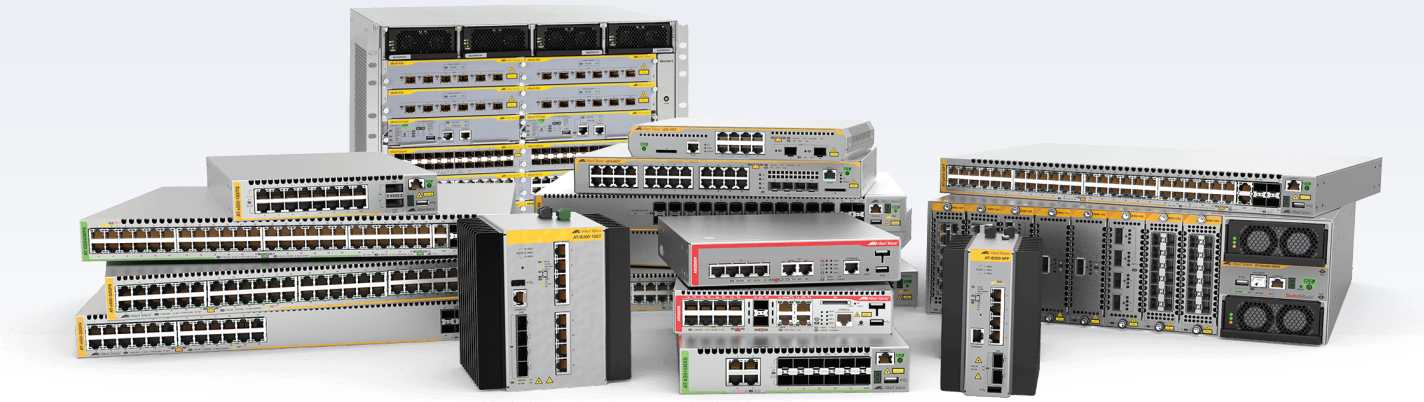
Release Note for AlliedWare Plus Software Version 5.5.1-1.x



AlliedWare Plus OPERATING SYSTEM

» AMF Cloud » SBx8100 Series » SBx908 GEN2 » x950 Series » x930 Series
» x550 Series » x530 Series » x530L Series » x510 Series » IX5 Series
» x320 Series » x310 Series » x230 Series » x220 Series
» IE500 Series » IE340 Series » IE300 Series » IE210L Series » IE200 Series
» XS900MX Series » GS980MX Series » GS980EM Series » GS980M Series
» GS970M Series » GS900MX/MPX Series » FS980M Series
» AR4050S » AR3050S » AR2050V » AR2010V » AR1050V

» 5.5.1-1.1 » 5.5.1-1.2 » 5.5.1-1.3 » 5.5.1-1.4

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 registered mail including a check for US$15 to cover production and shipping costs and a CD with the GPL code will be mailed to you.

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 5.5.1-1.4

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-1.4.

Caution: SSH was upgraded in 5.5.1-1.1, to increase security. Some older SSH clients may no longer connect to your AlliedWare Plus device. To resolve this, see "Older SSH clients can't connect to AlliedWare Plus devices" on page 36.

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 48.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 50. 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		01/2022	vaa-5.5.1-1.4.iso (VAA OS) vaa-5.5.1-1.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-1.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	01/2022	SBx81CFC960-5.5.1-1.4.rel
SBx908 GEN2	SBx908 GEN2	01/2022	SBx908NG-5.5.1-1.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	01/2022	x950-5.5.1-1.4.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	01/2022	x930-5.5.1-1.4.rel

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

Models	Family	Date	Software File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2022	x550-5.5.1-1.4.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	01/2022	x530-5.5.1-1.4.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	01/2022	x510-5.5.1-1.4.rel
IX5-28GPX	IX5	01/2022	IX5-5.5.1-1.4.rel
x320-10GH x320-11GPT	x320	01/2022	x320-5.5.1-1.4.rel
x310-26FT x310-26FP x310-50FT x310-50FP	x310	01/2022	x310-5.5.1-1.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2022	x230-5.5.1-1.4.rel
x220-28GS x220-52GT x220-52GP	x220	01/2022	x220-5.5.1-1.4.rel
IE510-28GSX	IE510-28GSX	01/2022	IE510-5.5.1-1.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	01/2022	IE340-5.5.1-1.4.rel
IE300-12GT IE300-12GP	IE300	01/2022	IE300-5.5.1-1.4.rel
IE210L-10GP IE210L-18GP	IE210L	01/2022	IE210-5.5.1-1.4.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	01/2022	IE200-5.5.1-1.4.rel
XS916MXT XS916MXS	XS900MX	01/2022	XS900-5.5.1-1.4.rel

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

Models	Family	Date	Software File
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	01/2022	GS980MX-5.5.1-1.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	01/2022	GS980EM-5.5.1-1.4.rel
GS980M/52 GS980M/52PS	GS980M	01/2022	GS980M-5.5.1-1.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2022	GS970-5.5.1-1.4.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	01/2022	GS900-5.5.1-1.4.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	01/2022	FS980-5.5.1-1.4.rel
AR4050S AR3050S	AR-series UTM firewalls	01/2022	AR4050S-5.5.1-1.4.rel AR3050S-5.5.1-1.4.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	01/2022	AR2050V-5.5.1-1.4.rel AR2010V-5.5.1-1.4.rel AR1050V-5.5.1-1.4.rel

Caution: Software version 5.5.1-1.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-1.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 44 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 46.

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

The 5.5.1-1.4 software version is ISSU compatible with previous software versions.

Enhancements

This section summarizes the enhancement in sofware version 5.5.1-1.4

IGMP

For all AlliedWare Plus devices that support IGMP, you can use the command:

```
awplus(config)# ip multicast handle-igmp-immediately
```

to process IGMP packets more quickly in networks with a low rate of IGMP packets. This allows clients to start receiving multicast traffic immediately. Without this command, these devices process IGMP packets after they receive 250 packets or after 1 second, whichever comes first.

Enabling this command is only recommended when using up to 4096 multicast streams.

ISSU: Effective when CFCs upgraded.

For more information about IGMP and multicast, see the IGMP/MLD Feature Overview and Configuration Guide.

Issues Resolved in Version 5.5.1-1.4

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-74538	**AMF**	Previously, the AMF isolated node recovery failed to recover when the AMF member was connected via a virtual link and obtained an address from a DHCP server. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-75341	**AMF**	Previously, in some circumstances, a device reachable via a virtual link could not be joined in a working-set. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y	–
CR-75505	**AMF**	Previously, under certain conditions, deleted supplicant entries would not be cleared from the device hardware table. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-74422	**AWC Lite**	Previously, configuring SNMP settings for an AP via WebAPI could cause the Centralized Wireless Manager (CWM) to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-74841	**AWC Lite**	With this software update, you can clear the wireless trigger settings by using the command: **`no wireless`**	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–
CR-74846	**AWC Lite**	With this software update, you can delete the CB-VAP BSSID settings by using using the command: **`no wireless`**	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-74702	**Firewall**	Previously, unicast UDP traffic flowing in one direction could incorrectly cause the firewall UDP limit to be reached, resulting in the UDP traffic being dropped. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-74058	**Open VPN**	Previously, memory exhaustion could occur while processing IPv4 routes during OpenVPN client reconnections. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-73716	**Pluggables**	Previously, on the x930-GSTX variant switch, the LX10a pluggable could sometimes fail to link up after a reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-74424	**Policy-based Routing, 5G**	Previously, when using the 5G interface with a policy-based routing rule, the wrong route could be selected. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-75006	**Port Authentication**	Previously, MAC authentication would only accept one MAC address per port on the IE200 switch. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-74467	**Port Authentication VCStack**	Previously, under rare circumstances, port authentication would not work on a stack backup member after the member rejoined the stack. This issue has been resolved.	–	–	Y	Y	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-74225	**Port Configuration**	Previously, on x530 variant switches with 5G copper ports, there was a low occurrence of an issue after configuring a 5G port with "speed 2500" or "speed auto 2500", where the port would show "configured speed 2500", yet also show "current speed 5000" in the command **show interface <portx.y.z>**. As a result, the port would not pass traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-74593	**System**	Previously, the combination of a large number of application-proxy blocks and a large number of incoming MAC addresses could possibly cause a device to retart unexpectedly. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-74645	**System**	Previously, the Web Authentication login screen would not be assessible after restarting the IMI process. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-74402	**Web Control**	Previously, memory exhaustion could occur when configuring Web Control. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

What's New in Version 5.5.1-1.3

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
x510 Series
x510L Series
IX5-28GPX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-1.3.

Caution: SSH was upgraded in 5.5.1-1.1, to increase security. Some older SSH clients may no longer connect to your AlliedWare Plus device. To resolve this, see "Older SSH clients can't connect to AlliedWare Plus devices" on page 36.

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 48.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 50. 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		10/2021	vaa-5.5.1-1.3.iso (VAA OS) vaa-5.5.1-1.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-1.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2021	SBx81CFC960-5.5.1-1.3.rel
SBx908 GEN2	SBx908 GEN2	10/2021	SBx908NG-5.5.1-1.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	10/2021	x950-5.5.1-1.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	10/2021	x930-5.5.1-1.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2021	x550-5.5.1-1.3.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	10/2021	x530-5.5.1-1.3.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	10/2021	x510-5.5.1-1.3.rel
IX5-28GPX	IX5	10/2021	IX5-5.5.1-1.3.rel
x320-10GH x320-11GPT	x320	10/2021	x320-5.5.1-1.3.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	10/2021	x310-5.5.1-1.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2021	x230-5.5.1-1.3.rel
x220-28GS x220-52GT x220-52GP	x220	10/2021	x220-5.5.1-1.3.rel
IE510-28GSX	IE510-28GSX	10/2021	IE510-5.5.1-1.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	10/2021	IE340-5.5.1-1.3.rel
IE300-12GT IE300-12GP	IE300	10/2021	IE300-5.5.1-1.3.rel
IE210L-10GP IE210L-18GP	IE210L	10/2021	IE210-5.5.1-1.3.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	10/2021	IE200-5.5.1-1.3.rel
XS916MXT XS916MXS	XS900MX	10/2021	XS900-5.5.1-1.3.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	10/2021	GS980MX-5.5.1-1.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2021	GS980EM-5.5.1-1.3.rel
GS980M/52 GS980M/52PS	GS980M	10/2021	GS980M-5.5.1-1.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2021	GS970-5.5.1-1.3.rel

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

Models	Family	Date	Software File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	10/2021	GS900-5.5.1-1.3.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	10/2021	FS980-5.5.1-1.3.rel
AR4050S AR3050S	AR-series UTM firewalls	10/2021	AR4050S-5.5.1-1.3.rel AR3050S-5.5.1-1.3.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	10/2021	AR2050V-5.5.1-1.3.rel AR2010V-5.5.1-1.3.rel AR1050V-5.5.1-1.3.rel

Caution: Software version 5.5.1-1.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-1.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 44 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 46.

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

The 5.5.1-1.3 software version is ISSU compatible with previous software versions.

Enhancements

This section summarizes the enhancements in 5.5.1-1.3

SSH server secure commands

ER-4395: Available on FS980M, GS900MX/MPX, GS70M, GS980EM, GS980M, XS900MX, IE200, IE300, IE340, IE210L, IE510, x220, x230/x230L, x310, x320, IX5, x510/x510L, x530 / x530L, x550, x930, x950, SBx908Gen2, SBx81CFC960, AR1050V, AR2010V/AR2050V, AR3050S and AR4050S Series.

This software update provides two new global configuration commands.

The commands are:

- (no) **`ssh server secure-mac`** - enable SSH to use only strong MAC algorithms
- (no) **`ssh server secure-algs`** - enable SSH to use only strong ciphers, KEX and MAC algorithms

The command **`ssh server secure-algs`** is equivalent to using the commands: 'ssh server secure-ciphers' , 'ssh server secure-kex' and 'ssh server secure-mac'.

The command **`show ssh server`** output has been modified to include the list of currently allowed MAC algorithms.

```
Test#show ssh server
Secure Shell Server Configuration
-----------------------------------------------------------------
SSH Server          : Enabled
Protocol            : IPv4,IPv6
Port                : 22

...

MAC                 : umac-128-etm@openssh.com,
                      hmac-sha2-256-etm@openssh.com,
                      hmac-sha2-512-etm@openssh.com,
                      umac-64@openssh.com,umac-128@openssh.com,
                      hmac-sha2-256,hmac-sha2-512
```

IGMP snooping

ER-4305: Available on x950 Series and the SBx908 GEN2

With this software update, IGMP snooping now works correctly on x950 Series and SBx908 GEN2 switches if an IP multicast packet with TTL=1 is received.

Issues Resolved in Version 5.5.1-1.3

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-74029	**ACL**	Previously, an AlliedWare Plus device could restart when all the following conditions were true: ■ The HW space was full with ACLs and has no room to add any more. ■ An ACL has been applied to HW via a VLAN filter or a policy map. ■ The ACL (that is already applied in the previous bullet) was edited with a new filter being added. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-74068	**ACL, Policy-based-routing**	Previously, on SBx81CFC960 line cards, when a policy based routing rule was applied, followed by another ACL/QOS rule applied globally/per port, the policy based routing rule could fail to route the packets matching that rule. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73727	**ACL, VCStack**	Previously, when modifying an ACL with a large number of filters that was currently attached to a large number of interfaces: ■ if the operation apply time took longer than 10 minutes, it could trigger a system reboot. ■ also, exiting liveupdate mode after first running the **`commit`** command could cause all the changes to be re-applied again, even if no further changes were made. These issues have been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	–	–	–	–	–
CR-72009	**ARP / Neighbor Discovery**	Previously, gratuitous ARPs might result in receiving VLANs to incorrectly perform opportunistic neighbor discovery. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-73790	**Boot**	Previously, on rare occasions, an AlliedWare Plus device might fail to boot. The device would automatically reset itself after 10 minutes. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-74835	**Boot**	Previously, on very rare occassions, the AR2050V router could fail to boot up correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–
CR-74630	**CLI, PKI**	Previously, the PKI configuration could fail to run at bootup if there were spaces in the subject-name of a PKI Trustpoint. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73760	**DHCP Snooping**	Previously, DHCP Snooping ACLs may not have been installed correctly and could operate independently on each port. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-74247	**DPI**	This software update addresses the security vulnerability identified in CVE-2021-36082.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-74082	**IDS / IPS, URL Filter**	Previously, if an Ethernet packet with an error (e.g. FCS error) was received while an AR1050V was running either IPS or URL Filtering, it was possible for that error packet to get stuck in an infinite loop of processing. This would cause the CPU to ramp to 90% and stay there. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-74358	**IDS, IPS**	Previously, on devices with IPS enabled and "category http-events action deny" set, HTTP POST messages containing HTTP Multipart data (e.g. a form submission) might incorrectly be dropped. If this occurred, then an info-level log message would be generated in the form: IPS[4455]: [Drop] IPS: http-events HTTP multipart generic error URL:http://... This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-74752	**PoE**	With this software update, the PoE error message has been updated when an invalid signature is detected. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73557	**Port Authentication**	Previously, when dynamic VLANs were used in conjunction with MAC authentication, The MAC entry of the new supplicant could be incorrectly removed from the FDB table. The missing MAC may be detected by an auth audit and recovered along with a log message generated indicating the entry was missing. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-74342	**QoS, Switching**	Previously, if multiple policers, via service-policy, or QSP were added to the x530s series, then they would not work correctly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	Y	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-74465	**SNMP**	Previously, certain forms of memory corruption could cause the SNMP process to restart periodically. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-74667	**SSH**	Previously, the command **`crypto key destroy hostkey`** could fail to be executed in Secure Mode. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-74719	**SSH**	This software update enables the compatibility between older and new AlliedWare Plus versions using OpenSSH. It allows the device to check that an ECDSA host key exists when enabling the SSH service, and if not, it will create one. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-74495	**Storm Control**	Previously, storm-control configuration could not be applied to 40G ports on an XLEM card. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-74221	**System**	Previously, an internal error could occur in very rare cases that could deplete some of the switching system resources. Over time it was possible for this to eventually result in a VCStack separation. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-74751	**System**	Previously, (since 5.5.1-0.1 firmware), there was an increased memory consumption which could impact on the performance of Alliedware Plus devices. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	Y	Y	–

What's New in Version 5.5.1-1.2

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
x510 Series
IX5-28GPX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-1.2.

Caution: SSH was upgraded in 5.5.1-1.1, to increase security. Some older SSH clients may no longer connect to your AlliedWare Plus device. To resolve this, see "Older SSH clients can't connect to AlliedWare Plus devices" on page 36.

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 48.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 50. 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		08/2021	vaa-5.5.1-1.2.iso (VAA OS) vaa-5.5.1-1.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-1.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2021	SBx81CFC960-5.5.1-1.2.rel
SBx908 GEN2	SBx908 GEN2	08/2021	SBx908NG-5.5.1-1.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	08/2021	x950-5.5.1-1.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	08/2021	x930-5.5.1-1.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2021	x550-5.5.1-1.2.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	08/2021	x530-5.5.1-1.2.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	08/2021	x510-5.5.1-1.2.rel
IX5-28GPX	IX5	08/2021	IX5-5.5.1-1.2.rel
x320-10GH x320-11GPT	x320	08/2021	x320-5.5.1-1.2.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	08/2021	x310-5.5.1-1.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2021	x230-5.5.1-1.2.rel
x220-28GS x220-52GT x220-52GP	x220	08/2021	x220-5.5.1-1.2.rel
IE510-28GSX	IE510-28GSX	08/2021	IE510-5.5.1-1.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	08/2021	IE340-5.5.1-1.2.rel
IE300-12GT IE300-12GP	IE300	08/2021	IE300-5.5.1-1.2.rel
IE210L-10GP IE210L-18GP	IE210L	08/2021	IE210-5.5.1-1.2.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2021	IE200-5.5.1-1.2.rel
XS916MXT XS916MXS	XS900MX	08/2021	XS900-5.5.1-1.2.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	08/2021	GS980MX-5.5.1-1.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	08/2021	GS980EM-5.5.1-1.2.rel
GS980M/52 GS980M/52PS	GS980M	08/2021	GS980M-5.5.1-1.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2021	GS970-5.5.1-1.2.rel

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

Models	Family	Date	Software File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2021	GS900-5.5.1-1.2.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	08/2021	FS980-5.5.1-1.2.rel
AR4050S AR3050S	AR-series UTM firewalls	08/2021	AR4050S-5.5.1-1.2.rel AR3050S-5.5.1-1.2.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	08/2021	AR2050V-5.5.1-1.2.rel AR2010V-5.5.1-1.2.rel AR1050V-5.5.1-1.2.rel

Caution: Software version 5.5.1-1.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-1.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 44 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 46.

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

The 5.5.1-1.2 software version is ISSU incompatible with previous software versions.

New Features and Enhancements

This section summarizes the new features in 5.5.1-1.2.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 43.

Support for x530, x530L and GS980MX series

Version 5.5.1-1.2 supports all x530, x530L and GS980MX series switches. This means 5.5.1-1.2 supports the following new features:

New in 5.5.1-1.2:

- "Jumbo frames for Layer 3 switched traffic and control packets" on page 22
- "VXLAN Enhancements" on page 23
- "VCStack over 1G on the x530, x530L and GS980MX" on page 24

From 5.5.1-1.1, now supported on x530, x530L and GS980MX series switches:

- "RADIUS Change of Authorization" on page 29
- "Enhanced ping polling for web authentication" on page 30
- "Configuring a DHCP server to be VRF aware" on page 31
- "sFlow supports multiple collectors" on page 32
- "Guest node and Access Point SNMP traps" on page 33

Jumbo frames for Layer 3 switched traffic and control packets

Newly available on x530 and GS980MX series switches.

From version 5.5.1-1.2 onwards, jumbo frames are supported for Layer 3 switching and control packets. Once jumbo frame support is enabled, the maximum packet size can now be up to 9216 bytes for devices that support Layer 3 jumbo frames.

Jumbo frames for Layer 3 switches increases performance by minimizing the amount of packet overhead relative to the amount of data transmitted. For example, you could use jumbo frames in SAN (Storage Area Networks) which are dedicated networks used by servers to access block-level storage.

To configure jumbo frames for Layer 3 switching and control packets, you need to:

- turn on jumbo frame support, using the **platform jumboframe** command for the required switchports, and
- increase the MTU value, using the **mtu** command for the required VLANs.

For more information about how to configure Layer 3 jumbo frames for Layer 3 switches, see the Switching Feature Overview and Configuration Guide.

VXLAN Enhancements

Available on x530 Series

Virtual Extensible LAN (VXLAN) is an overlay encapsulation technology. It creates a virtual network overlaid on top of the existing physical network infrastructure. It uses the underlay IP network and builds a flexible Layer 2 overlay logical network on it.

Software version 5.5.1-1.2 includes some improvements and an aggregator enhancement.

Improvements

From version 5.5.1-1.2 onwards there have been some improvements made over what was supported in 5.5.1-0.x.

ARPs are automatically resolved for tunnel underlay nexthop

With this software version, VXLAN will automatically resolve an ARP for each remote VTEPs that is configured, and these will be automatically re-resolved after an ARP cache flush from the CLI and by other features such as STP, EPSR, auth, or as a result of ports going down and back up. This avoids the need for other underlay traffic or workarounds such as ping-polling to be put in place as recommended in the VXLAN Feature Overview and Configuration Guide.

VLAN ID and priority information taken from the overlay VLAN tag

Previously, if a VXLAN packet contained an overlay VLAN tag (i.e. a VLAN tag within the inner frame) then the following things would happen when the VXLAN encapsulation was removed:

- The inner frame was bridged into the VLAN indicated by the VLAN tag instead of the VLAN specified by the **map-access** configuration command.
- The Priority Code Point within the VLAN tag was preserved if the frame was forwarded out a trunk port.

This meant that with 5.5.1-0.x you had to manually configure a workaround using class maps and policy maps to drop these frames, as was shown in Rev A of the VXLAN Feature Overview and Configuration Guide with the PMAP_DROP_VXLAN_OVERLAY_TAGGED policy map and CMAP_DROP_VXLAN_OVERLAY_TAGGED class map configurations.

With 5.5.1-1.2 onwards, the manual policy-map workaround is no longer required. When the first VXLAN tunnel is added into hardware, a tunnel termination entry is also added that is used to drop 802.1Q VLAN tagged passenger packets. Only 1 global entry is added to cover all VXLAN tunnels. The entry is automatically removed when the last VXLAN tunnel is removed from hardware.

Aggregator enhancement

The x530 now supports aggregators as downlinks in a VXLAN scenario. Specifically that means that the local LAN side traffic can pass over aggregated ports to/from the x530, which can then encapsulate/decapsulate the traffic to/from a VXLAN tunnel. The VXLAN tunnel side (aka uplink) still does not support aggregators; the VXLAN tunnel must egress over a single port. This applies to both static and dynamic aggregators.

For more information on the VXLAN feature, see the VXLAN Feature Overview and Configuration Guide.

VCStack over 1G on the x530, x530L and GS980MX

Available on x530 and GS980MX Series

From 5.5.1-1.2 onwards, VCStack is supported on 1G copper ports and SFP ports on the x530 and x530L series (including x530DP models) and the GS980MX series.

VCStack, in conjunction with link aggregation, provides a highly available system where network resources are spread out across stacked units, providing excellent resiliency.

You can form a stack with up to 4 members using VCStack on 1G copper and SFP ports. Note that you can stack up to 8 units at 2.5/5/10G speeds.

Note: For any two directly linked stack members, all stackports must originate from a single packet processor and go to a single packet processor. For 52 port models, this means all 1G stackports to another member must be in the port range 1-24 or 25-52 (excluding 41-48 on models with 5G ports in that range).

For more information on VCStack, see the Virtual Chassis Stacking (VCStack) Feature Overview and Configuration Guide.

What's New in Version 5.5.1-1.1

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series[1]
x530L Series[1]
x510 Series
IX5-28GPX
x320 Series
x310 Series
x230 Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980MX Series[1]
GS980EM Series
GS980M Series
GS970M Series
GS900MX/MPX Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

1. x530, x530L and GS980MX series will be supported from 5.5.1-1.2

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-1.1.

Caution: SSH has been upgraded in 5.5.1-1.1, to increase security. Some older SSH clients may no longer connect to your AlliedWare Plus device. To resolve this, see "Older SSH clients can't connect to AlliedWare Plus devices" on page 36.

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 48.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 50. 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		08/2021	vaa-5.5.1-1.1.iso (VAA OS) vaa-5.5.1-1.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-1.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2021	SBx81CFC960-5.5.1-1.1.rel
SBx908 GEN2	SBx908 GEN2	08/2021	SBx908NG-5.5.1-1.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	08/2021	x950-5.5.1-1.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	08/2021	x930-5.5.1-1.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2021	x550-5.5.1-1.1.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L		Support coming in 5.5.1-1.2
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	08/2021	x510-5.5.1-1.1.rel
IX5-28GPX	IX5	08/2021	IX5-5.5.1-1.1.rel
x320-10GH x320-11GPT	x320	08/2021	x320-5.5.1-1.1.rel

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

Models	Family	Date	Software File
x310-26FT x310-26FP x310-50FT x310-50FP	x310	08/2021	x310-5.5.1-1.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2021	x230-5.5.1-1.1.rel
x220-28GS x220-52GT x220-52GP	x220	08/2021	x220-5.5.1-1.1.rel
IE510-28GSX	IE510-28GSX	08/2021	IE510-5.5.1-1.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	08/2021	IE340-5.5.1-1.1.rel
IE300-12GT IE300-12GP	IE300	08/2021	IE300-5.5.1-1.1.rel
IE210L-10GP IE210L-18GP	IE210L	08/2021	IE210-5.5.1-1.1.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2021	IE200-5.5.1-1.1.rel
XS916MXT XS916MXS	XS900MX	08/2021	XS900-5.5.1-1.1.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX		Support coming in 5.5.1-1.2
GS980EM/10H GS980EM/11PT	GS980EM	08/2021	GS980EM-5.5.1-1.1.rel
GS980M/52 GS980M/52PS	GS980M	08/2021	GS980M-5.5.1-1.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2021	GS970-5.5.1-1.1.rel

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

Models	Family	Date	Software File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2021	GS900-5.5.1-1.1.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	08/2021	FS980-5.5.1-1.1.rel
AR4050S AR3050S	AR-series UTM firewalls	08/2021	AR4050S-5.5.1-1.1.rel AR3050S-5.5.1-1.1.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	08/2021	AR2050V-5.5.1-1.1.rel AR2010V-5.5.1-1.1.rel AR1050V-5.5.1-1.1.rel

Caution: Software version 5.5.1-1.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-1.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 44 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 46.

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

The 5.5.1-1.1 software version is ISSU incompatible with previous software versions.

New Features and Enhancements

This section summarizes the new features in 5.5.1-1.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 43.

RADIUS Change of Authorization

Available on all devices that support port authentication.

From version 5.5.1-1.1 onwards, you can use the RADIUS Change of Authorization (CoA) feature to change a supplicant's VLAN access, or terminate a supplicant's session, while that supplicant's session is in progress.

In a typical authorization scenario, a supplicant requests permission to join a network using one of the three authentication methods, 802.1X, MAC-based, or web-based. The authenticator, also known as the Network Access Server (NAS), passes the supplicant's credentials to the RADIUS server, which will either accept or reject the request. When accepting the request the RADIUS server can also set certain characteristics of the supplicant's session, such as which VLAN they can access.

The RADIUS protocol does not support unsolicited messages from the RADIUS server to the authenticator. This means that once a supplicant has been authorized their session characteristics cannot be changed unless the RADIUS server is updated and the supplicant re-authenticates. RADIUS CoA allows an administrator to change a supplicant's session characteristics, or terminate a supplicant's session, without the need for the supplicant to re-authenticate.

When RADIUS CoA is configured, your AlliedWare Plus authenticator (NAS) acts as a Dynamic Authorization Server (DAS). This means it accepts CoA messages from a Dynamic Authorization Client (DAC). To setup your device as a DAS you just need to add the DAC to a list of authorized DACs using the following command:

```
radius dynamic-authorization-client <ip-address>
key <key-string>
```

You will also need to configure port authentication and a RADIUS server on your device.

For more information on the AlliedWare Plus implementation of port authentication and RADIUS CoA, see the AAA and Port Authentication Feature Overview and Configuration Guide.

ACL Memory Optimization

Newly available on SBx81CFC960, x320, x220, GS980EM, GS980M, and FS980M series switches. Already supported on x530, x530L and GS980MX series switches

From 5.5.1-1.1 onwards, ACL memory usage is more efficient.

Previously, global rules were duplicated for each port that had a per-port rule, which increased memory usage. With this software version, ports are able to share some rules to optimize total ACL memory usage.

You can see this in the output of the command **show platform classifier statistics utilization brief**. The output will now show fewer entries occupied.

Before software version 5.5.1-1.1:

```
awplus#show platform classifier statistics utilization brief
...
                    Used/Total
...
Global ACL          84
ACL                 28
...
Total               112 /   512 (21.88%)
```

After software version 5.5.1-1.1:

```
awplus#show platform classifier statistics utilization brief
...
                    Used/Total
...
Global ACL          3
ACL                 1
...
Total               4 /   512 (0.78%)
```

Enhanced ping polling for web authentication

Available on all devices except AR1050V, AR2010V, and AMF Cloud

From version 5.5.1-1.1 onwards, you can use ARP ping polling to check that a web authenticated supplicant (client device), is still connected.

A new command is available:

```
[no] auth-web-server ping-poll type {arp|ping}
```

Use this command to set the type of polling used to check that a web authenticated supplicant is still connected. The polling can be done using the default ICMP (ping) messages, or ARP messages. ARP polling works when a firewall is present, while ICMP is sometimes blocked by a firewall. The polling will not start until ping-polling is enabled and the supplicant has been authorized.

For example, to set the polling type to ARP, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
awplus(config)# auth-web-server ping-poll type arp
```

For more information on the web-authentication and ping polling, see the AAA and Port Authentication Feature Overview and Configuration Guide.

Configuring a DHCP server to be VRF aware

Available on SBx81CFC960, SBx908 GEN2, x950, x930, AR4050S, AR3050S, AR2050V. Will be available on x530 Series from 5.5.1-1.2 onwards

From version 5.5.1-1.1 onwards, you can configure a DHCP server to be VRF aware. This means you can associate a VRF with a DHCP address pool and (optionally) use the same DHCP lease across multiple isolated networks. You can configure DHCP pools with the same or different network and address ranges associated with each.

New Command

There is a new command: vrf <name> which allows you to add a VRF name to a DHCP server's address pool.

For example, to add the VRF named 'red' to the DHCP address pool named 'red_pool', use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool red_pool
awplus(dhcp-config)# vrf red
```

Updated commands

The following commands have been updated as follows:

- **show ip dhcp server statistics** - includes a new parameter: `vrf <name>`
- **show ip dhcp server statistics** - displays VRF information
- **show counter dhcp-server** - displays VRF information
- **show ip dhcp binding** - displays VRF information
- **clear ip dhcp binding** - includes support for VRF

VLAN-based Q-in-Q with DHCP snooping

Available on SBx81CFC960

From version 5.5.1-1.1 (and 5.5.1-0.3) onwards, the SBx8100 supports VLAN-based Q-in-Q (VLAN stacking) for DHCP snooped packets.

For more information about VLANs and Q-in-Q (VLAN stacking) on your device, see the VLANs Feature Overview and Configuration Guide. For more information about DHCP snooping, see the DHCP Snooping Feature Overview and Configuration Guide.

sFlow supports multiple collectors

Available on SBx81CFC960, SBx908 GEN2, x950, x930, x550, x510, IX5, x320, x310, x230, x230L, x220, IE510, IE340, IE300, IE210L, GS980EM, and GS970M Series switches. Will be available on x530 and x530L Series from 5.5.1-1.2 onwards

sFlow is a network monitoring protocol which provides a means for collecting packets, together with interface counters, and then exporting them to an external collector. The collector displays statistics about the traffic flowing through the device.

From software version 5.5.1-1.1 onwards, you can configure multiple collectors. Previously, you could only configure a single collector.

A new command is available to create up to five collectors: **sflow collector id**

```
sflow collector id <1-5> ip <ip-address> [port <1-65535>|max-datagram-size <200-1500>]
sflow collector id <1-5> ipv6 <ipv6-address> [port <1-65535>|max-datagram-size <200-1500>]
no sflow collector id <1-5>
```

The key for adding and deleting collectors is the collector ID. Port and max-datagram-size are optional parameters and the default values are used if unset.

For example, to set the address of collector 1 to 192.168.1.36 with default port and max-datagram size, use the commands:

```
awplus# configure terminal
awplus(config)# sflow collector id 1 ip 192.168.1.36
```

Deprecated commands

The command **sflow collector id** deprecates the following two sFlow commands:

- sflow collector
- sflow collector max-data-gram size

Existing sFlow configurations are automatically converted into the new format when you update your AlliedWare Plus software version.

For more information on the sFlow feature, see the sFlow Feature Overview and Configuration Guide.

Media Redundancy Protocol (MRP) supported on VCStack

Available on x930 Series and IE510-28GSX switches

From 5.5.1-1.1 onwards, MRP is supported in Virtual Chassis Stacking environments.

For more information on VCStack, see the Virtual Chassis Stacking (VCStack) Feature Overview and Configuration Guide.

For more information on MRP, see the Media Redundancy Protocol (MRP) Feature Overview and Configuration Guide.

Guest node and Access Point SNMP traps

AMF guest node SNMP traps: available on all AMF Master devices that support guest nodes and SNMP traps.

Access point SNMP Traps: available on all AlliedWare Plus devices that support the AWC Wireless Manager and SNMP traps.

From 5.5.1-1.1 onwards, guests nodes joining or leaving the network will now create a trap notification. You can use the **snmp-server enable trap atmfguestnode** command to enable or disable these traps. You can use the **type atmf guest** command to create a trigger to execute on these events.

In addition, when an AP enters or leaves the managed state, it will now create a trap notification. You can use the **snmp-server enable trap cwmap** command to enable or disable these traps.

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

MACsec on XEM2-12XS v2 and XEM2-8XSTm

Available on SBx908 GEN2 and x950 Series

MACsec (Media Access Control Security) provides line-rate encryption and protection of traffic passing over a Layer 2 network or link.

Software version 5.5.1-1.1 adds support for MACsec on:

- x950 (XEM2-12XS v2 and ports 5-8 on the XEM2-8XSTm)
- SBx908 GEN2 (XEM2-12XS v2 and ports 5-8 on the XEM2-8XSTm)

in addition to previous support for MACsec on:

- x930 (all front panel 1G ports)
- x950 (XEM2-12XS)
- SBx908 GEN2 (XEM2-12XS)

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

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.1-x.x and may affect your device or network behavior if you upgrade:

- Older SSH clients can't connect to AlliedWare Plus devices
- Upgrade compatibility for SBx908 GEN2 and x950 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

If you are upgrading from an earlier version than 5.5.1-x.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.0-1.x version, please check the 5.5.0-2.x release note. Release notes are available from our website, including:

- 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

Older SSH clients can't connect to AlliedWare Plus devices

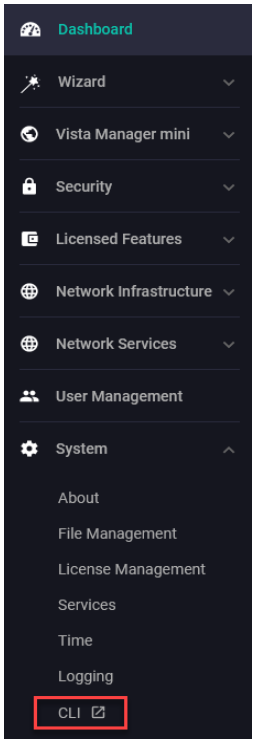
In AlliedWare Plus version 5.5.1-1.1, OpenSSH was upgraded. This means 5.5.1-1.x no longer supports the following insecure options:

- the ssh-rsa algorithm in OpenSSH, which is based on SHA1
- SSH protocol version 1

Unfortunately, some older SSH clients and older libraries still expect to use ssh-rsa. Therefore, before you upgrade to 5.5.1-1.x, we recommend you:

- ensure your SSH client is up to date, and
- create an ECDSA key for the server to use in case the client does not support secure SSH RSA algorithms

To create the ECDSA key, use the following steps:



1. Access the CLI of the AlliedWare Plus device. If you have already upgraded to 5.5.1-1.x and can no longer use your SSH client, you can access the device through its console port or its GUI as shown in this screenshot.

2. Create an ECDSA key using the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey ecdsa 384
```

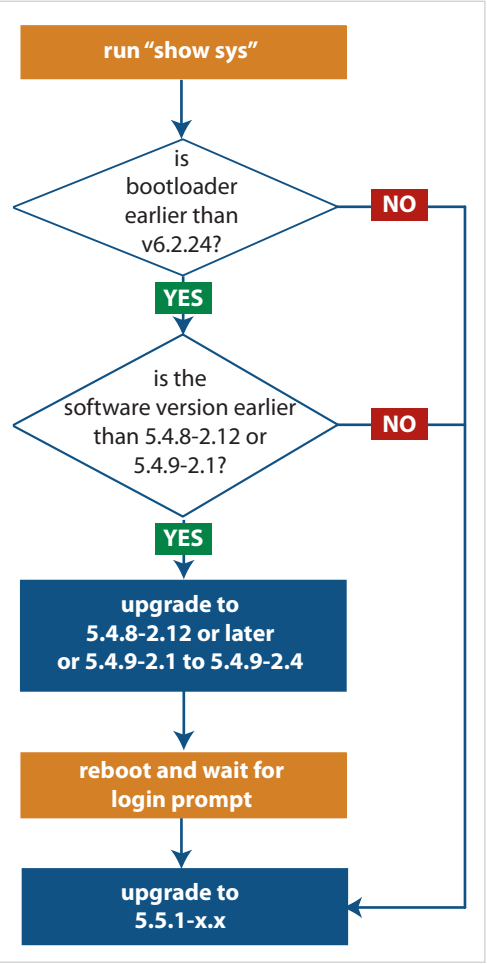
3. Either reboot the device, or turn the SSH service off and on again, using the commands:

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

Note that you only need to do this procedure on existing AlliedWare Plus devices. From 5.5.1-1.1 onwards, AlliedWare Plus automatically creates an ECDSA key on factory-new devices and devices that have been returned to a factory state.

Upgrade compatibility for SBx908 GEN2 and x950 Series switches

On the SBx908 GEN2 and x950 Series switches, please check your bootloader and current software version before you upgrade to AlliedWare Plus version 5.5.1-x.x.



If your bootloader is older than 6.2.24, you can only upgrade to 5.5.1-x.x from the following software versions:

- 5.4.8-2.12 or a later 5.4.8-2.x version,
- or 5.4.9-2.1, 5.4.9-2.2, 5.4.9-2.3 or 5.4.9-2.4
- or any 5.5.0-x.x or 5.5.1-x.x version

If your bootloader is older than 6.2.24, your switch must be running one of the above versions when you upgrade to 5.5.1-x.x.

If your bootloader is older than 6.2.24, you cannot upgrade to 5.5.1-x.x directly from:

- **5.4.9-1.x,**
- **5.4.9-0.x, or**
- **any version before 5.4.8-2.12**

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

```
awplus# show system
```

If you experience issues when upgrading, please contact your Allied Telesis support team. See our website at alliedtelesis.com/support.

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
Some commands not available when accessing CLI via Vista Manager	*All Alliedware Plus devices*	From 5.5.1-0.1 onwards, users accessing the AlliedWare Plus command line via Vista Manager are unable to use the following CLI commands: ■ atmf select-area ■ no atmf select-area

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.1 license on your switch if you are upgrading to 5.5.1-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 44 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 46.

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 5.5.1-1.x from:

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

On these switches, you **cannot** use rolling reboot to upgrade to 5.5.1-1.x 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 5.5.1-1.x from:

- 5.5.1-0.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 5.5.1-1.x from:

- 5.5.1-0.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 5.5.1-1.x and:

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

On these switches, auto-synchronization is not supported between 5.5.1-1.x 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 5.5.1-1.x and:

- 5.5.1-0.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 5.5.1-1.x and:

- 5.5.1-0.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 5.5.1-0.x and 5.4.6-1.1 or **any** earlier releases.

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

If using an AMF controller

If your Controller or **any** of your Masters are running 5.4.7-1.1 or later, then the Controller and **all** of the Masters must run 5.4.7-1.1 or later. However, the software on Member nodes can be older than 5.4.7-1.1. Otherwise, the "show atmf area nodes" command and the "show atmf area guests" command will not function, and Vista Manager EX will show incorrect network topology.

If using secure mode

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

If using Vista Manager EX

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

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

If using none of the above

If none of the above apply, then nodes running version 5.5.1-1.x are compatible with nodes running:

- 5.5.1-0.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 Feature Guides in the right-hand menu.
- **Datasheets** - find these by searching for the product series and then selecting Datasheets in the right-hand menu.
- **Installation Guides** - find these by searching for the product series and then selecting Installation Guides in the right-hand menu.
- **Command References** - find these by searching for the product series and then selecting Manuals in the right-hand menu.

Verifying the Release File

On 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 checksum of the file.

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

Caution

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

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

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

Licensing this Version on an SBx908 GEN2 Switch

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

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

1. Obtain the MAC address for a switch

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

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

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

2. Obtain a release license for a switch

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

3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

```
awplus#show license

Board region: Global

Index                          : 1
License name                   : Base License
Customer name                  : Base License
Type of license                : Full
License issue date             : 20-Mar-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                   : 5.5.1
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Aug-2021
License expiry date            : N/A
Release                        : 5.5.1
```

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                   : 5.5.1
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Aug-2021
License expiry date            : N/A
Release                        : 5.5.1
```

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 44 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 46.

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

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

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

Product	Command
SBx8100 with CFC960	`awplus(config)# boot system SBx8100-5.5.1-1.4.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.1-1.4.rel`
x950 series	`awplus(config)# boot system x950-5.5.1-1.4.rel`
x930 series	`awplus(config)# boot system x930-5.5.1-1.4.rel`
x550 series	`awplus(config)# boot system x550-5.5.1-1.4.rel`
x530 series	`awplus(config)# boot system x530-5.5.1-1.4.rel`
x510 series	`awplus(config)# boot system x510-5.5.1-1.4.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.5.1-1.4.rel`
x320 series	`awplus(config)# boot system x320-5.5.1-1.4.rel`
x310 series	`awplus(config)# boot system x310-5.5.1-1.4.rel`
x230 series	`awplus(config)# boot system x230-5.5.1-1.4.rel`
x220 series	`awplus(config)# boot system x220-5.5.1-1.4.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.5.1-1.4.rel`

Product	Command
IE340 series	`awplus(config)# boot system IE340-5.5.1-1.4.rel`
IE300 series	`awplus(config)# boot system IE300-5.5.1-1.4.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.1-1.4.rel`
IE200 series	`awplus(config)# boot system IE200-5.5.1-1.4.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.1-1.4.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.1-1.4.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.1-1.4.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.1-1.4.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.1-1.4.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.5.1-1.4.rel`
FS980M series	`awplus(config)# boot system FS980-5.5.1-1.4.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.1-1.4.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.1-1.4.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.5.1-1.4.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.1-1.4.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.1-1.4.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
   ```

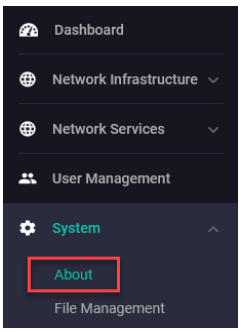
   Alternatively, on unconfigured devices you can use the default address, which is:

   - 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 5.5.1-1.4 is 2.9.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 51 or "Update the GUI on AR-Series devices" on page 52.

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 filename for v2.9.0 of the GUI is awplus-gui_551_24.gui.

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

2. Log into the GUI:

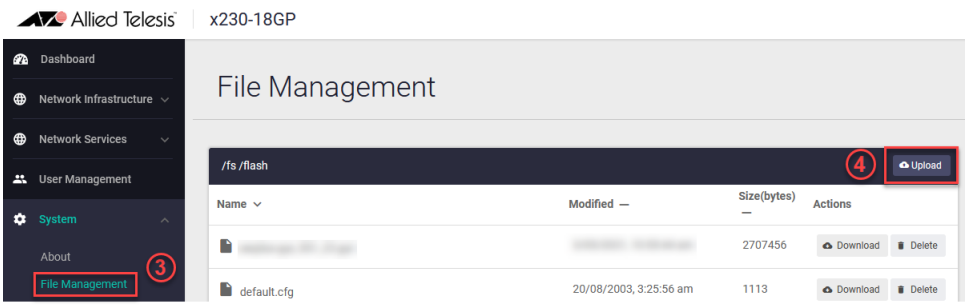
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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 v2.9.0 or later.