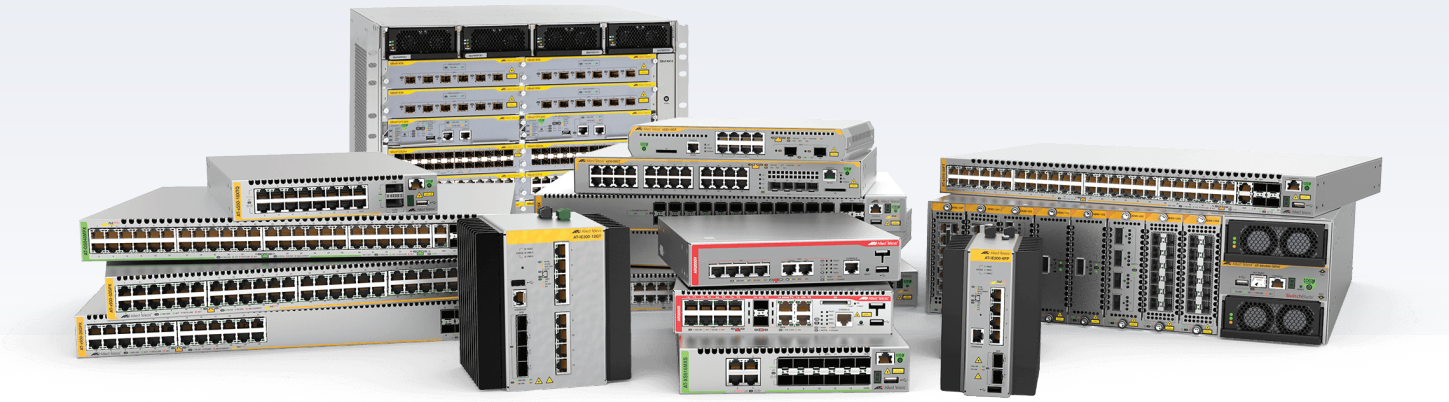
Release Note for AlliedWare Plus Software Version 5.5.0-1.x



AlliedWare Plus OPERATING SYSTEM

» 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 » GS980M Series » GS980EM Series » GS970M Series

» GS900MX/MPX Series » FS980M Series » AMF Cloud

» AR4050S » AR3050S » AR2050V » AR2010V » AR1050V

» 5.5.0-1.1 » 5.5.0-1.2 » 5.5.0-1.3 » 5.5.0-1.4 » 5.5.0-1.5

Acknowledgments

Getting the most from this Release Note

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

Content

What's New in Version 5.5.0-1.5

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
x510 Series
x510L Series
IX5-28GPX
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
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 5.5.0-1.5.

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.

Caution: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 69.

For instructions on how to update the web-based GUI, see "Installing and Accessing the Web-based GUI on Switches" on page 71 or "Installing and Accessing the Web-based GUI on AR-Series Devices" on page 74. 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		01/2021	vaa-5.5.0-1.5.iso (VAA OS) vaa-5.5.0-1.5. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-1.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	01/2021	SBx81CFC960-5.5.0-1.5.rel
SBx908 GEN2	SBx908 GEN2	01/2021	SBx908NG-5.5.0-1.5.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	01/2021	x950-5.5.0-1.5.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	01/2021	x930-5.5.0-1.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2021	x550-5.5.0-1.5.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX x530L-28GPX x530L-28GTX x530L-52GTX	x530 and x530L	01/2021	x530-5.5.0-1.5.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	01/2021	x510-5.5.0-1.5.rel
IX5-28GPX	IX5	01/2021	IX5-5.5.0-1.5.rel
x320-10GH x320-11GPT	x320	01/2021	x320-5.5.0-1.5.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	01/2021	x310-5.5.0-1.5.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2021	x230-5.5.0-1.5.rel
x220-28GS x220-52GT x220-52GP	x220	01/2021	x220-5.5.0-1.5.rel
IE510-28GSX	IE510-28GSX	01/2021	IE510-5.5.0-1.5.rel
IE340-12GT[1] IE340-12GP IE340-20GP IE340L-18GP	IE340	01/2021	IE340-5.5.0-1.5.rel
IE300-12GT IE300-12GP	IE300	01/2021	IE300-5.5.0-1.5.rel
IE210L-10GP IE210L-18GP	IE210L	01/2021	IE210-5.5.0-1.5.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	01/2021	IE200-5.5.0-1.5.rel
XS916MXT XS916MXS	XS900MX	01/2021	XS900-5.5.0-1.5.rel
GS980EM/10H GS980EM/11PT	GS980EM	01/2021	GS980EM-5.5.0-1.5.rel
GS980M/52 GS980M/52PS	GS980M	01/2021	GS980M-5.5.0-1.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2021	GS970-5.5.0-1.5.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	01/2021	GS900-5.5.0-1.5.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	01/2021	FS980-5.5.0-1.5.rel
AR4050S AR3050S	AR-series UTM firewalls	01/2021	AR4050S-5.5.0-1.5.rel AR3050S-5.5.0-1.5.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	01/2021	AR2050V-5.5.0-1.5.rel AR2010V-5.5.0-1.5.rel AR1050V-5.5.0-1.5.rel

1.Recently added models: IE340-12GT, IE340-12GP

Caution: Software version 5.5.0-1.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-1.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 65 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 67.

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

The 5.5.0-1.5 software version is ISSU compatible with previous software versions.

Enhancements in Version 5.5.0-1.5

Reducing IGMP hardware entries

Available on XS900MX, FS980, GS900MX, GS980M, GS980MX, x320, x530, x530L, x550, x930, x950, SBx8100 CFC960, and SBx908 GEN2 Series.

From version 5.5.0-1.5 onwards, a new multicast command is available:

```
ip igmp flood-group
```

This command adds an all sources multicast entry into the switches multicast hardware table to flood multicast packets to all ports within the VLAN without mirroring the traffic to the CPU. This significantly reduces the number of hardware entries consumed.

To configure an IGMP flooding group to L2 ports only use the following commands. This will flood any UDP packet to group 239.255.255.250 to all ports in vlan1.

```
awplus(config)#int vlan1
awplus(config-if)#ip igmp flood-group 239.255.255.250
```

For more information on IGMP flooding, see the IGMP/MLD Feature Overview and Configuration Guide.

Improvements to flash file sytem

Available on x220, x530, x530L, x550, and SBx8100 CFC960 Series

From version 5.5.0-1.5 onwards, an improvement has been made to the flash file system on certain platforms.

Previously, on platforms that used NAND flash, bit flips in erased pages could lead to uncorrectable errors and a reformatting of the file system. This issue has been resolved.

Configure SSH server to use only best-current-practice key exchange algorithms

Available on AlliedWare Plus devices

From version 5.5.0-1.5 onwards, the AlliedWare Plus SSH server has been modified to allow users to specify only key exchange algorithms which are consistent with key exchange algorithms currently considered as best-current-practice to be used by the SSH server and the algorithm list does not include diffie-hellman-group-exchange-sha1 key exchange algorithm.

The new command is as follows:

```
awplus(config)#(no) ssh server secure-kex
```

Specifying the command will result in the following key exchange algorithms being used by the AlliedWare Plus SSH server:

- curve25519-sha256@libssh.org,
- ecdh-sha2-nistp521
- ecdh-sha2-nistp384
- ecdh-sha2-nistp256
- diffie-hellman-group-exchange-sha256

The **show ssh server** command output has also been modified to show the current ciphers in use.

For example:

```
awplus(config)#show ssh server

Secure Shell Server Configuration
-----------------------------------------------------------------------------
SSH Server : Disabled
Protocol : None
Port : 22
Version : 2,1
Services : scp, sftp
User Authentication : publickey, password
Resolve Hosts : Disabled
Session Timeout : 0 (Off)
Login Timeout : 60 seconds
Maximum Authentication Tries : 6
Maximum Startups : 10
Debug : NONE
Ciphers : aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
KEX : curve25519-sha256@libssh.org,
                                        ecdh-sha2-nistp521,ecdh-sha2-nistp384,
                                        ecdh-sha2-nistp256,
                                        diffie-hellman-group-exchange-sha256 "
```

Issues Resolved in Version 5.5.0-1.5

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70764	**ACL**	Previously, it was not possible to edit a hardware access-list containing an ACL-Group after it was applied to an interface on certain 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	–	–	–	–	–
CR-70236	**AMF**	Previously, when a device connected via an AMF link, was moved from one upstream device to a different upstream device and both upstream devices had virtual uplinks, it was possible that Layer 3 communication might not resume for the device. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-70998	**Device GUI, HTTP Service, Web API**	Previously, it was possible to download certain files from the device over HTTPS without authorization if the: ■ HTTP service was enabled ■ AlliedWare Plus Device GUI was not installed on the device. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-70704	**DHCP Client IPv6**	Previously, a state change, either an IPv6 address being removed, or configuration changing, could cause the IPv6 prefix to no longer be advertised. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70921	**DHCP Client IPv6**	Previously, when a DHCPv6 client had been assigned with a prefix by an upstream DHCPv6 server, and the server changed the prefix assignment to a different prefix, resetting the upstream interface could cause the default route via the upstream server to disappear. 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-71037	**DHCP Client IPv6**	Previously, a DHCPv6-PD client configured with the **`default-route-to-server`** command might end up with multiple default routes, after the upstream link went down and up again accompanied by a change of DHCP server. As a result, the default route with the nexthop of the previous DHCP server would fail to be withdrawn. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-71616	**DHCPv6 Client, IPv6**	Previously, if an AlliedWare Plus DHCP client received a reply with status code of "NoBinding" after sending a "REBIND", then it would keep using the assigned address until expiry. This meant that the server pool could have been renumbered without doing a RECONFIGURE, or the server could have been replaced by a new server with a different address pool, but the client would not be updated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71129	**DHCPv6 Prefix Delegation**	Previously, when a DHCPv6-PD client was running on an interface (connected to the PD server), if: ■ the interface went down and up multiple times ■ and the PD server assigned different prefixes resulting in a DHCPv6 rebind and reply packets exchanges, then occasionally the NSM module could undergo an unexpected re-boot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–
CR-71215	**DHCPv6 Prefix Delegation**	Previously, if a DHCP-PD client received prefix-delegations for a new prefix with lifetimes of 0, the AlliedWare Plus management daemon could restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-69890	**Firewall - IPS**	Previously some active FTP connections could not be tracked by IPS with its default built-in rules. This issue has been resolved by introducing a new IPS category that specifically tracks active FTP connections.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70309	**IGMP Snooping**	Previously, packets destined to the IPv4 all-routers address could have been incorrectly blocked in hardware after IGMP snooping was disabled and re-enabled. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-71194	**IPv6 Tunnel**	Previously, for source IPv6 prefix selection, MAP-E used to select the first IPv6 prefix found that was in the vendor accepted range. With this software update, MAP-E now, in addition to checking the vendor accepted range, prefers undeprecated IPv6 prefixes over deprecated IPv6 prefixes for source IPv6 prefix selection. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-71387	**IPv6 Tunnel**	Previously, MAP-E used to request map rules in a loop when multiple upstream IPv6 prefixes were used. This issue has been resolved. With this software update, it now uses the most valid address, based on if it is deprecated or not.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70746	**IPv6 Tunneling**	Previously, MAP-E used to update configuration even if both the running configuration and the new configuration had an empty field. Also, previously, an update on MAP-E rules could occur regardless if there was a configuration change. These issues have been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70836	**IPv6 Tunneling**	Previously, MAP-E could sometimes add dynamic addresses with incorrect lifetimes. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70068	**MLDv2** **IGMPv3**	Previously L2 and L3 multicast hardware entries on some switch platforms could be unexpectedly removed in MLDv2 or IGMPv3 networks when the command **`platform l2mc-overlap`** was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70789	**Multicast routing**	Previously the error log "*No more free mll pairs*" could be generated frequently due to a slight mis-match between the software and hardware MLL table limit on some LIFs. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-70937	**Multicast Routing**	Previously, shadow multicast routes were not aged out on VCStack backup members, which had the potential to cause "*multicast table full*" errors following a failover. This issue has been resolved by enabling ageing on multicast routes for VCStack backup members.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-71897	**Multicasting Forwarding Hardware**	Previously, IP IGMP flooding groups were not forwarding the traffic correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-59904	**PoE**	Previously, the IE300 could not power some 60W PoE cameras due to differences in pre-802.3bt standard implementations. Now you can use the command **`power-inline disconnect-defer`** to power these devices correctly. This command defers the DC disconnect detection in hardware. Some 60W PDs take longer than the 802.3at standard time for drawing the minimum DC current on an individual pair. By deferring the enabling of the DC disconnect logic it allows both sets of pairs to power up and start drawing current. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70785	**Policy Based Routing (PBR)**	Previously when **`match tcp-flag`** was set in a class-map, any PBR nexthops within the same policy-map may not have been automatically resolved when matching traffic flows through the device. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-70923	**Port Authentication**	Previously, application of a dynamic VLAN by port authentication would not work if that VLAN was preceded by a user named VLAN in the VLAN database. This issue only occurred if the two VLANs had consecutive VIDs. This issue has been resolved.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-70388	**Private VLAN** **MLD Snooping**	Previously an error message - for example: `"DBG:hsl_hw_impl_l2_add_fdb 1802: Could not add MC MAC. ifx 5002 3333.ff9d.e1cb vid 2"` could be generated when IPv6 multicast traffic was received on a member port of a private VLAN on which MLD snooping was enabled. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-70672	**Routing**	Previously, if a connected route was down (for example due to the VLAN interface being shut down) and was replaced by a route from a routing protocol, then when the VLAN came back up the connected route could fail to be reinstated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70899	**SSH Server**	The AlliedWare Plus SSH server has been modified to allow users to specify only key exchange algorithms which are consistent with key exchange algorithms currently considered as best-current-practice to be used by the SSH server and the algorithm list does not include diffie-hellman-group-exchange-sha1 key exchange algorithm. The new command is as follows: (no) ssh server secure-kex For more information, see **"Enhancements in Version 5.5.0-1.5" on page 5**	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-70914	**System**	Previously, if an interface was configured with AN IPv6 address derived from a prefix appended to the eui64 address of the interface, and the interface performed router advertisement for the same prefix, then the address would have decrementing lifetimes, and eventually the address would have lifetimes of zero. As a result, the address would no longer be used for the interface, which caused the routing to cease on that interface. 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	–
CR-71468	**Tunnel**	Previously, after changing the IP address on a tunnel, traffic was not being forwarded. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70866	**USB Modem**	Previously after a reboot or power cycle some external USB modems would not always transition to link up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–		–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-68827	**VLAN**	Previously, on x530 series and SBx8100 switches, If a VLAN classifier was applied on an interface, packets received matching that VLAN classifier on another interface could be incorrectly dropped. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–

What's New in Version 5.5.0-1.4

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
x510 Series
x510L Series
IX5-28GPX
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
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 5.5.0-1.4.

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.

Caution: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 69.

For instructions on how to update the web-based GUI, see "Installing and Accessing the Web-based GUI on Switches" on page 71 or "Installing and Accessing the Web-based GUI on AR-Series Devices" on page 74. 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		11/2020	vaa-5.5.0-1.4.iso (VAA OS) vaa-5.5.0-1.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-1.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2020	SBx81CFC960-5.5.0-1.4.rel
SBx908 GEN2	SBx908 GEN2	11/2020	SBx908NG-5.5.0-1.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	11/2020	x950-5.5.0-1.4.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2020	x930-5.5.0-1.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2020	x550-5.5.0-1.4.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX x530L-28GPX x530L-28GTX x530L-52GTX	x530 and x530L	11/2020	x530-5.5.0-1.4.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	11/2020	x510-5.5.0-1.4.rel
IX5-28GPX	IX5	11/2020	IX5-5.5.0-1.4.rel
x320-10GH x320-11GPT	x320	11/2020	x320-5.5.0-1.4.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2020	x310-5.5.0-1.4.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2020	x230-5.5.0-1.4.rel
x220-28GS x220-52GT x220-52GP	x220	11/2020	x220-5.5.0-1.4.rel
IE510-28GSX	IE510-28GSX	11/2020	IE510-5.5.0-1.4.rel
IE340-20GP IE340L-18GP	IE340	11/2020	IE340-5.5.0-1.4.rel
IE300-12GT IE300-12GP	IE300	11/2020	IE300-5.5.0-1.4.rel
IE210L-10GP IE210L-18GP	IE210L	11/2020	IE210-5.5.0-1.4.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2020	IE200-5.5.0-1.4.rel
XS916MXT XS916MXS	XS900MX	11/2020	XS900-5.5.0-1.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2020	GS980EM-5.5.0-1.4.rel
GS980M/52 GS980M/52PS	GS980M	11/2020	GS980M-5.5.0-1.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2020	GS970-5.5.0-1.4.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2020	GS900-5.5.0-1.4.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	11/2020	FS980-5.5.0-1.4.rel
AR4050S AR3050S	AR-series UTM firewalls	11/2020	AR4050S-5.5.0-1.4.rel AR3050S-5.5.0-1.4.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	11/2020	AR2050V-5.5.0-1.4.rel AR2010V-5.5.0-1.4.rel AR1050V-5.5.0-1.4.rel

Caution: Software version 5.5.0-1.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-1.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 65 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 67.

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

The 5.5.0-1.4 software version is ISSU compatible with previous software versions.

Enhancements in Version 5.5.0-1.4

PPPoE relay

Version 5.5.0-1.4 supports PPPoE relay on AR Series Routers

PPPoE is a common deployment method for ISPs, allowing them to utilize PPP facilities for identifying and authenticating individual users.

The PPPoE RFC 2516 allows for an intermediate relay device, located between the Host operating as a PPPoE client and an Access Concentrator. This device relays the PPPoE Active Discovery packets and the subsequent PPPoE session packets between the Host and the Access Concentrator as though they are in the same Layer 2 domain.

PPPoE relay tracks state information for multiple Layer 2 PPPoE sessions, and allows multiple PPPoE client connections to be relayed between one or more client LANs and a WAN, allowing access to one or more service provider PPPoE Access Concentrators - whilst at the same time allowing Layer 3 IP traffic routing from the internal LAN(s) to the Internet. For more information on PPPoE relay and how to configure it, see the PPP Feature Overview and Configuration Guide.

Issues Resolved in Version 5.5.0-1.4

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70647	**ACS**	Previously, detection of the AMF-Sec-Mini GUI URL that was displayed in the Device GUI was not working correctly, and the 'Open' button was not displayed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	Y	–
CR-64604	**AMF**	Previously, it was possible that the order of configuring the AMF functionality could incorrectly update an internal database that VISTA manager relied upon. As a result, VISTA manager did not display the correct network topology. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-69724	**AMF**	Previously, the transitioning of an AMF node from AMF member to AMF master could lead to an inconsistent setting of the restricted login functionality across the network. This setting is generally controlled and communicated to the network by the AMF master. Due to the restricted login, functionality was being erroneously enabled on some devices. User logins were delayed for 15 seconds as the AMF functionality attempted to contact neighbouring nodes, which eventually failed 15 seconds later. This update ensures the consistency of the AMF restricted login functionality across the network. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70236	**AMF**	Previously, when a device connected via an AMF link, was moved from one upstream device to a different upstream device and both upstream devices had virtual uplinks, it was possible that Layer 3 communication might not resume for the device. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-70488	**AMF**	Previously, AMF provisioning in secure mode could fail. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-70586	**AMF**	Previously, when executing the **`write config`** command on an AMF node connected to another AMF node via a virtual-link, it could fail to distribute a recovery configuration file to all directly connected (downlink, crosslink) adjacent nodes. It could also fail to store a recovery configuration file on any inserted media device (USB/SDCARD). 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
CR-70380	**FAN**	With this software update, the fan profile on x530 PoE variants have been improved to allow for quieter operation.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-70360	**IPv6**	Previously, the IPv6 prefixes specified with minimum lifetimes were incorrectly advertised with the default lifetimes value instead. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70378	**IPv6**	With this software update, the preferred and valid lifetime values of IPv6 advertised in AWP router advertisements will now be the lower of the valid and preferred lifetimes of: ■ the prefix in the configuration ■ any address that matches that prefix on the outgoing interface (i.e an address statically assigned to the interface with non default lifetimes)	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70209	**LLDP**	Previously, Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) packets could be missing Type-Length Values (TLVs). As a result, the device could not respond correctly to other devices Logical Link Control Protocol Data Units (LLPDUs). 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-57296	**Open VPN**	This software update addresses the open VPN vulnerabilities stated in CVE-2017-7478.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-57947	**OpenVPN**	This software update addresses the open VPN vulnerabilities stated in CVE-2017-7508, 7520 and 7521.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70687	**PoE**	Previously, on an IE300 switch, it was possible for PoE state reported by the various GUIs did not reflect the configured state. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-70261	**Port Security**	Previously, when multiple MAC addresses were learnt and cleared simultaneously on a switch where port security was configured, it was possible for the switch to restart unexpectedly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69445	**Storm Control**	With this software update, it is now possible to configure multiple storm-control types and rates on individual port for x220, GS980M and x230-52 variant switches.	–	–	–	–	Y	–	–	–	–	–	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-70302	**Tunnel**	Previously, the **`ip unnumbered`** command could fail on a tunnel interface while configuring a router during startup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70402	**Tunnel**	Previously, configuration entered on a tunnel that was not fully configured and operational would not appear in the running-config. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-70026	**VCStack**	Previously, there was a small chance that if a stack member left the stack and rebooted in less than a minute, then the re-booted stack member may not join the stack correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	–	–	–	–	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-69861	**VCStack**	Previously, it was possible for SBx8100 CFC960 line cards to fail to initialise due to an internal communication failure. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–

What's New in Version 5.5.0-1.3

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
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
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 5.5.0-1.3.

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.

Caution: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 69.

For instructions on how to update the web-based GUI, see "Installing and Accessing the Web-based GUI on Switches" on page 71 or "Installing and Accessing the Web-based GUI on AR-Series Devices" on page 74. 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		10/2020	vaa-5.5.0-1.3.iso (VAA OS) vaa-5.5.0-1.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-1.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2020	SBx81CFC960-5.5.0-1.3.rel
SBx908 GEN2	SBx908 GEN2	10/2020	SBx908NG-5.5.0-1.3.rel
x950-28XSQ x950-28XTQm	x950	10/2020	x950-5.5.0-1.3.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	10/2020	x930-5.5.0-1.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2020	x550-5.5.0-1.3.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	10/2020	x530-5.5.0-1.3.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	10/2020	x510-5.5.0-1.3.rel
IX5-28GPX	IX5	10/2020	IX5-5.5.0-1.3.rel
x320-10GH x320-11GPT	x320	10/2020	x320-5.5.0-1.3.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	10/2020	x310-5.5.0-1.3.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2020	x230-5.5.0-1.3.rel
x220-28GS x220-52GT x220-52GP	x220	10/2020	x220-5.5.0-1.3.rel
IE510-28GSX	IE510-28GSX	10/2020	IE510-5.5.0-1.3.rel
IE340-20GP IE340L-18GP	IE340	10/2020	IE340-5.5.0-1.3.rel
IE300-12GT IE300-12GP	IE300	10/2020	IE300-5.5.0-1.3.rel
IE210L-10GP IE210L-18GP	IE210L	10/2020	IE210-5.5.0-1.3.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	10/2020	IE200-5.5.0-1.3.rel
XS916MXT XS916MXS	XS900MX	10/2020	XS900-5.5.0-1.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2020	GS980EM-5.5.0-1.3.rel
GS980M/52 GS980M/52PS	GS980M	10/2020	GS980M-5.5.0-1.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2020	GS970-5.5.0-1.3.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	10/2020	GS900-5.5.0-1.3.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	10/2020	FS980-5.5.0-1.3.rel
AR4050S AR3050S	AR-series UTM firewalls	10/2020	AR4050S-5.5.0-1.3.rel AR3050S-5.5.0-1.3.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	10/2020	AR2050V-5.5.0-1.3.rel AR2010V-5.5.0-1.3.rel AR1050V-5.5.0-1.3.rel

Caution: Software version 5.5.0-1.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-1.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 65 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 67.

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

The 5.5.0-1.3 software version is ISSU compatible with previous software versions.

Enhancements in Version 5.5.0-1.3

This AlliedWare Plus maintenance version includes the following enhancements:

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-3543	**CLI** **Router High Availability**	With this software update, It is now possible to manually activate the bypass mode of WAN interfaces on the AR4050S, AR3050S and AR2050V Series by using the CLI. When the bypass mode is activated a relay electrically disconnects the cable plugged into the WAN port and reconnects it to bypass port. This allows the WAN cable to be fed through to another device. Bypass mode is deactivated by default. Bypass mode can be activated by entering Interface Mode and for the WAN interface and using the command **wan-bypass**. i.e. `interface eth1` `  wan-bypass` Bypass mode can be deactivated by entering Interface Mode and for the WAN interface and using the 'no' variation of the command **wan-bypass**. If bypass mode for a WAN interface has been activated manually it is not possible to associate it with a VRRP instance. Bypass mode must be manually deactivated first. Similarly, it is not possible to manually activate bypass mode if the WAN interface is currently associated with a VRRP instance. To manually control bypass mode, remove the association from the VRRP instance using the command **no ha associate**.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-3570 **ER-3623** **ER-3624** **ER-3592**	**Web API** **Device GUI**	This software update adds a WEB GUI API to allow the Vista Manager to install the device GUI file from flash. The command **`gui preference flash`** has been added. When this command is configured, Vista Manager will load the device GUI files from flash with the precedence for installing the GUI files. Without configuring the CLI command, if there exists a webgui.gui file in the flash:/.resources/downloaded/ folder, then this file will take the precedence of GUI files in flash. If there are no GUI files in flash, it will check if the webgui.gui exists in the flash:/.resources/downloaded/ folder, then load it from there. If this command is not configured, the installing precedence will be the webgui.gui in the hidden folder first, then the device GUI file in flash. ISSU: 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

Issues Resolved in Version 5.5.0-1.3

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69722	**AMF**	Previously, an AMF guest node could be reset (i.e. leave and then re-join the AMF network) with every LLDP neighbour information update. 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
CR-69767	**AMF**	Previously, a very unusual combination of AMF provisioning commands left the file system pointing to a non-existent directory. As a result, when AMF backup was performed, it became confused attempting to locate the non-existent directory. The solution of this software update ensures that the AMF backups return to the home directory before initiating the backup. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-69942	**AMF**	Previously, a transition from an active amf-link to an amf-crosslink on active ports would not work. 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-69857	**AMF** **VAA**	Previously, when configuring area-links on a VAA, including for container masters, error messages such as "fail to create or destroy a VLAN device", or "fail to add an interface to a bridge" would be logged. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-69834	**ARP** **Neighbor Discovery**	Previously, clearing IPv6 neighbours did not remove dynamically learned entries. 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	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69557	**ARP Neighbor Discovery**	Previously, multicast traffic with a TTL value of "1" could be incorrectly reflected out a trunk port configured for NLB. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	Y	–	Y	Y	–	–	Y	Y	–	Y	Y	–	Y	–	–	–	–	–
CR-68555	**Auto-negotiation**	Previously, it was possible for an x530 variant switch to not detect a port speed change when the link-partner renegotiated the link speed down to 100M (on 2.5G or 5G ports). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-69714	**BGP**	Previously, when redistributing IPv4 OSPF or RIP routes with route tags attached into other routing protocols, the tag was not included as part of the redistribution. This prevented route-maps from being able to filter these tagged routes. This issue has been resolved. Now, any routes with tags attached will have the tag preserved when redistributing into a protocol, allowing route-maps to filter those tagged routes. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-63424	**Device Security**	This software update addressed the Linux security vulnerability issue outlined in CVE-2019-11068 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-65671	**Device Security**	This software update addressed the OpenSSL security vulnerability issue outlined in CVE-2019-1563. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-65672	**Device Security**	This software update addressed the TFTP and FTP security vulnerability issue outlined in CVE-2019-5481 and CVE-2019-5482 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-66034	**Device Security**	This software update addressed the HTTP security vulnerability issue outlined in CVE-2019-17420 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-68475	**Device Security**	This software update addressed the HAProxy loadbalancing security vulnerability issue outlined in CVE-2020-11100 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-69979	**DNS**	Previously, when multiple DNS servers were configured, the total number of DNS servers was restricted to 3, this was incorrect, the limit of 3 DNS servers should have only applied to DNS servers that are used for global resolution (and not any that are limited to specific suffix lists). 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	–
CR-70012	**DNS**	Previously, when using DNS-Relay with domain lists, if there were multiple servers for the same suffix and the first one failed to provide an answer, it was possible that the device would attempt to query the wrong server for the suffix. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-69849	**DPI**	This software update addresses the buffer overflow vulnerability issue as outlined in CVE-2020-15471 to CVE-2020-15476.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-69946	**Flow Control**	Previously, ports connected to a SPTx pluggable could link up even if disabled. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-69867	**HTTP Service**	This software update addresses the HTTP Service security vulnerability issue as outlined in CVE-2020-15049.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69373	**MAC Thrashing**	Previously, MAC entries could randomly get deleted from some SBx8100 line cards running on the same chassis while traffic was flowing, resulting in unnecessary unicast traffic flooding. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-69506	**MAC Thrashing Trigger**	Previously, if thrash-limiting with action **`vlan-disable`** on aggregators as well as the findme trigger were both configured, port LEDs could sometimes continue to flash indefinitely if ports linked down while thrash-limiting was active. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-69815	**Multicast Forwarding**	Previously, after dynamic channel group went down, and then up again, the multicast traffic over the aggregator link would not recover. This issue has been resolved.	–	–	Y	Y	Y	–	Y	Y	Y	Y	Y	–	Y	Y	–	Y	Y	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-69771	**Port Auth VCStack**	Previously, when port authentication was configured, a late join stack member could sometimes trigger the message "*VCS sync timeout for lock-step operation*" to be logged. This was due to a mismatch of the supplicants information on stack members. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	–	–	–	Y	–	–	–	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-70073	**PPPoE**	With this software update, PPPoE relay instances can now be created with alphanumeric characters, hyphens, and underscores.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-68468	**RADIUS**	This software update addressed the radius security vulnerability issue outlined in CVE-2019-17185 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69788	**SNMP**	Previously, when using SNMP discovery with some devices, it was possible for the process to lock up. 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-70115	**SNMP**	Previously, SNMP information was unable to be obtained by IPv6. 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-68471	**SNMP** **VCStack**	Previously, changing the PVID of a port on a backup member could result in MAC address table entries for the previous VLAN not being deleted from the MAC address table. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	–	Y	–	–	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-60459	**SSH**	This software update addresses the OpenSSH user enumeration vulnerability as described in CVE-2018-15473. I ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-69105	**SSH**	With this software update, the SSH server has been modified to allow only ciphers which are consistent with ciphers currently offered by OpenSSH by default, and does not include CBC ciphers. The new command as part of this implementation is: **`(no)ssh server secure-ciphers`** In addition, the **`show ssh server`** command output has also been modified to show the current ciphers in use. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69398	**SSH**	In software version 5.4.9-2.1 onwards, an issue was discovered where the SSH client would only negotiate hmac-sha1 algorithm for hash-based message authentication code. This issue has been resolved. Now, the SSH client by default will negotiate the following algorithms for HMAC: ■ umac-64-etm@openssh.com ■ umac-128-etm@openssh.com ■ hmac-sha2-256-etm@openssh.com ■ hmac-sha2-512-etm@openssh.com ■ hmac-sha1-etm@openssh.com ■ umac-64@openssh.com ■ umac-128@openssh.com ■ hmac-sha2-256 ■ hmac-sha2-512 ■ hmac-sha1 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-67464	**SSH** **DOS Detection**	Previously, when IPS was enabled, every packet that matched a drop rule would result in an alert message being logged. As a result, under DoS condition, SSH was unresponsive because the device was busy logging. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-69818	**VAA** **AMF**	Previously, VAA virtual machines deployed on Microsoft Azure would fail to deploy. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-70026	**VCStack**	Previously, there was a small chance that if a stack member left the stack and rebooted in less than a minute, then the remote mounts for the rebooted stack node would not be added properly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	–	–	–	–	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-69812	**VLAN**	With this software update, adding multiple VLAN stacking rules on the same port is now possible. 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-69760	**Web API**	Previously, the CPU load value in the device GUI on AlliedWare+ devices could show a different value to the values shown on the CLI. This was due to a difference in the way that the values were calculated. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-69923	**Web API**	Previously, using the RestFul API to obtain ESPR state could result in a slow memory leak. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–

What's New in Version 5.5.0-1.2

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
x510L Series
IX5-28GPX
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
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 5.5.0-1.2.

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.

Caution: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 69.

For instructions on how to update the web-based GUI, see "Installing and Accessing the Web-based GUI on Switches" on page 71 or "Installing and Accessing the Web-based GUI on AR-Series Devices" on page 74. 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		07/2020	vaa-5.5.0-1.2.iso (VAA OS) vaa-5.5.0-1.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-1.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	07/2020	SBx81CFC960-5.5.0-1.2.rel
SBx908 GEN2	SBx908 GEN2	07/2020	SBx908NG-5.5.0-1.2.rel
x950-28XSQ x950-28XTQm	x950	07/2020	x950-5.5.0-1.2.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2020	x930-5.5.0-1.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2020	x550-5.5.0-1.2.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	07/2020	x530-5.5.0-1.2.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	07/2020	x510-5.5.0-1.2.rel
IX5-28GPX	IX5	07/2020	IX5-5.5.0-1.2.rel
x320-10GH x320-11GPT	x320	07/2020	x320-5.5.0-1.2.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2020	x310-5.5.0-1.2.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2020	x230-5.5.0-1.2.rel
x220-28GS x220-52GT x220-52GP	x220	07/2020	x220-5.5.0-1.2.rel
IE510-28GSX	IE510-28GSX	07/2020	IE510-5.5.0-1.2.rel
IE340-20GP IE340L-18GP	IE340	07/2020	IE340-5.5.0-1.2.rel
IE300-12GT IE300-12GP	IE300	07/2020	IE300-5.5.0-1.2.rel
IE210L-10GP IE210L-18GP	IE210L	07/2020	IE210-5.5.0-1.2.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2020	IE200-5.5.0-1.2.rel
XS916MXT XS916MXS	XS900MX	07/2020	XS900-5.5.0-1.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	07/2020	GS980EM-5.5.0-1.2.rel
GS980M/52 GS980M/52PS	GS980M	07/2020	GS980M-5.5.0-1.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2020	GS970-5.5.0-1.2.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	07/2020	GS900-5.5.0-1.2.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	07/2020	FS980-5.5.0-1.2.rel
AR4050S AR3050S	AR-series UTM firewalls	07/2020	AR4050S-5.5.0-1.2.rel AR3050S-5.5.0-1.2.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	07/2020	AR2050V-5.5.0-1.2.rel AR2010V-5.5.0-1.2.rel AR1050V-5.5.0-1.2.rel

Caution: Software version 5.5.0-1.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-1.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 65 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 67.

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

The 5.5.0-1.2 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.0-1.2

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-69857	AMF VAA	Previously, when configuring area-links on a VAA, including for container masters, the following type of error messages could be logged: ■ Fail to create or destroy a VLAN device ■ Fail to add an interface to a bridge This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-69818	VAA	Previously, VAA virtual machines deployed on Microsoft Azure could fail to deploy. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y

What's New in Version 5.5.0-1.1

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
x510 Series
x510L Series
IX5-28GPX
x320-10GH
x310 Series
x230 Series
x230L Series
x220 Series
IE510-28GSX
IE340 Series
IE300 Series
IE210L Series
IE200 Series
XS900MX Series
GS980EM/10H
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 5.5.0-1.1.

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.

Caution: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 69.

For instructions on how to update the web-based GUI, see "Installing and Accessing the Web-based GUI on Switches" on page 71 or "Installing and Accessing the Web-based GUI on AR-Series Devices" on page 74. 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		07/2020	vaa-5.5.0-1.1.iso (VAA OS) vaa-5.5.0-1.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.5.0-1.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	07/2020	SBx81CFC960-5.5.0-1.1.rel
SBx908 GEN2	SBx908 GEN2	07/2020	SBx908NG-5.5.0-1.1.rel
x950-28XSQ x950-28XTQm	x950	07/2020	x950-5.5.0-1.1.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2020	x930-5.5.0-1.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2020	x550-5.5.0-1.1.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GPX	x530 and x530L	07/2020	x530-5.5.0-1.1.rel
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510 and x510L	07/2020	x510-5.5.0-1.1.rel
IX5-28GPX	IX5	07/2020	IX5-5.5.0-1.1.rel
x320-10GH x320-11GPT	x320	07/2020	x320-5.5.0-1.1.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2020	x310-5.5.0-1.1.rel

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

Models	Family	Date	Software File
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2020	x230-5.5.0-1.1.rel
x220-28GS x220-52GT x220-52GP	x220	07/2020	x220-5.5.0-1.1.rel
IE510-28GSX	IE510-28GSX	07/2020	IE510-5.5.0-1.1.rel
IE340-20GP IE340L-18GP	IE340	07/2020	IE340-5.5.0-1.1.rel
IE300-12GT IE300-12GP	IE300	07/2020	IE300-5.5.0-1.1.rel
IE210L-10GP IE210L-18GP	IE210L	07/2020	IE210-5.5.0-1.1.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2020	IE200-5.5.0-1.1.rel
XS916MXT XS916MXS	XS900MX	07/2020	XS900-5.5.0-1.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	07/2020	GS980EM-5.5.0-1.1.rel
GS980M/52 GS980M/52PS	GS980M	07/2020	GS980M-5.5.0-1.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2020	GS970-5.5.0-1.1.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	07/2020	GS900-5.5.0-1.1.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	07/2020	FS980-5.5.0-1.1.rel
AR4050S AR3050S	AR-series UTM firewalls	07/2020	AR4050S-5.5.0-1.1.rel AR3050S-5.5.0-1.1.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	07/2020	AR2050V-5.5.0-1.1.rel AR2010V-5.5.0-1.1.rel AR1050V-5.5.0-1.1.rel

Caution: Software version 5.5.0-1.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 5.5.0 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.0 license installed, that license also covers all later 5.5.0 versions, including 5.5.0-1.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 65 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 67.

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

The 5.5.0-1.1 software version is ISSU incompatible with previous software versions.

New Products

Version 5.5.0-1.1 supports the following upcoming and recently-released products.

x320-11GPT Gigabit Layer 3 PoE Pass-Through Switches

Supported since 5.5.0-1.1

These switches have 8 x 10/100/1000T PoE+ ports, 1 x 10/100/1000 PoE-in port, and 2 x 100/1000X SFP uplinks, with the ability to be both powered by PoE, and pass-through PoE to end devices. In combination with the x320-10GH, they are designed for IoT device connectivity in today's smart building networks.

Key features include:

- Power by PoE from the x320-10GH and pass-through PoE to end devices, or power with a separate AC power adapter
- 30W PoE+ per port for connecting and powering end devices
- Continuous PoE maximizes end-point connectivity
- Active Fiber Monitoring secures uplink connectivity
- Allied Telesis Autonomous Management Framework™ (AMF) for easy management
- Fanless design provides silent operation
- DIN rail and rack-mount options.

For more information, see our website at www.alliedtelesis.com/products/switches/x320-series.

GS980EM/11PT Gigabit Layer 3 Lite PoE Pass-Through Switches

Supported since 5.5.0-1.1

These switches have 8 x 10/100/1000T PoE+ ports, 1 x 10/100/1000 PoE-in port, and 2 x 100/1000X SFP uplinks, with the ability to be both powered by PoE, and pass-through PoE to end devices. In combination with the GS980EM/10H, they are designed for IoT device connectivity in today's converged business networks.

Key features include:

- Power by PoE from the GS980EM/10H and pass-through PoE to end devices, or power with a separate AC power adapter
- 30W PoE+ per port for connecting and powering end devices
- Active Fiber Monitoring secures uplink connectivity
- Allied Telesis Autonomous Management Framework™ (AMF) Edge

- Fanless design provides silent operation
- DIN rail and rack-mount options.

For more information, see our website at https://www.alliedtelesis.com/products/switches/gs980em-series.

New Features and Enhancements

This section summarizes the new features in 5.5.0-1.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 64.

Autonomous Management Framework (AMF) Enhancements

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

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

Version 5.5.0-1.1 includes the following AMF enhancements.

AMF link support on Eth interfaces

Available on all AR-series devices

From version 5.5.0-1.1 onwards, AMF up/down links and AMF area links are supported over an AR-series device's Eth interfaces. This enables you to provision and recover AMF nodes over these interfaces.

To use this feature your AMF network must be in AMF secure mode.

Use the **atmf-link** and **atmf-arealink** commands on an Eth interface to configure it as an AMF link. For example, to configure an AMF up/down link on Eth1 interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# atmf-link
```

By default AMF recovery is disabled on these links. Enable recovery by running the **atmf recover over-eth** command in privileged exec mode:

```
awplus# atmf recover over-eth
```

This setting persists even after restoring a device to a "clean" state with the **erase factory-default** or **atmf cleanup** command.

For more information on AMF, AMF secure mode, and AMF links, see the AMF Feature Overview and Configuration Guide.

Easier replacement of TQ model AMF Guest nodes using login fallback

Available on AlliedWare Plus devices that support wireless management

From version 5.5.0-1.1 onwards, you can enable login fall back on TQ model AMF guest nodes using the command **login-fallback enable**. This feature helps speed up TQ replacement in the field, by enabling a TQ's factory default username/password settings.

Here's how it works

When a new TQ replaces a broken TQ, the new device is assumed to have the factory default settings. AMF logs in to the new TQ using the factory default manager/friend settings. The new TQ is then discovered and managed as an AMF guest node by an AMF master or member. This means any backed up settings for the replaced guest node can also be recovered.

To use the login fallback feature, first create an AMF guest class for TQ model APs. Then enable the login fall back feature.

Example

To enable login fallback on the guest-class AT-TQ5k, use the commands:

```
node1#configuration terminal
node1(config)#atmf guest-class AT-TQ5k
node1(config-atmf-guest)#login-fallback enable
```

The command is disabled by default.

With this software version, the output of the command **show atmf links guest detail** now includes whether login fallback is turned on for wireless management.

Access Control List (ACL) groups

Available on all AlliedWare Plus switches

From 5.5.0-1.1 onwards, you can combine Access Control List (ACL) rules into groups to simplify configuration. ACL groups allow for smaller configuration files to achieve the same ACL configuration. By specifying a list of hosts or ports as a group, that group can be used in an ACL instead of having to specify an ACL for each host/port combination. In some cases, this can be a large saving in configuration.

ACL groups can be used when adding ACLs for multiple hosts that require the same filtering. For example, blocking three ports on four hosts requires twelve lines of ACLs. Using host groups and port groups, only one ACL needs to be entered in the configuration. The hardware entries are not changed; twelve entries are still used in the ACL table. ACL groups are supported in global ACLs on devices that support global ACLs.

For more information on ACLs see the Access Control List (ACL) Feature Overview and Configuration Guide.

Dynamic ACL assignments via Port Authentication

Available on GS900MX/MPX, GS980EM, GS980M, GS970M, IE210, IE300, IE510, IX5, SBx908 GEN2, x220, x230, x310, x320, x510, x530, x530L, x930, and x950 Series switches

From version 5.5.0-1.1 onwards, you can configure port authentication to dynamically apply Access Control Lists (ACLs) when a supplicant is authorized. These ACLs are removed when the supplicant disconnects.

Dynamic ACLs give you greater control over a supplicant's network access by pairing ACLs with 802.1X, MAC, and web-based authentication. Dynamic ACLs offer the following advantages:

- They provide an easy method of applying ACLs per supplicant.
- As they are only installed when a supplicant is connected (and authorized), the number of ACLs is kept low to avoid wasting hardware resources.
- ACLs are defined on the central RADIUS server, this means they can be applied to all switches that use the same RADIUS server.
- Dynamic ACLs support the same filtering rules as static ACLs and will work with IP, IPv6, ICMP, UDP, TCP, IP protocols and MAC matches.
- You can configure a mix of static and dynamic ACLs on a switch.

Dynamic ACLs are supported on switch ports and static aggregators.

Configuring Dynamic ACLs

Step 1: Configure port authentication on your switch.

For example to enable auth-mac, use the following commands.

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# auth-mac enable
```

Step 2: Enable Dynamic ACLs on the port.

Dynamic ACLs are disabled by default.

```
awplus(config-if)# auth dynamic-acl enable
```

Step 3: Define Dynamic ACL rules on the RADIUS server.

Dynamic ACLs are defined on the RADIUS server for each user (keyed by username for 802.1X and web-based authentication, or by MAC address for MAC authentication). They are defined using one of the following standard RADIUS attributes:

- NAS-Filter-Rule (attribute type 92): to define a single ACL filter rule, or
- Filter-Id (attribute type 11): to define an existing named or numbered hardware ACL.

Multiple rules are allowed but NAS-Filter-Rule and Filter-Id cannot be mixed.

For example, to reject IP traffic from 192.168.1.x to any destination except 192.168.2.x, define these two rules for the user on the RADIUS server:

```
NAS-Filter-Rule = "ip:permit ip 192.168.1.0/24 192.168.2.0/24"
NAS-Filter-Rule = "ip:deny ip 192.168.1.0/24 any"
```

Alternatively, you could use ACLs that are already defined on the authenticating switch. In this situation you just specify which ACLs to use on the RADIUS server.

So, for example, if these two rules are defined on the authenticating switch:

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

You would define the following on the RADIUS server:

```
Filter-Id = "3000"
Filter-Id = "3001"
```

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

For more information on ACLs see the Access Control List (ACL) Feature Overview and Configuration Guide.

VLAN-based Q-in-Q (VLAN stacking)

Available on SBx8100 Series switches.

On the SBx8100 Series switch, AlliedWare Plus 5.5.0-1.1 adds support for VLAN-based Q-in-Q. VLAN-based Q-in-Q is also known as VLAN-based VLAN stacking or VLAN-based double-tagging. When you configure this VLAN stacking for a customer VLAN, it applies an outer-VLAN tag to all traffic from that VLAN as it traverses the service provider's network. The outer tag is removed for traffic from the provider network ingressing via the provider port, which is configured as a member of the outer VLAN.

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

Bridges supported as MAP-E upstream interface type

Available on AR-series routers

From version 5.5.0-1.1 onwards, bridges are supported as an 'upstream' interface type for IPv6 transition services.

For example, to configure the softwire configuration ('test') to use a bridge 'br1'as an upstream-interface, use the following commands:

```
awplus# configure terminal
awplus(config)# softwire-configuration test
awplus(config-softwire)# upstream-interface br1
```

Firewall session limit for UDP and TCP connections

Available on AR1050V, AR2010V, AR2050V, AR3050S and AR4050S

From version 5.5.0-1.1 onwards, firewall session rules apply to UDP and TCP connections.

Previously, firewall session limiting rules only applied to TCP connections. Now UDP connections will also be included in the limit count. For customers already using this feature, particularly where the limit is set quite low and with users that often hit the limit, they may wish to increase their limits by some proportion to account for the presence of UDP in a users traffic profile. For most configurations where the limit is applied to prevent extreme usage or abuse there may be no need to increase the limit. There is no new configuration associated with this change.

Improvements when in Secure Mode

Available on all AlliedWare Plus devices that support Secure Mode.

From version 5.5.0-1.1 onwards, the following new and updated commands are available in Secure Mode:

New commands

no debug core-file

Core files may disclose sensitive memory contents. This command prevents such core files from being generated.

crypto secure-mode delete hostkey

When booting into secure mode, a device will automatically generate a hostkey for use when encrypting configuration secrets. This command deletes that hostkey file, making encrypted secrets non-recoverable.

Modified commands

enable password

In secure mode, the **enable password** command allows changing effective privilege level up to the base level configured for the current user, and will require a password if one has been configured for the requested privilege level.

crypto verify

This command is updated with options: bootrom and signed.

bootrom: This tells the device that the signature provided is for the bootrom. It stores that hash permanently, preventing boot if the bootloader is modified.

signed: The hash used is from a <release>.sig file and calculated as a keyed HMAC-SHA.

```
crypto verify signed <filename> <hash-value>
crypto verify bootrom <hash-value>
```

When using signature verification, if:

- the release verified is the boot release
- and the device is running in secure mode
- and signed verification succeeds

then the signed hash is also stored into the device and enforced on all subsequent boots.

This means that if you change the software version, the switch will not boot up. You can only change the software version if you reset the switch to the factory defaults before changing the software version, by using the command **erase factory-default**.

snmp user

SNMPv3 user authentication now supports sha-256.

Shared secrets

Shared secrets are now stored encrypted via hostkey in generated configuration files when in secure mode.

Unsupported commands

The following commands are not supported in Secure Mode:

- license
- aaa authentication login
- aaa authorization commands
- aaa accounting login
- aaa accounting commands
- aaa authentication enable default group tacacs+
- tacacs-server host

The 'no' version of the following commands are not supported in Secure Mode:

- tacacs-server key
- tacacs-server timeout
- ip tacacs source-interface
- show tacacs+ and radius-server local

Stacking

Stacking is not supported in secure mode. Now, when a stacking command is used an error message is displayed.

Updated SSH Server Ciphers

Available on all devices that support SSH.

From version 5.5.0-1.1 onwards, the following new and updated commands are available for SSH server:

New command

ssh server secure-ciphers

This command sets the SSH server to only negotiate ciphers regarded as current-best-practice. The command uses the same cipher string as the OpenSSH default which excludes CBC, as CBC has been regarded as a weak cipher.

When the command is used, the ciphers included are: chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, and aes256-gcm@openssh.com.

To configure the SSH server to only negotiate ciphers regarded as current-best-practice, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-ciphers
```

Updated show command

show ssh server

The output of this show command is modified to show the current ciphers in use.

Figure 1: Example output from **show ssh server**:

```
AR4050S-master#show ssh server
Secure Shell Server Configuration
-----------------------------------------------------------
SSH Server                          : Enabled
Protocol                            : IPv4,IPv6
Port                                : 22
Version                             : 2,1
Services                            : scp, sftp
User Authentication                 : publickey, password
Resolve Hosts                       : Disabled
Session Timeout                     : 0 (Off)
Login Timeout                       : 60 seconds
Maximum Authentication Tries        : 6
Maximum Startups                    : 10
Debug                               : NONE
Ciphers                             : chacha20-poly1305@openssh.com,aes128-ctr,ae
s192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
```

MODBUS on IE510

Available on IE510-28GSX Industrial Ethernet switches

From version 5.5.0-1.1 onwards, MODBUS support is added to the IE510 platform which is the first switch to support both hardware alarm monitoring and stacking.

This enhancement is ideal for scenarios that use MODBUS and require the high port density allowed by IE510 stacking.

New Active Fiber Monitoring MIB Object

From version 5.5.0-1.1 onwards, a new MIB object is available for Active Fiber Monitoring.

Previously, the last 12 readings for a fiber monitoring interface were available in the at-fiber-monitoring MIB as a space-separated string. This was difficult for some SNMP management systems to interpret.

To make this easier, a new entry "atFiberMonLastReading" has been added to the state table in the at-fiber-monitoring MIB at .1.3.6.1.4.1.207.8.4.4.3.27.3.1.9.

This entry returns the last reading read by fiber monitoring on an interface as an integer.

The values returned by existing MIB entries have not changed.

IP Helper now VRF-lite aware

Available on products that support VRF-lite

From version 5.5.0-1.1 onwards, IP Helper correctly forwards broadcast UDP frames on a VLAN configured for VRF-lite.

IP Helper forwards broadcast UDP frames from one Layer 3 interface to a configured specific IP address. With this capability, UDP frames can be forwarded as a lightweight proxy for certain broadcast protocols.

Previously, this only worked on VLANs not configured to use VRF-lite (in other words, using the default 'Global' VRF). Now IP Helper works as expected with other VRF IDs assigned to a VLAN with IP-Helper configured.

Expanded MAC filter entries for TQ5403 Series APs

Available on SBx908 GEN2, x950, x930, and x530 Series switches, and AR-Series firewalls and routers, when managing the TQ5403, TQ5403e and TQm5403 APs.

From version 5.5.0-1.1 onwards, the maximum number of MAC addresses that can be entered per MAC filter entry increases from 1024 to 2048 entries.

Use the **filter-entry** command to set a MAC filter entry (descriptive name) to a wireless MAC filter. With this software release, the maximum number of MAC filter entries is increased to 2048. For example:

```
awplus(config)#wireless
awplus(config-wireless)#wireless-mac-filter 100
awplus(config-wireless-mac-flt)#filter-entry 012a.eb12.3456
description PC01
```

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.0-x.x and may affect your device or network behavior if you upgrade:

- VCStack compatibility
- 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 - read this if stacking x530 Series switches
- 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 5.5.0-x.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.4.9-1.x version, please check the 5.4.9-2.x release note. Release notes are available from our website, including:

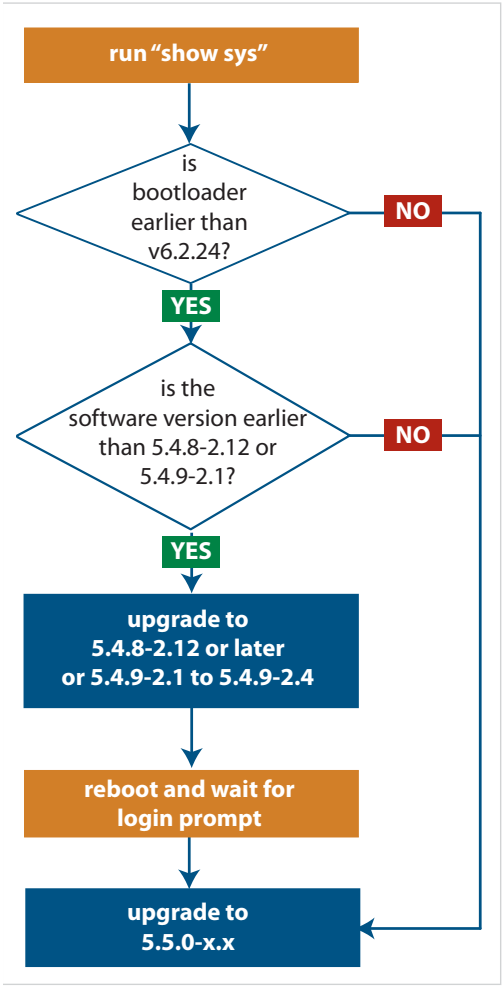
- 5.4.9-x.x release notes
- 5.4.8-x.x release notes
- 5.4.7-x.x release notes
- 5.4.6-x.x release notes

VCStack compatibility

There are restrictions on which software versions you can use rolling reboot with, and restrictions in how to form a new VCStack or add new members to a stack. For details, see "Upgrading a VCStack with rolling reboot" on page 60 and "Forming or extending a VCStack with auto-synchronization" on page 61.

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 5.5.0-x.x.



If your bootloader is older than 6.2.24, you can only upgrade to 5.5.0-x.x from the following software versions:

- 5.4.8-2.12, 5.4.8-2.13 or later, or
- 5.4.9-2.1, 5.4.9-2.2, 5.4.9-2.3 or 5.4.9-2.4, or
- any older 5.5.0-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 5.5.0-x.x.

If your bootloader is older than 6.2.24, you cannot upgrade to 5.5.0-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 "Boot-loader 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
VLAN Statistic commands removed from x220, x320 and x530 Series switches	*x220, x320 and x530 Series switches*	From 5.5.0-1.1 onwards, the following commands have been removed from the x220, x320 and x530 Series switches: ■ vlan statistics ■ clear vlan statistics ■ show vlan statistics The commands were removed because the VLAN statistics feature is not available on these products.
Storm Control is improved for large packets	*SBx908 GEN2, x950, x930, x550, x510, x310, x230, XS900MX, GS900MX/MPX, and GS970M Series switches*	The command **storm-control {broadcast|multicast|dlf} level** enables you to limit broadcast, multicast or DLF packets to a percentage of line speed. From 5.5.0-0.1 onwards, this command applies the specified percentage in the same way for packets of all sizes. Previously, larger packets would take more bandwidth than expected. You may need to adjust your specified levels to allow for the changed functionality.
diffie-hellman-group1-sha1 is removed as an SSH key exchange algorithm	*All AlliedWare Plus devices*	From 5.5.0-0.1 onwards, diffie-hellman-group1-sha1 has been removed as an SSH key exchange algorithm option. If you are using a legacy SSH client, you may need to upgrade your client.
Provisioned ports are no longer accessible using MODBUS	*All AlliedWare Plus devices that support MODBUS*	Provisioned ports are no longer accessible using MODBUS.
In Secure Mode, devices reboot if they fail to initialize a critical service	*All AlliedWare Plus devices that support Secure Mode*	From 5.5.0-0.1 and 5.4.9-2.3 onwards, in Secure Mode, failure while initializing a critical service will cause the device to reboot.

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.0 license on your switch if you are upgrading to 5.5.0-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 65 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 67.

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 5.5.0-1.x from:

- 5.5.0-0.x

On these switches, you **cannot** use rolling reboot to upgrade to 5.5.0-1.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 5.5.0-1.x from:

- 5.5.0-0.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 5.5.0-1.x from:

- 5.5.0-0.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 5.5.0-1.x and:

- 5.5.0-0.x

On these switches, auto-synchronization is not supported between 5.5.0-1.x and any version earlier than 5.5.0-0.x.

For CFC960 cards on 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 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 different 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 5.5.0-1.x and:

- 5.5.0-0.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 5.5.0-1.x and:

- 5.5.0-0.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 5.5.0-1.x and 5.4.6-1.1 or **any** earlier releases.

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

If using an AMF controller

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

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

If using secure mode

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

If using Vista Manager EX

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

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

If using none of the above

If none of the above apply, then nodes running version 5.5.0-1.x are compatible with nodes running:

- 5.5.0-0.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 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-2019
Features included              : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                                 EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                                 L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VCStack, VRRP

Index                          : 2
License name                   : 5.5.0
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2020
License expiry date            : N/A
Release                        : 5.5.0
```

Licensing this Version on an SBx8100 Series CFC960 Control Card

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

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

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

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

1. Obtain the MAC address for a control card

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

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

```
awplus#show system mac license

MAC address for licensing:


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

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

2. Obtain a release license for a control card

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

3. Apply a release license on a control card

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

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

Index                          : 2
License name                   : 5.5.0
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2020
License expiry date            : N/A
Release                        : 5.5.0
```

Installing this Software Version

Caution: On SBx908 GEN2 and x950 Series switches, you can only upgrade to this release from certain earlier releases. See Upgrade compatibility for SBx908 GEN2 and x950 Series switches for details.

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 65 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 67.

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 SBx8100-5.5.0-1.5.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.0-1.5.rel`
x950 series	`awplus(config)# boot system x950-5.5.0-1.5.rel`
x930 series	`awplus(config)# boot system x930-5.5.0-1.5.rel`
x550 series	`awplus(config)# boot system x550-5.5.0-1.5.rel`
x530 series	`awplus(config)# boot system x530-5.5.0-1.5.rel`
x510 series	`awplus(config)# boot system x510-5.5.0-1.5.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.5.0-1.5.rel`
x320 series	`awplus(config)# boot system x320-5.5.0-1.5.rel`

Product	Command
x310 series	`awplus(config)# boot system x310-5.5.0-1.5.rel`
x230 series	`awplus(config)# boot system x230-5.5.0-1.5.rel`
x220 series	`awplus(config)# boot system x220-5.5.0-1.5.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.5.0-1.5.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.0-1.5.rel`
IE300 series	`awplus(config)# boot system IE300-5.5.0-1.5.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.0-1.5.rel`
IE200 series	`awplus(config)# boot system IE200-5.5.0-1.5.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.0-1.5.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.0-1.5.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.0-1.5.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.0-1.5.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.5.0-1.5.rel`
FS980M series	`awplus(config)# boot system FS980-5.5.0-1.5.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.0-1.5.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.0-1.5.rel`
AR2050V	`awplus(config)5z# boot system AR2050V-5.5.0-1.5.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.0-1.5.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.0-1.5.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
```

Installing and Accessing the Web-based GUI on Switches

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

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

On SBx908 GEN2 switches, x950 Series, x930 Series, x550 Series and x530 Series, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

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

Check if the GUI is installed

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

Browse to the GUI

Perform the following steps to browse to the GUI.

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

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

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

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

3. If you do not see a login page, you need to install the GUI, as described in "Install the GUI if it is not installed" on page 75. If you see a login page, log in. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the About page in the GUI and check the field called **GUI version**. The version to use with 5.5.0-1.5 is 2.7.1.

If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 75.

Install the GUI if it is not installed

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

1. Obtain the GUI file from our Software Download center. The filename for v2.7.1 of the GUI is awplus-gui_550_21.gui.

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

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

   - TFTP server
   - USB Flash drive
   - SD card

   For example, to copy the v2.7.1 GUI file from your USB Flash drive, use the following commands:

   ```
   awplus>enable
   awplus#copy usb awplus-gui_550_21.gui flash
   ```

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

   ```
   awplus#dir
   ```

3. Delete any previous Java switch GUI files.

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

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

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

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

5. Make sure the HTTP service is running:

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

6. Log into the GUI:

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

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

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

Update the GUI if it is not the latest version

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

1. Obtain the GUI file from our Software Download center. The filename for v2.7.1 of the GUI is awplus-gui_550_21.gui.

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

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

   - TFTP server
   - USB Flash drive
   - SD card

   For example, to copy the v2.7.1 GUI file from your USB Flash drive, use the following commands:

   ```
   awplus>enable
   awplus#copy usb awplus-gui_550_21.gui flash
   ```

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

   ```
   awplus#dir
   ```

3. Stop and restart the HTTP service:

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

4. Log into the GUI:

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

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

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

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

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

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

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

On AR4050S, AR3050S, AR2050V and AR2010V devices, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

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

Check if the GUI is installed

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

Browse to the GUI

Perform the following steps to browse to the GUI.

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

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

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

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

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

3. If you do not see a login page, you need to install the GUI, as described in "Install the GUI if it is not installed" on page 75. If you see a login page, log in. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.0-1.5 is 2.7.1. If you have an earlier version, update it as described in "Update the GUI if it is not the latest version" on page 75.

Install the GUI if it is not installed

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

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

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

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

   ```
   awplus# update webgui now
   ```

4. Make sure the HTTP service is running:

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

5. Log into the GUI:

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

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

Update the GUI if it is not the latest version

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

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

   ```
   awplus# update webgui now
   ```

2. Stop and restart the HTTP service:

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

3. Log into the GUI:

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

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