

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR3040S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-76264** | **VCStack** | Previously, on occasion, x330 Series stack ports installed with optical fibre SFP+ pluggables could fail to link up following a failover.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – |
| **CR-76178** | **STP Static Aggregators** | Previously, using static aggregators on a stack with spanning tree could result in ports being blocked at startup.<br>This issue has been resolved. | – | Y | – | – | – | – | – | – | – | – | Y | – | Y | Y | Y | – | Y | – | – | – | – | – | – |

# What's New in Version 5.5.2-1.2

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
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE Virtual UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-1.2.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 59.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 61. 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 | | 09/2022 | vaa-5.5.2-1.2.iso (VAA OS)<br>vaa-5.5.2-1.2.vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.5.2-1.2.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 09/2022 | SBx81CFC960-5.5.2-1.2.rel |
| SBx908 GEN2 | SBx908 GEN2 | 09/2022 | SBx908NG-5.5.2-1.2.rel |
| x950-28XSQ<br>x950-28XTQm<br>x950-52XSQ<br>x950-52XTQm | x950 | 09/2022 | x950-5.5.2-1.2.rel |
| x930-28GTX<br>x930-28GPX<br>x930-28GSTX<br>x930-52GTX<br>x930-52GPX | x930 | 09/2022 | x930-5.5.2-1.2.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 09/2022 | x550-5.5.2-1.2.rel |
| x530-10GHXm<br>x530-18GHXm<br>x530-28GTXm<br>x530-28GPXm<br>x530-52GTXm<br>x530-52GPXm<br>x530DP-28GHXm<br>x530DP-52GHXm<br>x530L-10GHXm<br>x530L-18GHXm<br>x530L-28GTX<br>x530L-28GPX<br>x530L-52GTX<br>x530L-52GPX | x530 and x530L | 09/2022 | x530-5.5.2-1.2.rel |
| x330-10GTX<br>x330-20GTX<br>x330-28GTX | x330 | 09/2022 | x330-5.5.2-1.2.rel |
| x320-10GH<br>x320-11GPT | x320 | 09/2022 | x320-5.5.2-1.2.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 | 09/2022 | x230-5.5.2-1.2.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 09/2022 | x220-5.5.2-1.2.rel |
| IE340-12GT<br>IE340-12GP<br>IE340-20GP<br>IE340L-18GP | IE340 | 09/2022 | IE340-5.5.2-1.2.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 09/2022 | IE210-5.5.2-1.2.rel |
| XS916MXT<br>XS916MXS | XS900MX | 09/2022 | XS900-5.5.2-1.2.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| GS980MX/10HSm<br>GS980MX/18HSm<br>GS980MX/28<br>GS980MX/28PSm<br>GS980MX/52<br>GS980MX/52PSm | GS980MX | 09/2022 | GS980MX-5.5.2-1.2.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 09/2022 | GS980EM-5.5.2-1.2.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 09/2022 | GS980M-5.5.2-1.2.rel |
| GS970EMX/10<br>GS970EMX/20<br>GS970EMX/28 | GS970EMX | 09/2022 | GS970EMX-5.5.2-1.2.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 09/2022 | GS970-5.5.2-1.2.rel |
| 10GbE Virtual UTM Firewall | vFW | 09/2022 | ATVSTAPL-1.7.1.iso and<br>vfw-x86_64-5.5.2-1.2.app |
| AR4050S<br>AR4050S-5G<br>AR3050S | AR-series UTM firewalls | 09/2022 | AR4050S-5.5.2-1.2.rel<br>AR3050S-5.5.2-1.2.rel |
| AR2050V<br>AR2010V<br>AR1050 V | AR-series VPN routers | 09/2022 | AR2050V-5.5.2-1.2.rel<br>AR2010V-5.5.2-1.2.rel<br>AR1050V-5.5.2-1.2.rel |

**Caution**: Software version 5.5.2-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-1.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 55 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 57.

## Unsupported devices

Version 5.5.2-1.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-1.2 software version is ISSU compatible with previous software versions.

# New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.2-1.2:

## SSH and secure key exchange algorithms

**CR-77520** In this release, an optional new parameter **exclude-nist-curves** has been added to the command **ssh server secure-kex**. The new parameter allows you to specify only key exchange algorithms which are currently considered as best current practice to be used by the SSH server.

The new syntax is:

```
ssh server secure-kex [exclude-nist-curves|]
```

If **exclude-nist-curves** is specified, NIST based curves key exchange algorithms are excluded from the list of allowable key exchange algorithms used by the SSH server. This means the following algorithms are used:

- curve25519-sha256@libssh.org
- diffie-hellman-group-exchange-sha256

Also this release introduces a new command **(no) ssh server secure-hostkey** that allows you to exclude NIST curves based hostkey algorithms.

If this command is specified, the hostkey algorithms used by the SSH server will be:

- ssh-ed25519
- rsa-sha2-256
- rsa-sha2-512

Consequently, there is a change of definition for the **ssh server secure-algs** command. In this release, the command also implicitly enables **ssh server secure-hostkey**.

Also note that if the command **ssh server secure-kex exclude-nist-curves** is specified along with all of the following commands:

```
ssh server secure-mac
ssh server secure-ciphers
ssh server secure-hostkey
```

they are not equal to the command **ssh server secure-algs**.

The command **ssh server secure-algs** is equivalent to the following commands being specified:

```
ssh server secure-kex
ssh server secure-mac
ssh server secure-ciphers
ssh server secure-hostkey
```

Another enhancement included with this software release, is the ability for AlliedWare Plus devices to auto-generate the ed25519 hostkey automatically, if it does not exist on the device. Also, you can create ed25519 hostkey/userkey pairs manually, using the following new commands:

```
crypto key generate hostkey ed25519
crypto key generate userkey USERNAME ed25519
```

and destroy the key using the commands:

```
crypto key destroy hostkey (rsa|ecdsa|ed25519)
crypto key destroy userkey USERNAME (rsa|dsa|rsa1|ecdsa|
ed25519)
```

Lastly, both the AlliedWare Plus SSH server and client now also include the ED25519 hostkey algorithm as the default hostkey algorithm used in SSH communication.

ISSU: Effective when CFCs upgraded.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 54.

# Issues Resolved in Version 5.5.2-1.2

This AlliedWare Plus maintenance version includes the following resolved issues:

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR4050S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77518** | **API** | Previously, if you opened a web-shell session from the device GUI and then logged out of the device GUI, the browser would request basic authentication credentials for the shell.<br>If these were entered, the browser would cache the basic authentication credentials and send them with all future HTTPS requests to the device while the browser remained open, even if this was not necessary (due to form authentication for the GUI).<br>This issue has been resolved. The web-shell no longer sets the header that induces the browser to request basic authentication credentials after the device GUI is logged out.<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 | – |
| **CR-73756** | **Environmental Monitoring** | Previously, on the x530 Series, it was possible for some temperature sensors to get hot enough to trigger temperature alarms without the fan RPM increasing.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – |
| **CR-77533** | **Environmental Monitoring** | Previously, it was possible for an IE340 device to encounter an exception error at startup. | – | – | – | – | – | – | Y | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – |

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR4050S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-77493** | **HTTP Service** | With this software update, HTTPS access to Alliedware Plus devices has been enhanced to use only strong ciphersuites. The ciphersuites supported from this release and onward are:<br>■ ECDHE-ECDSA-AES128-GCM-SHA256<br>■ ECDHE-RSA-AES128-GCM-SHA256<br>■ ECDHE-ECDSA-AES256-GCM-SHA384<br>■ ECDHE-RSA-AES256-GCM-SHA384<br>■ DHE-RSA-AES128-GCM-SHA256<br>■ DHE-RSA-AES256-GCM-SHA384 I<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 | – |
| **CR-77445** | **Multicast Routing** | Previously, if **`ipv6 mld snooping`** was disabled, IPv6 multicast routing would not recover after a network outage.<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 | – |
| **CR-77504** | **SSL** | This software update addresses an SSL vulnerability as specified in CVE-2021-3712.<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 | – |
| **CR-77534** | **SSL** | This software update addresses an SSL vulnerability as specified in CVE-2022-2068.<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 | – |
| **CR-77084** | **System** | This software update addresses a file system vulnerability as specified in CVE-2022-1348.<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 | – |
| **CR-77468** | **System** | This software update addresses a linux kernel vulnerability as specified in CVE-2022-0185.<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 | – |
| **CR-77469** | **System** | This software update addresses a file system vulnerability as specified in CVE-2019-5188.<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 | – |

| CR | Module | Description | GS970M/EMX | XS900MX | GS980M | GS980MX | GS980EM | IE210L | IE340 | x220 | x230, x230L | x320 | x330 | x510, 510L | x530, x530L | x550 | x930 | x950 | SBx8100 CFC960 | x908Gen2 | AR1050V | AR2010V | AR2050V | AR3050S/AR4050S | AR4050S-5G | AMF Cloud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CR-75835** | **VCStack** | Previously, it was possible for packet corruption to occur on the stack links, resulting in the packet being discarded with an FCS error.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | Y | – | – | – | – | – | – |
| **CR-77530** | **VCStack** | Previously, it was possible for an x950 or SBx908NG stack to restart unexpectedly during MAC address learning and aging.<br>This issue has been resolved. | – | – | – | – | – | – | – | – | – | – | – | – | – | – | – | Y | – | Y | – | – | – | – | – | – |

# What's New in Version 5.5.2-1.1

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
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE Virtual UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

# Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-1.1.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 59.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 61. 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 | | 07/2022 | vaa-5.5.2-1.1.iso (VAA OS)<br>vaa-5.5.2-1.1.vhd and upload_vhd.py (for AWS)<br>vaa_azure-5.5.2-1.1.vhd (for Microsoft Azure) |
| SBx81CFC960 | SBx8100 | 07/2022 | SBx81CFC960-5.5.2-1.1.rel |
| SBx908 GEN2 | SBx908 GEN2 | 07/2022 | SBx908NG-5.5.2-1.1.rel |
| x950-28XSQ<br>x950-28XTQm<br>x950-52XSQ<br>x950-52XTQm | x950 | 07/2022 | x950-5.5.2-1.1.rel |
| x930-28GTX<br>x930-28GPX<br>x930-28GSTX<br>x930-52GTX<br>x930-52GPX | x930 | 07/2022 | x930-5.5.2-1.1.rel |
| x550-18SXQ<br>x550-18XTQ<br>x550-18XSPQm | x550 | 07/2022 | x550-5.5.2-1.1.rel |
| x530-10GHXm<br>x530-18GHXm<br>x530-28GTXm<br>x530-28GPXm<br>x530-52GTXm<br>x530-52GPXm<br>x530DP-28GHXm<br>x530DP-52GHXm<br>x530L-10GHXm<br>x530L-18GHXm<br>x530L-28GTX<br>x530L-28GPX<br>x530L-52GTX<br>x530L-52GPX | x530 and x530L | 07/2022 | x530-5.5.2-1.1.rel |
| x330-10GTX<br>x330-20GTX<br>x330-28GTX | x330 | 07/2022 | x330-5.5.2-1.1.rel |
| x320-10GH<br>x320-11GPT | x320 | 07/2022 | x320-5.5.2-1.1.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 | 07/2022 | x230-5.5.2-1.1.rel |
| x220-28GS<br>x220-52GT<br>x220-52GP | x220 | 07/2022 | x220-5.5.2-1.1.rel |
| IE340-12GT<br>IE340-12GP<br>IE340-20GP<br>IE340L-18GP | IE340 | 07/2022 | IE340-5.5.2-1.1.rel |
| IE210L-10GP<br>IE210L-18GP | IE210L | 07/2022 | IE210-5.5.2-1.1.rel |
| XS916MXT<br>XS916MXS | XS900MX | 07/2022 | XS900-5.5.2-1.1.rel |

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

| Models | Family | Date | Software File |
|---|---|---|---|
| GS980MX/10HSm<br>GS980MX/18HSm<br>GS980MX/28<br>GS980MX/28PSm<br>GS980MX/52<br>GS980MX/52PSm | GS980MX | 07/2022 | GS980MX-5.5.2-1.1.rel |
| GS980EM/10H<br>GS980EM/11PT | GS980EM | 07/2022 | GS980EM-5.5.2-1.1.rel |
| GS980M/52<br>GS980M/52PS | GS980M | 07/2022 | GS980M-5.5.2-1.1.rel |
| GS970EMX/10<br>GS970EMX/20<br>GS970EMX/28 | GS970EMX | 07/2022 | GS970EMX-5.5.2-1.1.rel |
| GS970M/10PS<br>GS970M/10<br>GS970M/18PS<br>GS970M/18<br>GS970M/28PS<br>GS970M/28 | GS970M | 07/2022 | GS970-5.5.2-1.1.rel |
| 10GbE Virtual UTM Firewall | vFW | 07/2022 | ATVSTAPL-1.7.1.iso and<br>vfw-x86_64-5.5.2-1.1.app |
| AR4050S<br>AR4050S-5G<br>AR3050S | AR-series UTM firewalls | 07/2022 | AR4050S-5.5.2-1.1.rel<br>AR3050S-5.5.2-1.1.rel |
| AR2050V<br>AR2010V<br>AR1050 V | AR-series VPN routers | 07/2022 | AR2050V-5.5.2-1.1.rel<br>AR2010V-5.5.2-1.1.rel<br>AR1050V-5.5.2-1.1.rel |

**Caution**: Software version 5.5.2-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-1.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 55 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 57.

## Unsupported devices

Version 5.5.2-1.x does not support:

- GS900MX and GS900MPX Series
- FS980M Series
- IE200 Series
- IE300 Series
- IE510-28GSX switches
- x310 Series
- x510, x510L and x510DP Series
- IX5-28GPX switches

The last version to support the above switches is 5.5.1-2.x.

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

The 5.5.2-1.1 software version is not ISSU compatible with previous software versions.

# New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.2-1.1:


- "Management Features on VRF-lite" on page 38
- "Bi-directional Forwarding Detection (BFD) enhancements" on page 38
- "VCStack and aggregator enhancements for VxLAN" on page 39
- "OpenFlow trustpoints" on page 39
- "Improved authentication methods for SSL-VPN: two-factor authentication and LDAP" on page 40
- "Tunnel inline-processing" on page 41
- "Excluding flows from Web Redirect by specifying their IP address" on page 41
- "Auto-completion of application names and entities" on page 42
- "Enhancements to port authentication with IP phones" on page 42
- "Triggers based on environment sensor changes" on page 43
- "Update to the method used for hashing passwords" on page 43
- "Enable or disable TCP port forwarding on the SSH server" on page 43
- "Increase to number of wireless Channel Blanket VAPs" on page 44
- "Use a USB stick to turn on wireless Emergency Mode" on page 44
- "Increase to number of MAC address filter entries for wireless controller" on page 45


To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 54.

# Management Features on VRF-lite

*Available on all AlliedWare Plus devices that support VRF-lite*

From 5.5.2-1.1 onwards, a number of additional AlliedWare Plus management features can be constrained to a named VRF.

These features either operate as clients or servers. For the servers, if the server is configured with a named VRF, clients will only be able to connect to the server from within the same VRF. For clients, if the client is configured with a named VRF, it will only be able to connect to a server through an interface that is also contained in the same named VRF. If a VRF is not specified in the configuration, the feature will reside in the global VRF as per previous behavior.

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

Utilities that are newly available within a VRF domain include:

- **Some network and file management utilities** - see the Configuration and File Management Feature Overview and Configuration Guide
- **SSH** - see the SSH Feature Overview and Configuration Guide
- **Syslog** - see the Logging Feature Overview and Configuration Guide
- **DNS** - see the DNS Feature Overview and Configuration Guide
- **SNMP** - see the SNMP Feature Overview and Configuration Guide
- **Authentication** - see the AAA and Port Authentication Feature Overview and Configuration Guide
- **RADIUS** - see the RADIUS Feature Overview and Configuration Guide
- **TACACS**+ - see the TACACS+ Feature Overview and Configuration Guide.

Utilities that remain unavailable within a VRF domain include:

- Telnet Server
- SNMP Server
- NTP Server

# Bi-directional Forwarding Detection (BFD) enhancements

*Available on SBx8100, SBx908 GEN2, x950, x930, and x530 Series switches*

From 5.5.2-1.1 onwards, Bi-directional Forwarding Detection (BFD) is now supported on x530 Series switches, in addition to the SBx8100, SBx908 GEN2, x950, and x930 Series.

BFD provides a consistent failure detection method for network administrators, in addition to fast forwarding path failure detection. The network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates seen with different routing protocol hello mechanisms.

In addition, the following new features have also been added:

- BFD supports applying profiles to OSPF multihop and IPv4 static routes.
- BFD supports VRF-Lite for OSPF, BGP, and IPv4 static routes.

For more information, see the Bi-directional Forwarding Detection (BFD) Feature Overview and Configuration Guide.

## VCStack and aggregator enhancements for VxLAN

*Available on SBx908 GEN2, x950, and x530 Series switches*

From 5.5.2-1.1 onwards, VXLAN is supported on 2-member VCStack installations on SBx908 GEN2 and x950. Previously, VCStack was only supported on x530 Series switches.

As part of this enhancement, VxLAN now supports link aggregators as downlinks and uplinks. Previously, aggregators were only supported on x530 Series and only as downlinks.

For more information on VxLAN, see the VxLAN Feature Overview and Configuration Guide. For more information on VCStack, see the VCStack Feature Overview and Configuration Guide.

## OpenFlow trustpoints

*Available on all AlliedWare Plus devices that support OpenFlow*

From 5.5.2-1.1 onwards, all trustpoints are supported. Prior to this release, only the 'local' self-signed trustpoint was supported.

To connect over TLS, every OpenFlow switch must have a unique private/public key pair and a certificate that signs the public key. A **trustpoint** is a named set of files including a private key and signed certificate that allows secure connection using SSL.

For more information on configuring OpenFlow and trustpoints, see the OpenFlow Feature Overview and Configuration Guide.

# Improved authentication methods for SSL-VPN: two-factor authentication and LDAP

*Available on all AlliedWare Plus devices that support OpenVPN and AAA authentication.*

From 5.5.2-1.1 onwards, SSL OpenVPN authentication supports two-factor authentication using Google authenticator, and authentication via LDAP.

- **Two-factor authentication** (2FA) - supported for OpenVPN only.

  2FA increases authentication security by requiring a second method of authentication. This AlliedWare Plus version supports 2FA for OpenVPN connections via a mobile authenticator app using TOTP and HOTP as described in RFC-6238 and RFC-4226. One well-known implementation of this is Google authenticator.
- **Lightweight Directory Access Protocol** (LDAP) - supported for OpenVPN and other authentication types.

  LDAP:

  - is an authentication protocol that facilitates user access to various IT resources e.g. applications, servers, networking equipment, and file servers. LDAP is also leveraged as a directory store of information about users, and can be used to locate individuals, organizations, and devices on a network.
  - can be used when connecting to internal networks over OpenVPN. Although both LDAP and RADIUS are interchangeable on AlliedWare Plus devices as an authentication protocol, LDAP is added because of its ability to interact with directory services such as Microsoft's Active Directory (AD).

## Configuring 2FA

With an existing working OpenVPN configuration on your AlliedWare Plus device, adding two-factor authentication is simple and requires the following actions:

- enable the 2FA service
- create a 2FA user and load a shared secret key into the users mobile device
- enable 2FA in the OpenVPN via AAA configuration.

From then on all connections to OpenVPN will require two-factor authentication. There are also a number of global options that can be used to change certain behaviors of the feature, like whether to allow users with no 2FA configuration to connect.

## Configuring LDAP

To enable a user to connect to an internal network through OpenVPN, you simply:

- configure an LDAP server to connect to
- create a LDAP server group - for AAA login
- enable LDAP authentication of OpenVPN tunnels globally.

For more detailed information on configuring 2FA, see the OpenVPN Feature Overview Guide. For LDAP, see the LDAP Feature Overview and Configuration Guide.

# Tunnel inline-processing

*Available on vFW, AR4050S, AR4050S-5G, AR3050S, AR2050V, AR2010V, and AR1050V*

From version 5.5.2-1.1 onwards, you can use **tunnel inline-processing** to improve the forwarding performance of incoming application traffic. Use this feature when traffic is encapsulated within an encrypted VPN and subsequently processed and identified via Deep Packet Inspection (DPI).

Tunnel inline-processing is useful because it means packets are decrypted before being analysed and processed via the DPI engine. This is especially important for VPN traffic, where you actually want to identify application traffic transported within the IPSEC VPN, rather than the outer encrypted IPsec VPN headers.

This also avoids the need to configure tunnel security-reprocessing, which is the alternative, less efficient option. With tunnel security-reprocessing configured, the DPI engine processes incoming VPN traffic twice (before and after decryption), in order to identify incoming application traffic transported via an encrypted VPN.

**New commands**

For example, to enable tunnel inline-processing on tunnel 0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel inline-processing
```

Use the following command to display tunnel inline-processing counters:

```
awplus# show tunnel inline-processing counters
```

For more information on tunnel inline-processing, see the IPsec Feature Overview and Configuration Guide

# Excluding flows from Web Redirect by specifying their IP address

*Available on vFW, AR4050S, AR4050S-5G, AR3050S, AR2050V, and AR2010V*

From 5.5.2-1.1 onwards, a new exclusion method has been added to Web Redirect. You can now specify flows to exclude from being redirected by entering their destination IP or IPv6 address or subnet. Previously, you could exclude flows on the basis of their destination URL but not their destination IP address.

To exclude by IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# exclude dst-ip <address>
```

For more information on configuring Web Redirect, see the Web Redirect Feature Overview and Configuration Guide.

## Auto-completion of application names and entities

*Available on vFW, AR4050S, AR4050S-5G, AR3050S, AR2050V, AR2010V, and AR1050V*

From 5.5.2-1.1 onwards, it is easier to specify the name of an existing DPI application or firewall entity in commands. Previously, you had to type the whole application or entity name into the command line. Now, you can use the tab key to auto-complete names.

This affects a number of commands, including:

- the firewall **rule** command
- the firewall **connection-limit** command
- the NAT **rule** command
- the web-control **rule** command
- the web-control **bypass-web-control** command
- the policy-based routing **ip policy-route** and **ipv6 policy-route** commands
- the **application** command
- the traffic-control **rule** command.

## Enhancements to port authentication with IP phones

*Available on all devices that support port authentication*

From 5.5.2-1.1 onwards, two new port authentication options exist to increase security for networks with IP phones. Both options prevent unwanted supplicants from connecting to the network when a host (e.g. a PC) connects to an AlliedWare Plus NAS via an IP phone.

In this situation, you mostly want to allow only that host and phone to connect via the port on the NAS. There are now two ways you can do this:

- Specify how many tagged and untagged VLANs can authenticate on a port, or
- Specify that a port can have a single voice and a single data supplicant

For details of each of these options, and step-by-step configuration examples, see "Limit the number of supplicants when connecting via an IP phone" in the AAA and Port Authentication Feature Overview and Configuration Guide.

## Triggers based on environment sensor changes

*Available on all AlliedWare Plus devices that have environment sensors*

From 5.5.2-1.1 onwards, you can create triggers that will activate when the device's environment sensors detect an event, and run commands of your choice. Environment sensor events are shown in the output of the command **show system environment,** and include device temperature, power settings, voltage, and fan speed.

Depending on the device and sensor, you can create a trigger to run when:

- the sensor's state changes, for example when a loss of power is detected for a power supply, or when power is restored, or both.
- the sensor's reading crosses a high or low threshold, for example when the device temperature becomes too high, or returns to normal, or both.

For the details of these options and a step-by-step configuration guide, see the Triggers Feature Overview and Configuration Guide.

## Update to the method used for hashing passwords

*Available on all AlliedWare Plus devices*

AlliedWare Plus devices store user passwords in configuration files in hashed form. From 5.5.2-1.1 onwards, the hash method for these passwords has been upgraded.

## Enable or disable TCP port forwarding on the SSH server

*All AlliedWare Plus devices that support SSH server*

From 5.5.2-1.1 onwards, SSH TCP port forwarding is disabled by default to enhance security. A new command allows you to enable it:

```
awplus# configure terminal
awplus(config)# ssh server tcpforwarding
```

# Increase to number of wireless Channel Blanket VAPs

*Available on all devices that support Vista Manager mini for wireless control*

From 5.5.2-1.1 onwards, when an AlliedWare Plus device is acting as a wireless controller, it supports more Virtual Access Points (VAPs) for channel blanket installations on TQ5403, TQ5403e and TQ6602 access points. The new limits are:

| | TQ5403 and TQ5403e | TQ6602 |
|---|---|---|
| Maximum CB VAPs on each AP | 6 | 20 |
| Maximum CB VAPs on each radio | 3 | 10 |

This new limit requires the following firmware version on the AP:

- AT-TQ6602: 7.0.1-1.1 or later
- AT-TQ5403 and AT-TQ5403e: 6.0.1-1.1 or later.

It is also available through Device GUI version 2.12.0 or later on the AlliedWare Plus device that is acting as the wireless controller.

# Use a USB stick to turn on wireless Emergency Mode

*Available on all devices that support Vista Manager mini for wireless control*

AlliedWare Plus wireless controllers support Emergency Mode for wireless networks. Emergency Mode makes your wireless network available to the public in an emergency, such as a natural disaster.

From 5.5.2-1.1 onwards, AlliedWare Plus lets you put your wireless network into Emergency Mode by simply inserting a pre-prepared USB stick into the AlliedWare Plus device that is the wireless controller. This enhancement makes it easier to start Emergency Mode, because you don't have log into the AlliedWare Plus device to do so.

To do this using the CLI, insert an empty USB stick into the AlliedWare Plus device and use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# emergency-mode usb enable
awplus(config-wireless)# emergency-mode usb key ExampleKey
description ExampleEmergencyUSB
awplus(config-wireless)# end
awplus# wireless emergency-mode usb mark key ExampleKey
```

The **key** parameter in the commands **emergency-mode usb key** and **wireless emergency-mode usb mark key** must match.

You can also do this using Device GUI version 2.12.0 or later on the AlliedWare Plus device.

Once you have prepared the USB stick and the AlliedWare Plus device, to put the network into Emergency Mode, just insert the USB stick. As long as the keys on the device and the stick match, emergency mode will automatically activate. The device's port LEDs will blink to indicate it is in emergency mode.

For more information about configuring Emergency Mode, see the Wireless Management (AWC) with Vista Manager mini User Guide.

## Increase to number of MAC address filter entries for wireless controller

*Available on all devices that support Vista Manager mini for wireless control. The increase applies to TQ6702 GEN2, TQ6602 GEN2, TQm6702 GEN2, and TQm6602 GEN2. Several other APs already support 3048 MAC address filter entries.*

From 5.5.2-1.1 onwards, when an AlliedWare Plus device is acting as a wireless controller, it supports filtering up to 3072 MAC addresses on TQ6702 GEN2, TQ6602 GEN2, TQm6702 GEN2, and TQm6602 GEN2 Access Points.

To add a filter entry to a MAC filter with the CLI, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# wireless-mac-filter <filter-id>
awplus(config-wireless)# filter-entry <mac-address>
[description <description>]
```

Alternatively, the Device GUI makes it easy to add a large number of filter entries, by uploading a CSV file.

# Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.2-1.x and may affect your device or network behavior if you upgrade:

- Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches
- Changes that may affect device or network configuration

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

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

Please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.1-1.x version, please check the 5.5.1-2.x and 5.5.2-0.x release note. Release notes are available from our website, including:

- 5.5.2-x.x release notes
- 5.5.1-x.x release notes
- 5.5.0-x.x release notes
- 5.4.9-x.x release notes
- 5.4.8-x.x release notes
- 5.4.7-x.x release notes
- 5.4.6-x.x release notes

## Limits to Upgrade Compatibility on SwitchBlade x908 GEN2, x950 and x930 Series Switches

These switches can only be upgraded to the most recent firmware versions from specified older firmware versions. If you attempt to upgrade from other older firmware versions, the firmware becomes corrupt and the switch will not boot up.

**The solution** Before upgrading to the latest firmware version, upgrade to one of the specified older versions. See "Details for SBx908 GEN2 and x950 Series" on page 47 and "Details for x930 Series" on page 48 for details.

**Affected Products**

The following models could be affected:

| x930 Series running any bootloader version | x950 Series running bootloader versions older than 6.2.24 | SBx908 GEN2 running bootloader versions older than 6.2.24 |
|---|---|---|
| x930-28GTX | x950-28XSQ | SBx908 GEN2 |
| x930-28GPX | x950-28XTQm | |
| x930-52GTX | | |
| x930-52GPX | | |
| x930-28GSTX | | |

For SBx908 GEN2 and x950 Series, the restriction only applies to switches running bootloader versions older than 6.2.24.

## Recovering from upgrading from an incompatible version

If you try to upgrade from an incompatible firmware version, the switch will not finish booting up. If this happens, you can recover by using the bootloader menu to boot with a compatible version from an alternative source, such as a USB stick. See the Bootloader and Startup Feature Overview and Configuration Guide for details.

## Details for SBx908 GEN2 and x950 Series

For these switches, **versions 5.5.0-0.1** and later are affected, on switches where the bootloader is older than 6.2.24. If your bootloader is older than 6.2.24, you **cannot** upgrade to versions 5.5.0-0.1 and later directly from:

- 5.4.9-1.x
- 5.4.9-0.x
- any version before 5.4.8-2.12.

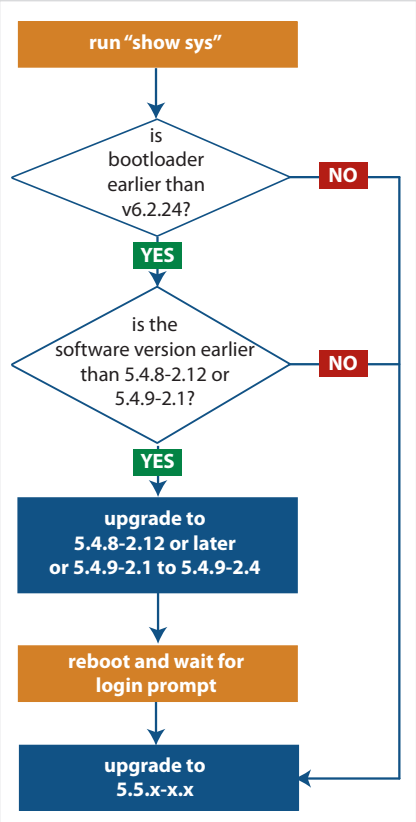
Instead, before upgrading from one of those versions to 5.5.0-0.1 or later, make sure your switch is running one of these specified versions:

- 5.4.8-2.12 or a later 5.4.8-2.x version
- 5.4.9-2.1 to 5.4.9-2.4.

If it is not, upgrade to one of these versions before upgrading to the desired 5.5.x-x.x version.

To see your bootloader and current software version, check the "Bootloader version" and "Software version" fields in the command:

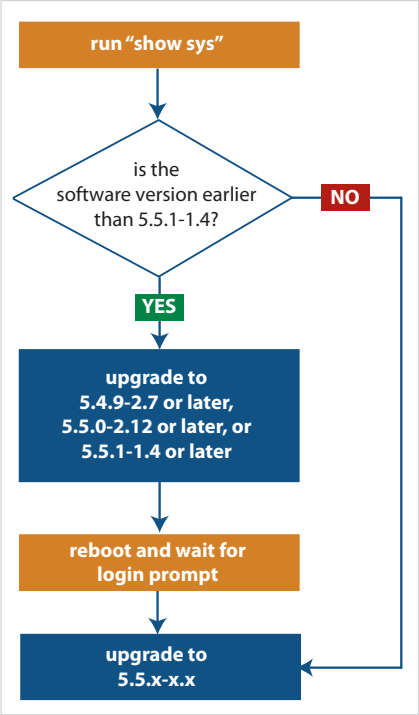
```
awplus# show system
```



## Details for x930 Series

For these switches, **versions 5.5.1-2.1** and later are affected, on switches with all bootloaders. You **cannot** upgrade to versions 5.5.1-2.1 and later directly from:

- 5.5.1-1.3 or earlier
- 5.5.1-0.x
- 5.5.0-2.11 or earlier
- 5.5.0-1.x
- 5.5.0-0.x
- any version before 5.4.9-2.7.




Instead, before upgrading from one of those versions to 5.5.1-2.1 or later, make sure your switch is running one of these specified versions:

- 5.4.9-2.7 or a later 5.4.9-2.x version
- 5.5.0-2.12 or a later 5.5.0-2.x version
- 5.5.1-1.4 or a later 5.5.1-1.x version.

If it is not, upgrade to one of these versions before upgrading to version 5.5.1-2.1 or later.

To see your current software version, check the "Software version" field in the command:

```
awplus# show system
```

# Changes that may affect device or network configuration

The following changes may require you to modify your device or network configuration when you upgrade to this release.

| Summary | Affected devices | Detail |
|---|---|---|
| Enable or disable TCP port forwarding on the SSH server | All AlliedWare Plus devices that support SSH server | From 5.5.2-1.1 onwards, SSH TCP port forwarding is disabled by default to enhance security. A new command allows you to enable it:<br><br>`awplus(config)# ssh server tcpforwarding` |

# Software release licensing

*Applies to SBx908 GEN2 and SBx8100 Series switches*

Please ensure you have a 5.5.2 license on your switch if you are upgrading to 5.5.2-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 55 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 57.

# Upgrading a VCStack with rolling reboot

*Applies to all stackable AlliedWare Plus switches, except SBx8100*

This version supports VCStack "rolling reboot" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

**For SBx908 GEN2, x950 and x550 Series switches**

You can use rolling reboot to upgrade to this version from:

- 5.5.2-0.x
- 5.5.1-x.x
- 5.5.0-x.x

On these switches, you **cannot** use rolling reboot to upgrade to this version from any version earlier than 5.5.0-0.x.

**For x530 Series switches using DAC to stack**

If you are using DACs (Direct Attach Cables) to connect stack members, you can use rolling reboot to upgrade to this version from:

- 5.5.2-0.x
- 5.5.1-x.x
- 5.5.0-x.x
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

**For other switches and for x530 switches using SFP+ to stack**

Otherwise, you can use rolling reboot to upgrade to this version from:

- 5.5.2-0.x
- 5.5.1-x.x
- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 5.4.4-1.x

**To use rolling reboot**

First enter the **boot system** command, which will install the new release file on all stack members. Then enter the **reboot rolling** command.

# Forming or extending a VCStack with auto-synchronization

*Applies to all stackable AlliedWare Plus switches*

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

If auto-synchronization is not supported between the software versions on the devices in your stack, you need to make sure all devices are running the same version before you connect the stack together.

**For SBx908 GEN2, x950 and x550 Series switches**

Auto-synchronization is supported between this version and:

- 5.5.2-0.x
- 5.5.1-x.x
- 5.5.1-0.x
- 5.5.0-x.x

On these switches, auto-synchronization is not supported between this version and any version earlier than 5.5.0-0.x.

**For CFC960 cards in an SBx8100 system**

If you want to combine CFC960 v2 and earlier CFC960 cards in a chassis or stack, make sure that the earlier cards are running 5.5.0-x.x or later before you combine them. This applies whether you:

- add a CFC960 v2 card to a chassis or stack that contains earlier CFC960 cards, or
- add an earlier CFC960 card to a chassis or stack that contains CFC960 v2 cards.

Auto-synchronization will not update the software on the earlier CFC960 cards.

Note that this situation only applies if your chassis or stack includes CFC960 v2 cards that are labeled "SBx81CFC960 v2" on the front panel of the card. All cards that are labeled "SBx81CFC960" are referred to as earlier cards, even if their documentation refers to them as version 2.

If you do combine cards that are running incompatible software, then remove the CFC960 v2 card or cards, update the software on the other cards, and re-install the CFC960 v2 cards.

**For x530 Series switches using DAC to stack**

If you are using DACs (Direct Attach Cables) to connect stack members, auto-synchronization is supported between this version and:

- 5.5.2-0.x
- 5.5.1-x.x
- 5.5.0-x.x
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

**For other switches and for x530 switches using SFP+ to stack**

Otherwise, auto-synchronization is supported between this version and:

- 5.5.2-0.x
- 5.5.1-x.x
- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-2.x
- 5.4.6-1.2 and all later 5.4.6-1.x versions.

It is not supported between this version 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. However, if this is not possible, then nodes running this version are compatible with nodes running:

- 5.5.2-0.x
- 5.5.1-x.x
- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 5.4.4-x.x
- 5.4.3-2.6 or later.

## Upgrading all devices in an AMF network

*Applies to all AlliedWare Plus devices*

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

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

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

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

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

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

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).

2. Decide which AMF upgrade method is most suitable.

3. Initiate the AMF network upgrade using the selected method. To do this:
   a. create a working-set of the nodes you want to upgrade
   b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
   c. Check the console messages to make sure that all nodes are “release ready”. If they are, follow the prompts to perform the upgrade.

# Obtaining User Documentation

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

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

# Verifying the Release File

On devices that support crypto secure mode, 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 hash of the file.

This command compares the SHA256 hash of the release file with the correct hash for the file. The correct hash is listed in the table of 5.5.2-1.5 Product hash values below or 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 hash. For example, all x930 Series switches have the same hash.

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

Table: 5.5.2-1.5 Product hash values

| Product family | Software File | Hash |
|---|---|---|
| AMF Cloud | vaa-5.5.2-1.5.rel | 171dc4b5c530389ecde250a2fbe3cfa0e7edf1da66ec68cc28029ba612858d50 |
| SBx8100 | SBx81CFC960-5.5.2-1.5.rel | 3be51c75fbd99fa42848d47d47440da1911638359fe3d0488d2b63f3f9f42f58 |
| SBx908 GEN2 | SBx908NG-5.5.2-1.5.rel | 0520cc25a225b8f67d280bd9fcb7e065b37528cccfd327d49d3cd3215406e2eb |
| x950 | x950-5.5.2-1.5.rel | 0520cc25a225b8f67d280bd9fcb7e065b37528cccfd327d49d3cd3215406e2eb |
| x930 | x930-5.5.2-1.5.rel | 1b0a628c85d9217f36341e3f3847f6358db1d02821e883e575c716c991825283 |
| x550 | x550-5.5.2-1.5.rel | 269e6d29b9d6350bfd7701513363bedeb9e518e2306fe91bb228ce2c28e49433 |
| x530 & x530L | x530-5.5.2-1.5.rel | 34f7fa41d280d97b4624b94a3af3879966637bc2f96b2d762965cd3c3aab4f5f |
| x330 | x330-5.5.2-1.5.rel | 36448b18bb75c6f0c7d3843727fe31461f01053aad58beaf02936b4cdd521c8a |

Table: 5.5.2-1.5 Product hash values

| Product family | Software File | Hash |
|---|---|---|
| x320 | x320-5.5.2-1.5.rel | 34f7fa41d280d97b4624b94a3af3879966637bc2f96b2d762965cd3c3aab4f5f |
| x230 & x230L | x230-5.5.2-1.5.rel | 106242d5ebba7db63d25333d4bd32ad4c5da78c917380c5e2d952948cf1b1985 |
| x220 | x220-5.5.2-1.5.rel | efc1cd1523369f685abfe9066da2e9f62649be0a759d1b4acc05ddc7f2fcf181 |
| IE340 & IE340L | IE340-5.5.2-1.5.rel | 3401ed27023426a05eb11542aad4bd6f89148efca15c565f27a912188b601a55 |
| IE210L | IE210-5.5.2-1.5.rel | 106242d5ebba7db63d25333d4bd32ad4c5da78c917380c5e2d952948cf1b1985 |
| XS900MX | XS900-5.5.2-1.5.rel | b5ba8749453d5399b9905e74da00eebb3d9e733d66d5c6808f43ca47465a2e8a |
| GS980MX | GS980MX-5.5.2-1.5.rel | b5ba8749453d5399b9905e74da00eebb3d9e733d66d5c6808f43ca47465a2e8a |
| GS980EM | GS980EM-5.5.2-1.5.rel | b5ba8749453d5399b9905e74da00eebb3d9e733d66d5c6808f43ca47465a2e8a |
| GS980M | GS980M-5.5.2-1.5.rel | efc1cd1523369f685abfe9066da2e9f62649be0a759d1b4acc05ddc7f2fcf181 |
| GS970EMX | GS970EMX-5.5.2-1.5.rel | 36448b18bb75c6f0c7d3843727fe31461f01053aad58beaf02936b4cdd521c8a |
| GS970M | GS970-5.5.2-1.5.rel | 106242d5ebba7db63d25333d4bd32ad4c5da78c917380c5e2d952948cf1b1985 |
| AR4050S-5G | AR4050S-5.5.2-1.5.rel | 2680d56f968bd01cdb89a08043eeef3877ebea1826b8761a768ef91b180faa52 |
| AR4050S | AR4050S-5.5.2-1.5.rel | 2680d56f968bd01cdb89a08043eeef3877ebea1826b8761a768ef91b180faa52 |
| AR3050S | AR3050S-5.5.2-1.5.rel | 2680d56f968bd01cdb89a08043eeef3877ebea1826b8761a768ef91b180faa52 |
| AR2050V | AR2050V-5.5.2-1.5.rel | 2680d56f968bd01cdb89a08043eeef3877ebea1826b8761a768ef91b180faa52 |
| AR2010V | AR2010V-5.5.2-1.5.rel | 2680d56f968bd01cdb89a08043eeef3877ebea1826b8761a768ef91b180faa52 |
| AR1050V | AR1050V-5.5.2-1.5.rel | 427296c045e88074a751a087a7e2dd5f83528a19721e73916fa71c8824f4d963 |

# 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-2021
Features included             : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                                EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                                L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                                RADIUS-100, RIP, VCStack, VRRP

Index                         : 2
License name                  : 5.5.2
Customer name                 : ABC Consulting
Quantity of licenses          : 1
Type of license               : Full
License issue date            : 20-Aug-2021
License expiry date           : N/A
Release                       : 5.5.2
```

# 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-2021
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.5.2
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Aug-2021
License expiry date            : N/A
Release                        : 5.5.2
```

# Installing this Software Version

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 55 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 57.

To install and enable this software version on a switch or AR series device, use the following steps:

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

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

| Product | Command |
|---|---|
| SBx8100 with CFC960 | `awplus(config)# boot system SBx8100-5.5.2-1.5.rel` |
| SBx908 GEN2 | `awplus(config)# boot system SBx908NG-5.5.2-1.5.rel` |
| x950 series | `awplus(config)# boot system x950-5.5.2-1.5.rel` |
| x930 series | `awplus(config)# boot system x930-5.5.2-1.5.rel` |
| x550 series | `awplus(config)# boot system x550-5.5.2-1.5.rel` |
| x530 series | `awplus(config)# boot system x530-5.5.2-1.5.rel` |
| x330-10GTX | `awplus(config)# boot system x330-5.5.2-1.5.rel` |
| x320 series | `awplus(config)# boot system x320-5.5.2-1.5.rel` |
| x230 series | `awplus(config)# boot system x230-5.5.2-1.5.rel` |
| x220 series | `awplus(config)# boot system x220-5.5.2-1.5.rel` |
| IE340 series | `awplus(config)# boot system IE340-5.5.2-1.5.rel` |
| IE210L series | `awplus(config)# boot system IE210-5.5.2-1.5.rel` |

| Product | Command |
|---|---|
| XS900MX series | `awplus(config)# boot system XS900-5.5.2-1.5.rel` |
| GS980M series | `awplus(config)# boot system GS980M-5.5.2-1.5.rel` |
| GS980EM series | `awplus(config)# boot system GS980EM-5.5.2-1.5.rel` |
| GS980MX series | `awplus(config)# boot system GS980MX-5.5.2-1.5.rel` |
| GS970EMX/10 | `awplus(config)# boot system GS970EMX-5.5.2-1.5.rel` |
| GS970M series | `awplus(config)# boot system GS970-5.5.2-1.5.rel` |
| AR4050S-5G | `awplus(config)# boot system AR4050S-5.5.2-1.5.rel` |
| AR4050S | `awplus(config)# boot system AR4050S-5.5.2-1.5.rel` |
| AR3050S | `awplus(config)# boot system AR3050S-5.5.2-1.5.rel` |
| AR2050V | `awplus(config)# boot system AR2050V-5.5.2-1.5.rel` |
| AR2010V | `awplus(config)# boot system AR2010V-5.5.2-1.5.rel` |
| AR1050V | `awplus(config)# boot system AR1050V-5.5.2-1.5.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
```

# Accessing and Updating the Web-based GUI

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

On select AlliedWare Plus devices, you can also optimize the performance of your Allied Telesis APs through Vista Manager mini.

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

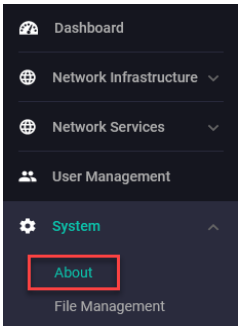
   Alternatively, on unconfigured devices you can use the default address, which is:

   - on switches: 169.254.42.42
   - on AR-Series: 192.168.1.1

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

3. 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*.

## Check the GUI version




To see which version you have, open the **System** > **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.2-1.5 is 2.13.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 62 or "Update the GUI on AR-Series devices" on page 63.

## Update the GUI on switches

Perform the following steps through the Device GUI and 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 GUI filename to use with AlliedWare Plus v5.5.2-x.x is awplus-gui_552_28.gui.

   The file is not device-specific; the same file works on all devices. Make sure that the version string in the filename (e.g. 552) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

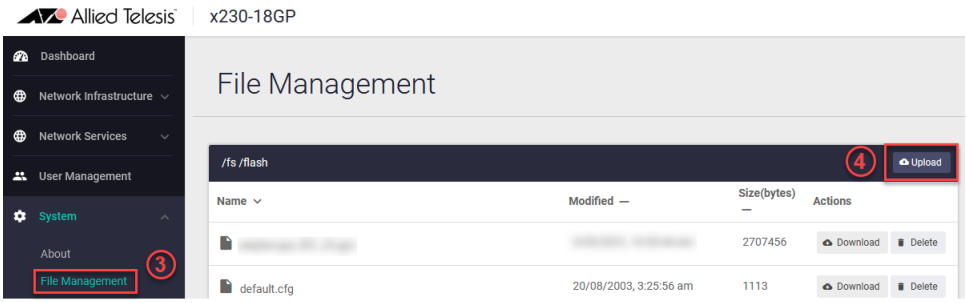
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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*.

3. Go to **System** > **File Management**

4. Click **Upload**.




5. Locate and select the GUI file you downloaded from our Software Download center. The new GUI file is added to the **File Management** window.

   You can delete older GUI files, but you do not have to.

6. Reboot the switch. Or alternatively, use **System** > **CLI** to access the command line interface, then use the following commands to stop and restart the HTTP service:

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

   To confirm that the correct file is now in use, then use the commands:

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

## Update the GUI on AR-Series devices

**Prerequisite:** On AR-Series devices, 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.

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

1. Log into the GUI and use **System** > **CLI** to access the command line interface.
2. Use the following commands to download the new GUI:

```
awplus> enable
awplus# update webgui now
```

3. Browse to the GUI and check that you have the latest version now, on the **System** > **About** page. You should have v2.13.0 or later.