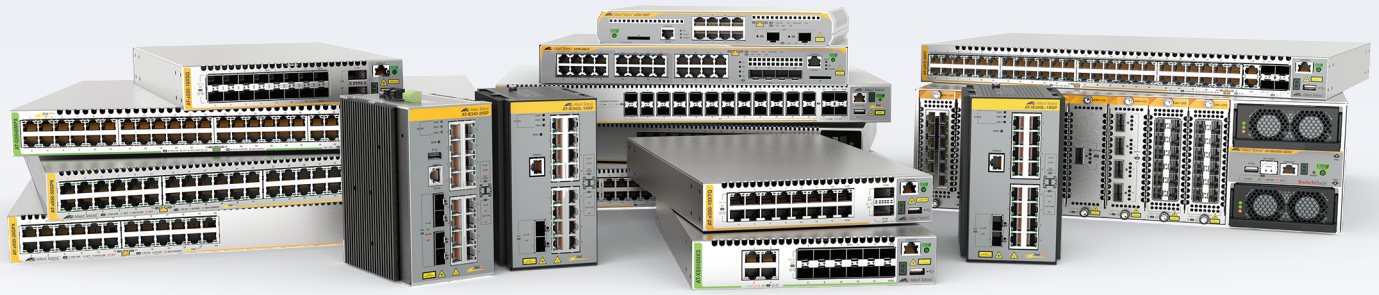
Release Note for AlliedWare Plus Software Version 5.5.3-0.x



AlliedWare Plus OPERATING SYSTEM

AMF Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S-5G
AR4050S
AR3050S
AR2050V
AR2010V
AR1050V

» 5.5.3-0.1 » 5.5.3-0.2 » 5.5.3-0.3 » 5.5.3-0.4

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/**

Contents

What's New in Version 5.5.3-0.4

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-0.4.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 58.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 60. 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		10/2023	vaa-5.5.3-0.4.iso (VAA OS) vaa-5.5.3-0.4.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-0.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2023	SBx81CFC960-5.5.3-0.4.rel
SBx908 GEN2	SBx908 GEN2	10/2023	SBx908NG-5.5.3-0.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	10/2023	x950-5.5.3-0.4.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	10/2023	x930-5.5.3-0.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2023	x550-5.5.3-0.4.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	10/2023	x530-5.5.3-0.4.rel
x330-10GTX x330-20GTX x330-28GTX	x330	10/2023	x330-5.5.3-0.4.rel
x320-10GH x320-11GPT	x320	10/2023	x320-5.5.3-0.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2023	x230-5.5.3-0.4.rel
x220-28GS x220-52GT x220-52GP	x220	10/2023	x220-5.5.3-0.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	10/2023	IE340-5.5.3-0.4.rel
IE220-6GHX IE220-10GHX	IE220	10/2023	IE220-5.5.3-0.4.rel
IE210L-10GP IE210L-18GP	IE210L	10/2023	IE210-5.5.3-0.4.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	10/2023	XS900-5.5.3-0.4.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	10/2023	GS980MX-5.5.3-0.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2023	GS980EM-5.5.3-0.4.rel
GS980M/52 GS980M/52PS	GS980M	10/2023	GS980M-5.5.3-0.4.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	10/2023	GS970EMX-5.5.3-0.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2023	GS970-5.5.3-0.4.rel
AR4000S-Cloud		10/2023	AR-4000S-Cloud-5.5.3-0.4.iso
10GbE UTM Firewall		10/2023	ATVSTAPL-1.8.1.iso and vfw-x86_64-5.5.3-0.4.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	10/2023	AR4050S-5.5.3-0.4.rel AR3050S-5.5.3-0.4.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	10/2023	AR2050V-5.5.3-0.4.rel AR2010V-5.5.3-0.4.rel AR1050V-5.5.3-0.4.rel

Caution: Software version 5.5.3-0.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 5.5.3 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.3 license installed, that license also covers all later 5.5.3 versions, including 5.5.3-1.x and 5.5.3-2.x. Such switches will 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 54 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 56.

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

The 5.5.3-0.4 software version is not ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the enhancements available in 5.5.3-0.4:

OpenFlow in-band controller connection

ER-5516 *Available on: IE220, IE340, SBx908NG, x230, x330, x530, x550, x930, and XS900 Series*

From version 5.5.3-1.2 onwards, AlliedWare Plus devices support in-band controller connection.

It is normal to connect the OpenFlow switch to its controller via a dedicated port which is not running as an OpenFlow port. In many cases with AlliedWare Plus devices, the eth0 port will be suitable for this purpose, although any port not configured as an OpenFlow port, in its own VLAN and with a properly assigned IP address will suffice.

There is however a mode in Open vSwitch that allows the controller connection to take place over an OpenFlow port. This is known as an 'in-band' controller connection.

Previously, OpenFlow did not allow in-band controller connections to be defined.

This software version adds support for this by adding an optional parameter, 'in-band' to the **openflow controller** command.

Syntax

```
openflow controller <controller-name> {tcp|ssl} <address>
<port> [in-band]
```

Example To add an Openflow controller for the switch whose name is 'controller1', with the address '10.1.2.1,' using the TCP protocol, and the IANA assigned port number of 6653. This is also an in-band controller:

```
awplus# configure terminal
awplus(config)# openflow controller controller1 tcp 10.1.2.1
6653 in-band
awplus(config)# interface of0
awplus(config-if)# ip address 10.45.234.1/24
```

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

Port authentication and 802.1x retransmission

ER-5399 *Available on: all AlliedWare Plus devices*

From version 5.5.3-0.4 onwards, AlliedWare Plus devices support the 802.1X retransmission mechanism.

This means that:

- if the Supplicant does not respond on an EAP Request, the Authenticator resends the EAP Request.
- if a timeout occurs and the maximum number of retransmissions is reached, the authentication process will fail.

This change is ISSU compatible with conditions. As long as 'dot1x max-req' is not configured on the new release during upgrade, the upgrade process is safe because without configuring 'dot1x max-req' there is no difference in authd in old and new releases. It does not require to boot LIFs with new release as the change exists in authd only.

To configure the maximum number of retransmissions, a new command is available:

Syntax

```
dot1x max-req <1-10>

no dot1x max-req
```

Example To configure the maximum number of EAP Request retransmission attempts for interface port1.0.1 to 3, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dot1x max-req 3
```

ISSU: Effective when CFCs upgraded

AMF auto-recovery for x330 and GS970EM series

ER-5385 *Available with x330 and GS970EM Series switches*

This enhancement introduces support for AMF auto-recovery on x330 and GS970EM Series when stackports have been disabled.

You can use the command **no stack <id> enable persistent** to create an internal persistent file on the replacement device which will be used during AMF auto recovery. This disables stacking ports and allows them to be used as AMF uplinks.

Previously, the x330 Series did not have the feature to prepare the device for atmf auto-recovery via default stacking ports. If a stack port is used as an AMF uplink port, and when that switch is recovered by AMF auto recovery with a replacement switch which has **no stack enable**, then auto recovery cannot be started, because configuration of that switch is not default.

Issues Resolved in Version 5.5.3-0.4

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

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79282	**ACL**	Previously, modifying a named IPv4 ACL group, configured using the **`acl-group ip address`** command, by adding or deleting an IP address entry, could lead to incorrect application of hardware access-lists on an interface when there were multiple hardware access-lists configured. Similar behaviour could occur for the named port ACL group commands, **`acl-group ip port`** and **`acl-group ipv6 address`**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79459	**ACL**	Previously, the system did not output any error when an ACL list on a port was oversubscribed. 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-78746	**AMF**	Previously, a non-existent AMF node was displayed on the AMF security list and it could not be removed manually. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79084	**AMF**	Previously, executing a 'delete' after performing certain AMF provisioning actions, such as configuring a provisioned node's configuration file, backup configuration file, firmware release, or backup firmware release, could result in leaving AMF provisioning without a valid working directory. This meant that subsequent AMF provisioning actions 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	–	–
CR-79709	**AMF**	Previously, it was possible for an AMF network to become unstable due to too many entries in the AMF database. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	Y	–	–
CR-79908	**AMF**	Previously, the AMF working-set output file was inaccessible due to restricted permissions under **`strict-user-process-control`** configuration. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-78747	**AMF, VCStack**	Previously, on a VCStack configured for AMF, there was a slight chance of a core dump of the 'ATMF-Topo' process. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-79757	**API, IPv6**	Previously, configurations involving softwire (MAP-E or LW4o6) may have occasionally experienced benign core-file generation related to a process called 'lua'. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-77632	**ARP / Neighbor Discovery, EPSR, MAC Thrashing, VCStack**	Previously, it was possible for EPSR blocking to be defeated for ARP packets (request and reply) ingressing a port on a VCS stack if the ingress port was on the backup member. This issue has been resolved.	Y	–	–	–	–	Y	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-79525	**ARP Neighbor Discovery**	Previously, ARP learning was causing memory exhaustion. 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	–
CR-75715	**ARP Neighbourhood Discovery**	Previously, on x930, x950, and SBx908 GEN2 platforms, the entries created by **`arp-mac-disparity unicast`** were not VLAN aware and could affect traffic on other VLANs. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	Y	–	–	–	–	–	–	–
CR-79616	**BFD**	Previously, the command **`show BFD peer`** would display VRFs according to their internal interface names rather than their user configured names. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	–	–	Y	Y	–	–
CR-77438	**Bootup**	Previously, the IE340 was slow to boot due to internal storage configurations. The boot up time has now been significantly improved.	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-79352	**Cellular Modem**	For the AR-4050S-5G: Previously, on occasion, the modem could be slow to start up and the band information would not be available, which resulted in an unexpected system re-start. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–
CR-79624	**Configuration Replay, Loop Protection**	Previously, when some VLANs were configured with names, creating an MST instance with one or more VLANs 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	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79447	**Device Security, File System, AMF**	Previously, when the command **`strict-user-process-control`** was executed on a working-set, it was only successfully executed on the local node. This issue has been resolved. With this software update, the command **`strict-user-process-control`** can only be executed on local nodes. To make the behaviour more apparent, now the command can only be executed either on a console of a node, or a working-set containing only the local node. 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-79324	**DHCP Snooping, Private VLAN**	Previously, when DHCP-snooping was in use in conjunction with private VLANs, DHCP responses arriving on a promiscuous port would not be received by a DHCP client attached via an isolated private VLAN. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	Y	–	–	–	Y	–	Y	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–
CR-78714	**DNS**	Previously, there could be issues loading web pages due to a DNS error. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79163	**DNS**	Previously, the DNS relay process could fail when upstream DNS servers were unreachable and deadtime was exceeded. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79420	**DNS**	This software update addresses a DNS vulnerability issue as specified in CVE-2022-4904 ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79421	**DNS**	This software update addresses a DNS vulnerability issue as specified in CVE-2023-28450. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79935	**DPI, Web Control**	Previously, when Digital Arts Web Categorization for either Web Control or DPI was enabled, it could cause memory exhaustion. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	–
CR-79328	**EPSR, VCStack**	Previously, if an EPSR ring was broken, a stack member in the EPSR ring could fail to rejoin the stack when the EPSR ring recovered. This issue has been resolved.	Y	Y	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-78551	**File System**	Previously, when the "strict-user-process-control" feature was enabled, certain system only files could still be accessed via the **mail** facility. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-78553	**File System**	Previously, when the "strict-user-process-control" feature was enabled, certain system only files could still be accessed via **SCP** or **SFTP**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79763	**Firewall**	Previously, a firewall rule was still getting hit even after removing zone/subnet/host from the rule. Configuration changes would only take effect after a device restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79948	**Firewall**	Previously, when entities had hosts or networks removed, the firewall rules that used these entities would continue to act on the removed entities. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-79415	**HTTP Service**	This software update addresses a HTTP Service vulnerability as specified in CVE-2023-25725 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-79747	**IDS/IPS**	This software update improves the performance of IPS basic (No provider).	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-79493	**IPv6**	With this software update, adding or removing an IPv6 address from a VLAN now notifies eventwatch on Vista Manager. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79167	**IPv6, Multicast**	Previously, IPv6 unregistered multicast packets that had "no next header" as an IPv6 extended header, were not being snooped by MLD snooping. 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-76763	**IPv6, Tunneling**	Previously, if one of the transactions to the map rule server failed, it could result in the softwire configuration being deleted and cause the IPv4 tunnel connectivity to be removed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79751	**IPv6, VRF-lite**	Previously, in certain situations, router-advertisements from connected routers could be lost following IPv6 being re-enabled (i.e. disabled then enabled). This was due to the 'RA-received' flag not being reset correctly when DAD was initiated on an interface. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-76785	**LACP**	Previously, executing the **`show diagnostic channel-group`** command could result in a gradual accumulation of memory usage per channel-group. Unfortunately, this memory was not released or freed after each run of the command. 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	–	–
CR-79291	**LLDP**	Previously, IE220 Series included the 'Type 3 and Type 4 extension' fields in the LLDP Power via MDI TLV, in LLDP packets sent from PoE+ (802.3at) ports. These fields should not have been included as the 'Type 3 and Type 4 extension' fields are PoE++ (802.3bt) only. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-79251	**Loop Detection**	Previously, after a system boot up, the first time a packet loop was detected by the loop protection feature, the specified action to break the loop did not operate correctly. LDF did operate correctly for any subsequently detected loops. This issue has been resolved.	Y	Y	–	–	–	Y	–	Y	–	Y	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79665	**MLD**	Previously, static MLD groups were not correctly added to interfaces on startup or when interface state changed. 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	–	–
ER-5516	**OpenFlow**	OpenFlow in-band controller connection From version 5.5.3-1.2 onwards, AlliedWare Plus devices support in-band controller connection.	–	Y	–	–	–	Y	–	–	Y	–	–	Y	Y	–	Y	–	–	–	–	–	–	–	–	–	–
CR-79183	**Pluggable Transceivers**	Previously, on very rare occasions, a system re-boot could occur following the removal of an SFP. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-72577	**Pluggable Transceivers**	Previously, under some circumstances, the x220, x320, x530, x530L, and GS980MX series could log a large amount of "*Port Manager queue has grown to XXX (250)*" messages, if the stacking DAC cable was inserted in the SFP+ port. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-79612	**Pluggable Transceivers**	Previously, on x330 series, some SFPs might not be able to correctly link up with other link partners. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-78924	**PoE, LLDP**	Previously, on platforms that support PoE: If LLDP was enabled and the Power via MDI TLV included **`lldp tlv-select all`** or **`lldp tlv-select power-management`**, then in rare cases, the PSE allocated power value in the LLDP packet transmitted was not calculated from the PD requested power value included in the same packet, and sometimes the PSE allocated power field contained an old value. This functionality was not conforming to the IEEE 802.3 specification (specifically "33.6.2 Data Link Layer classification timing requirements"). 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	–	–	–	–	–	–	–	–
CR-79057	**Port Configuration**	Previously, the ports on the x330 Series could occasionally flap when executing the **`show platform port`** command. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-73124	**Port Configuration VCStack**	Previously, the **`medium-type copper`** or **`medium-type fiber`** configuration would not apply correctly to a member joining a running stack and the configuration would be removed from the running-configuration. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-79410	**RADIUS**	This software update addresses RADIUS vulnerabilities as specified in CVE-2022-41860 and CVE-2022-41861. 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-79827	**Removable Media**	Previously, on x230 platforms there was an issue where an SD-card inserted into the slot may fail to be mounted by the device. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79427	**Security**	This software update addresses a Linux kernel vulnerability as specified in CVE-2023-0464. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79698	**Security**	With this update, the **`atmf cleanup`** and **`erase factory-default`** commands are not able to be run when the **`strict-user-process-control`** feature is enabled. The command **`strict-user-process-control`** must be disabled before these commands can be executed. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-78845	**Security, SSL**	This software update upgrades OpenSSL to 1.1.1u to address the security vulnerabilities specified in: CVE-2023-0286, CVE-2023-0215, CVE-2022-4450 and CVE-2022-4304.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-78955	**SNMP**	Previously, in SNMP traps for MAC thrashing, the VLAN ID was set to 0. This is now resolved and the VLAN ID is set to the VLAN the thrashing was detected on. 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-80830	**SNMP**	Previously, if SNMP service was disabled using the command **`no snmp-server`** and then re-enabled 10 minutes or longer later with the command **`snmp-server`**, some MIB objects in System Group (MIB-2, 1), such as System Contact, System Name, etc, would become unavailable. 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	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-77128	**SW Bridging**	Previously, the user configured MTU value for tunnel dot1q sub interfaces could sometimes change to a lower value, causing packets to be dropped. This issue has been resolved, and the user configured value will always be respected.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	–
CR-77361	**Switching**	Previously, on x530, x530L, and GS980MX Series, when changing to a lower port speed of 1G or 100M, the 10 or 18 port models might take a long time to link up, or might fail to link. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-79290	**Syslog, Bootup**	Previously, there was an internal issue with syslog, resulting in slow initialisation. 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-78367	**System**	Although the DoS vulnerability was not observed on AlliedWare Plus, a patch for CVE-2022-3435 has been implemented upstream as a precautionary measure. This patch effectively addresses the potential vulnerability. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79417	**System**	This software update addresses a security vulnerability as specified in CVE-2023-1095 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-79433	**System**	This software update addresses a security vulnerability as specified in CVE-2023-1077. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79435	**System**	This software update addresses a security vulnerability as specified in CVE-2023-0179. 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-79781	**System**	Previously, repeated entries of 'CTRL + C' keys on the CLI for copying, could cause an unexpected device restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-79521	**Tunnel**	Previously, the first VNE provisioning attempt could fail because the IPv6 address was not yet ready as it was in the process of being configured. This issue has been resolved. Now, the first attempt is delayed until the address is ready.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-79531	**Tunnel**	Previously, an update from the VNE provisioning server would be requested when the device received an RA, but there was no meaningful change to the IPv6 addresses of the interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–
CR-80188	**Tunnel**	Previously, the authentication URL was required to match the DNS TXT record to be able to send the username and password as part of the HTTP request. However, this is not a mandatory requirement of the specification. The URL in the **`tunnel provisioned authentication`** command can now be set as "any" so that the username and password will be sent regardless of the retrieved URL. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79359	**Tunneling**	Previously, when the MTU for a dot1q interface was left unset, the automatically calculated value was incorrect and often far lower than the MTU of the parent tunnel interface. This issue has now been resolved and the dot1q interface MTU will always be 4 bytes less than the parent tunnel MTU, to account for the encapsulation header size. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-79395	**Tunneling**	Previously, under some circumstances, IPSec tunnels could be unreachable over other IPSec tunnels. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–
CR-79116	**Unicast Routing QoS**	Previously, if QoS egress queue drop/transmit counters overflowed in hardware, the counters in **`show mls qos interface INTERFACE queue-counters`** would show correct values, however the CPU would become busy. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	Y	–	–	–	–	–	Y	–	Y	–	Y	–	–	–	Y	–	–	–	–	–	–	–	–
CR-79364	**Upstream Forwarding**	Previously, when moving hosts from an upstream to a downstream port, the device could undergo an unexpected system re-start. 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-78619	**VCStack**	Previously, on x950 Series stacks, under rare occasions, the stacking VLAN traffic would not be processed timely, resulting in TIPC timeouts and resiliency link healthcheck failures. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79504	**VCStack**	Previously, IP addresses learned by DHCP would not be properly learned by a backup member that joined an existing stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	–	–	–	–	–	–	–	–	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-78939	**VCStack**	Previously, after a stack member was rebooted, the stack master would generate a log: "*Failed to receive ipifwd message (-5)*" . This log was indicative of an internal error processing the loss of the interfaces and aggregators configured on the rebooting stack member. This issue has been resolved.	Y	Y	–	–	–	Y	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-80241	**VCStack**	Previously, a polling request from Vista Manager 3.10 or later could cause a system reboot on a VCStack master if the polling request arrived immediately after a VCStack failover, while the old master was in the process of rejoining the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-80579	**VCStack**	Previously, a system reboot could occur on an x930GSTX stack if the command **`show interface status`** was entered while connected via remote-login to a backup member, and if there was a linked up SFP inserted into another stack member. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-80760	**VCStack**	Previously, when SBx8100 line cards were rebooted via the **`reboot card`** command, in rare cases a VCStack Plus separation could occur. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-74973	**VCStack**	Previously, when a chassis was joining VCStack Plus with another chassis, the system could experience a duplicate master or a LIF may have had a problem joining. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-62372	**VCStack**	Previously, members of SBx908 GEN2 or x950 variant stacks could occasionally fail to intercommunicate properly and would show TIPC timeout messages. In very rare cases, this could lead to a duplicate master followed by one stack member rebooting. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–
CR-74973	**VCStack**	Previously, when a stack member was joining the stack, the other stack member might experience a duplicate master. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-79428	**VRF-lite**	Previously, the **`show run vrf`** output did not include BGP configuration. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79100	**VRRP**	Previously, when multiple instances of VRRP were running on different subnets with varying subnet masks, there was a problem where some of the VRRP virtual router addresses became unreachable. This occurred due to miscalculations in assigning the masks to the virtual router addresses. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–

What's New in Version 5.5.3-0.3

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-0.3.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 58.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 60. 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		07/2023	vaa-5.5.3-0.3.iso (VAA OS) vaa-5.5.3-0.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-0.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	07/2023	SBx81CFC960-5.5.3-0.3.rel
SBx908 GEN2	SBx908 GEN2	07/2023	SBx908NG-5.5.3-0.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	07/2023	x950-5.5.3-0.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	07/2023	x930-5.5.3-0.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2023	x550-5.5.3-0.3.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	07/2023	x530-5.5.3-0.3.rel
x330-10GTX x330-20GTX x330-28GTX	x330	07/2023	x330-5.5.3-0.3.rel
x320-10GH x320-11GPT	x320	07/2023	x320-5.5.3-0.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2023	x230-5.5.3-0.3.rel
x220-28GS x220-52GT x220-52GP	x220	07/2023	x220-5.5.3-0.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	07/2023	IE340-5.5.3-0.3.rel
IE220-6GHX IE220-10GHX	IE220	07/2023	IE220-5.5.3-0.3.rel
IE210L-10GP IE210L-18GP	IE210L	07/2023	IE210-5.5.3-0.3.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	07/2023	XS900-5.5.3-0.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	07/2023	GS980MX-5.5.3-0.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	07/2023	GS980EM-5.5.3-0.3.rel
GS980M/52 GS980M/52PS	GS980M	07/2023	GS980M-5.5.3-0.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	07/2023	GS970EMX-5.5.3-0.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2023	GS970-5.5.3-0.3.rel
AR4000S-Cloud		07/2023	AR-4000S-Cloud-5.5.3-0.3.iso
10GbE UTM Firewall		07/2023	ATVSTAPL-1.8.1.iso and vfw-x86_64-5.5.3-0.3.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	07/2023	AR4050S-5.5.3-0.3.rel AR3050S-5.5.3-0.3.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	07/2023	AR2050V-5.5.3-0.3.rel AR2010V-5.5.3-0.3.rel AR1050V-5.5.3-0.3.rel

Caution: Software version 5.5.3-0.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 5.5.3 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.3 license installed, that license also covers all later 5.5.3 versions, including 5.5.3-1.x and 5.5.3-2.x. Such switches will 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 54 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 56.

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

The 5.5.3-0.3 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.3-0.3

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

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79459	**ACL**	Previously, the system did not output any error when an ACL list on a port was oversubscribed. 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	–	–	–	–	–	–	–
CR-78714	**DNS**	Previously, there could be issues loading web pages due to a DNS error. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-72577	**Pluggable Tranceivers**	Previously, under some circumstances, the x220, x320, x530, x530L, GS980MX and GS980EM series could log a large amount of "Port Manager queue has grown to XXX (250)" messages, if the stacking DAC cable was inserted in the SFP+ port. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	Y	–	–	–	Y	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-79504	**VCStack**	Previously, IP addresses learned by DHCP would not be properly learned by a backup member that joined an existing stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	Y	Y	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-78939	**VCStack**	Previously, after a stack member was rebooted, the stack master would generate a log: "*Failed to receive ipifwd message (-5)*" . This log was indicative of an internal error processing the loss of the interfaces and aggregators configured on the rebooting stack member. This issue has been resolved.	Y	Y	–	–	–	Y	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–

What's New in Version 5.5.3-0.2

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
AR4000S-Cloud
10GbE UTM Firewall
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-0.2.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 58.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 60. 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		06/2023	vaa-5.5.3-0.2.iso (VAA OS) vaa-5.5.3-0.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-0.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	06/2023	SBx81CFC960-5.5.3-0.2.rel
SBx908 GEN2	SBx908 GEN2	06/2023	SBx908NG-5.5.3-0.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	06/2023	x950-5.5.3-0.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	06/2023	x930-5.5.3-0.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2023	x550-5.5.3-0.2.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	06/2023	x530-5.5.3-0.2.rel
x330-10GTX x330-20GTX x330-28GTX	x330	06/2023	x330-5.5.3-0.2.rel
x320-10GH x320-11GPT	x320	06/2023	x320-5.5.3-0.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	06/2023	x230-5.5.3-0.2.rel
x220-28GS x220-52GT x220-52GP	x220	06/2023	x220-5.5.3-0.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	06/2023	IE340-5.5.3-0.2.rel
IE220-6GHX IE220-10GHX	IE220	06/2023	IE220-5.5.3-0.2.rel
IE210L-10GP IE210L-18GP	IE210L	06/2023	IE210-5.5.3-0.2.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	06/2023	XS900-5.5.3-0.2.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	06/2023	GS980MX-5.5.3-0.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	06/2023	GS980EM-5.5.3-0.2.rel
GS980M/52 GS980M/52PS	GS980M	06/2023	GS980M-5.5.3-0.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	06/2023	GS970EMX-5.5.3-0.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2023	GS970-5.5.3-0.2.rel
AR4000S-Cloud		06/2023	AR-4000S-Cloud-5.5.3-0.2.iso
10GbE UTM Firewall		06/2023	ATVSTAPL-1.8.1.iso and vfw-x86_64-5.5.3-0.2.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	06/2023	AR4050S-5.5.3-0.2.rel AR3050S-5.5.3-0.2.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	06/2023	AR2050V-5.5.3-0.2.rel AR2010V-5.5.3-0.2.rel AR1050V-5.5.3-0.2.rel

Caution: Software version 5.5.3-0.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 5.5.3 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.3 license installed, that license also covers all later 5.5.3 versions, including 5.5.3-1.x and 5.5.3-2.x. Such switches will 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 54 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 56.

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

The 5.5.3-0.2 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the enhancements in 5.5.3-0.2

AMF auto recovery when stackports disabled

ER-5385: Available on GS970EMX and x330 Series.

This software update provides support for AMF auto recovery on the x330 and GS970EMX Series when stackports have been disabled.

The new optional parameter 'persistent' added to the command **no stack enable,** enables the creation of an internal persistent file on the replacement device. This file is utilized during AMF auto recovery to deactivate stacking ports, enabling them to be utilized as AMF uplinks.

In the past, the x330 and GS970EMX Series lacked the capability to ready the device for AMF auto-recovery through default stacking ports. If a stack port was utilized as an AMF uplink port and the switch underwent AMF auto-recovery with a replacement switch that had the **no stack enable** configuration, the auto-recovery process could not be initiated. This occurred due to the non-default configuration of the replacement switch.

Syntax `no stack <1-8> enable [persistent]`

Example To allow default stacking ports to be disabled and used as AMF uplinks during AMF auto-recovery of the VCS device via the AMF network, use the following commands:

```
awplus# configure terminal
awplus(config)# no stack 1 enable persistent
```

Issues Resolved in Version 5.5.3-0.2

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

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	IE510	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79282	**ACL**	Previously, modifying a named IPv4 ACL group, configured using the "**`acl-group ip address`**" command, by adding or deleting an IP address entry, could lead to incorrect application of hardware access-lists on an interface when there are multiple hardware access-lists configured. Similar behaviour could occur for the named port ACL group commands, **`acl-group ip port`** and **`acl-group ipv6 address`**. 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-78746	**AMF**	Previously, a non-existant AMF node was displayed on the AMF security list and it could not be removed manually. 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	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	IE510	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79084	**AMF**	Previously, executing a "delete" after performing certain AMF provisioning actions, such as configuring a provisioned node's configuration file, backup configuration file, firmware release, or backup firmware release, could result in leaving AMF provisioning without a valid working directory. This meant that subsequent AMF provisioning actions 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
CR-78747	**AMF, VCStack**	Previously, on a VCStack configured for AMF, there was a slight chance of a core dump of the 'ATMF-Topo' process. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-77632	**ARP / Neighbor Discovery, EPSR, MAC Thrashing, VCStack**	Previously, if the ingress port on a VCS (Virtual Chassis System) stack belonged to the backup member, it was possible to defeat EPSR (Ethernet Ring Protection Switching) blocking for ARP packets (both requests and replies) entering the port. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	Y	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-79352	**Cellular Modem**	Band restriction for wireless network is applied after a device boots. Previously, on occasion, the modem could be slow to start up and the band information would not be available, which resulted in an unexpected re-start. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	IE510	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79163	**DNS**	Previously, the DNS relay process could fail when upstream DNS servers were unreachable and deadtime was exceeded. 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-79328	**EPSR, VCStack**	Previously, if an EPSR ring was broken, a stack member in the EPSR ring could fail to rejoin the stack when the EPSR ring recovered. This issue has been resolved.	Y	Y	–	–	–	Y	–	–	Y	–	–	–	Y	–	–	Y	Y	–	Y	–	–	–	–	–	–	–
CR-78551	**File System**	Previously, when the "strict-user-process-control" feature was enabled, certain system only files could still be accessed via the **mail** facility. 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	–	–
CR-78553	**File System**	Previously, when the "strict-user-process-control" feature was enabled, certain system only files could still be accessed via SCP or SFTP. 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	–	–
CR-76763	**IPv6, Tunnelling**	Previously, if one of the transactions to the map rule server failed, it could result in the software configuration being deleted and cause the IPv4 tunnel connectivity to be removed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	IE510	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-76785	**LACP**	Previously, executing the **`show diagnostic channel-group`** command could result in a gradual accumulation of memory usage per channel-group. Unfortunately, this memory was not released or freed after each run of the command. 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	–	–
CR-79291	**LLDP**	Previously, IE220 Series included the 'Type 3 and Type 4 extension' fields in the LLDP Power via MDI TLV, in LLDP packets sent from PoE+ (802.3at) ports. These fields should not have been included as the 'Type 3 and Type 4 extension' fields are PoE++ (802.3bt) only. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-79251	**Loop Detection**	Previously, after a system boot up, the first time a packet loop was detected by the loop protection feature, the specified action to break the loop did not operate correctly. LDF did operate correctly for any subsequently detected loops. This issue has been resolved.	Y	Y	–	–	–	Y	–	Y	–	–	Y	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-79183	**Pluggable Transceivers**	Previously, on very rare occasions, a system re-boot could occur following the removal of an SFP. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-79057	**Port Configuration**	Previously, the ports on the x330 Series could occasionally flap when executing the **`show platform port`** command. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	IE510	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-77361	**Switching**	Previously, on x530, x530L and GS980MX Series, when changing to a lower port speed of 1G or 100M, the 10 or 18 port models might take a long time to link up, or might fail to link. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-78367	**System**	Although the DoS vulnerability was not observed on AlliedWare Plus, a patch for CVE-2022-3435 has been implemented upstream as a precautionary measure. This patch effectively addresses the potential vulnerability. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
CR-79364	**Upstream Forwarding**	Previously when moving hosts from an upstream to a downstream port, the device could undergo an unexpected re-start. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	Y	–	–	–	–	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–	–
CR-78619	**VCStack**	Previously, on x950 Series stacks, under rare occasions, the stacking VLAN traffic would not be processed timely, resulting in TIPC timeouts and resiliency link healthcheck failures. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–
CR-62372	**VCStack**	Previously, members of SBx908 GEN2 or x950 variant stacks could occasionally fail to inter-communicate properly and would show TIPC timeout messages. In the worst case this would lead to a duplicate master followed by one stack member rebooting. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	IE510	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-79100	**VRRP**	Previously, when multiple instances of VRRP were running on different subnets with varying subnet masks, there was a problem where some of the VRRP virtual router addresses became unreachable. This occurred due to miscalculations in assigning the masks to the virtual router addresses. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–

What's New in Version 5.5.3-0.1

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
IE340 Series
IE220 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR2050V
AR2010V
AR1050V

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-0.1.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 58.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 60. 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		04/2023	vaa-5.5.3-0.1.iso (VAA OS) vaa-5.5.3-0.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-0.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	04/2023	SBx81CFC960-5.5.3-0.1.rel
SBx908 GEN2	SBx908 GEN2	04/2023	SBx908NG-5.5.3-0.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	04/2023	x950-5.5.3-0.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	04/2023	x930-5.5.3-0.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2023	x550-5.5.3-0.1.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	04/2023	x530-5.5.3-0.1.rel
x330-10GTX x330-20GTX x330-28GTX	x330	04/2023	x330-5.5.3-0.1.rel
x320-10GH x320-11GPT	x320	04/2023	x320-5.5.3-0.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2023	x230-5.5.3-0.1.rel
x220-28GS x220-52GT x220-52GP	x220	04/2023	x220-5.5.3-0.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	04/2023	IE340-5.5.3-0.1.rel
IE220-6GHX IE220-10GHX	IE220	06/2023	IE220-5.5.3-0.2.rel
IE210L-10GP IE210L-18GP	IE210L	04/2023	IE210-5.5.3-0.1.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	04/2023	XS900-5.5.3-0.1.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	04/2023	GS980MX-5.5.3-0.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	04/2023	GS980EM-5.5.3-0.1.rel
GS980M/52 GS980M/52PS	GS980M	04/2023	GS980M-5.5.3-0.1.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	04/2023	GS970EMX-5.5.3-0.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2023	GS970-5.5.3-0.1.rel
AR4000S-Cloud		04/2023	AR-4000S-Cloud-5.5.3-0.1.iso
10GbE UTM Firewall		04/2023	ATVSTAPL-1.8.1.iso and vfw-x86_64-5.5.3-0.1.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	04/2023	AR4050S-5.5.3-0.1.rel AR3050S-5.5.3-0.1.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	04/2023	AR2050V-5.5.3-0.1.rel AR2010V-5.5.3-0.1.rel AR1050V-5.5.3-0.1.rel

Caution: Software version 5.5.3-0.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 5.5.3 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.3 license installed, that license also covers all later 5.5.3 versions, including 5.5.3-1.x and 5.5.3-2.x. Such switches will 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 54 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 56.

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

The 5.5.3-0.1 software version is not ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.3-0.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 53.

Support for PROFINET on IE340 Series

From version 5.5.3-0.1 onwards, AlliedWare Plus IE340 Series switches support PROFINET.

A fully conformant firmware version certified by Profinet International™ will be available on the IE340 Series as version 5.5.2-1.6 for customers who require a certified version.

PROFINET is a field bus open standard for data communication over Industrial Ethernet. PROFINET control and complexity exceeds older field bus systems like MODBUS.

The PROFINET Protocol suite interacts with and also specifies custom settings and profiles for other protocols. Amongst these are MRP, SNMP, and LLDP as well as using base 802.1Q facilities. PROFINET has different conformance classes for required features.

AlliedWare Plus™ devices:

- support Profinet Conformance Class B (CC-B).
- support one MRP ring for network redundancy. MRP interconnection is not supported.
- do not provide IO control/status to the external relays.
- currently support only one instance of PROFINET.

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

OpenVPN Two-Factor Authentication Enhancements

Available on all AlliedWare Plus firewalls and routers

From version 5.5.3-0.1 onwards Two-factor Authentication (2FA) for OpenVPN has been enhanced with the following features:

- OpenVPN certificate authentication (used as 2FA)
- 2FA self-registration
- 2FA email One-Time Password (OTP)

For more information about configuring these new 2FA features, see the OpenVPN Feature Overview and Configuration Guide.

IPsec certificate-based authentication

Available on all AlliedWare Plus firewalls and routers

From version 5.5.3-0.1 onwards, AlliedWare Plus firewalls and routers support IPsec certificate-based authentication.

IPsec certificate-based authentication provides a more secure, scalable, and manageable solution for secure IP communications than other methods like pre-shared keys.

IPsec also helps to meet regulatory and compliance requirements and provides non-repudiation. Non-repudiation is a security concept that ensures that a party cannot deny having performed a certain action, such as sending a message or making a transaction. It is typically achieved through the use of digital signatures, timestamps, and other forms of cryptographic evidence that can be used to prove that a particular action was taken by a specific individual or entity.

For more information about configuring certificate-based authentication on AlliedWare Plus firewalls and routers, see the IPsec Feature Overview and Configuration Guide.

Web Categorization and Web Control provider renamed from Webroot to OpenText

Available on AR4050S, AR4050S-5G, the 10GbE UTM Firewall, and AR4000S-Cloud

From version 5.5.3-0.1 onwards, the AlliedWare Plus provider for the Web Categorization and Web Control features has been renamed.

Formerly Webroot, the provider is now known as OpenText. While the name has changed, the functionality remains the same as before.

Updated commands

The provider has been updated in the following commands:

- provider (web-control)

```
awplus(config-web-control)# provider [digitalarts|opentext]
```

- web-categorization

```
awplus(config-dpi)# web-categorization [digital-arts|opentext]
```

- show dpi

```
awplus#show dpi
Status:      running
Provider:    built-in
Mode:        assured
Counters:    global only
Providing application database: disabled
Web Categorization:          enabled
Web Categorization Provider: opentext
```

For more information about advanced network security features on the AlliedWare Plus UTM firewalls, see the Advanced Network Protection Feature Overview and Configuration Guide.

Configuring multiple firewall instances

Available on the 10GbE UTM firewall

From version 5.5.3-0.1 onwards, a feature has been highlighted to show that the same licensed VST-APL-06 or VST-APL-10 appliance can host multiple virtual firewall instances. These multiple virtual UTM firewall instances may be created to manage different elements of a network independently, with capabilities equivalent to VRF-lite, including overlapping addressing. These multiple instances provide the functionality of VRF without the limitations of VRF-lite.

For more information about configuring multiple firewall instances, see the 10GbE UTM Firewall User Guide.

Speed-based licenses for AR4000S-Cloud Firewalls

From 5.5.3-0.1 onwards, there are two basic licenses available for AR4000S-Cloud firewalls: AT-AR4-VPN10S and AT-AR4-VPN10H.

The VPN10S “Standard speed” base license supports deploying on local hardware or in the cloud with 1/2.5/5G interface connectivity.

The VPN10H “High speed” base license supports deploying on local hardware or in the cloud with 10/25/40/100G interface connectivity.

Both the VPN10S and VPN10H base licenses include VPN connectivity for 10 branch office locations, as well as advanced firewall and routing functionality.

Secure TLS authentication in the mail client

Available on all AlliedWare Plus products

From version 5.5.3-0.1 onwards, AlliedWare Plus switches and firewalls support secure TLS authentication in the mail client.

If you are configuring your SMTP server for a device, you can send emails to SMTP servers over a TLS connection. This makes sending email from AlliedWare Plus devices more secure. It also allows people to use other SMTP servers that do not accept emails over clear-text connection.

A secure TCP connection is created after negotiation with the server, which involves choosing the encryption algorithm to use, STARTTLS or SMTPS.

For information about configuring secure TLS and SMTP on AlliedWare Plus switches and firewalls, see the Mail (SMTP) Feature Overview and Configuration Guide.

AMF auto-recovery for TQ5403 series APs

Available with AMF and AMF Plus for all AlliedWare Plus products except AMF Cloud, the 10GbE UTM firewall and AR2010V. Requires TQ5403 series firmware version 6.0.3-0.1 or later.

From version 5.5.3-0.1 onwards, it is possible to use AMF auto-recovery to recover a TQ5403, TQ5403e or TQm5403 access point. For a step-by-step example of how to set this up, see the Node Recovery chapter of the AMF Plus Feature Overview and Configuration Guide.

Using ACLs to drop unwanted packets without sending them to the CPU

Available on SBx908 GEN2, x950, x930, x550 and x230 Series switches.

From version 5.5.3-0.1 onwards, you can use a new action on hardware ACLs to drop packets and make sure that they aren't sent to the switch's CPU. This may be useful if you want to drop packets that AlliedWare Plus would normally send to the switch's CPU.

Note that on other AlliedWare Plus switches, the action of **deny** already prevents packets from going to the CPU.

For example, this new action may be useful if you have AMF Security and it is registering MAC addresses because it receives loop detection frames (LDF) from other switches in your network. You can use this action to prevent AMF Security from seeing the LDF frames.

For an example of using this to drop loop detection frames (LDF), see the Access Control List (ACL) Feature Overview and Configuration Guide.

Logging of packets denied by hardware Access Control Lists (ACLs)

Available on SBx908 GEN2, x950, x550, x530, x320, and x220 Series switches.

From version 5.5.3-0.1 onwards, you can turn on logging of packets that are denied by hardware IP ACLs, on the above switches. Hardware IP ACLs are ACLs with an ID number from 3000 to 3699. If you turn on logging, the switch will produce a log message when it drops denied packets.

For a step-by-step procedure, see the Access Control List (ACL) Feature Overview and Configuration Guide.

Disabling the eco-friendly button

Available on all AlliedWare Plus devices that have an eco-friendly button.

From 5.5.3-0.1 onwards, a new command lets you disable the eco-friendly button on the front panel of devices that have one. This stops the eco-friendly button from being accidentally pressed. Pressing the eco-friendly button turns off LEDs, so pressing it accidentally can lead to confusion about the state of the device.

The button is enabled by default. To disable it, use the command:

```
awplus(config)# no ecofriendly button enable
```

To enable the button again, use the command:

```
awplus(config)# ecofriendly button enable
```

Export and import two-factor authentication (2FA) user data

Available on all AlliedWare Plus firewalls and routers

From version 5.5.3-0.1 onwards, the process to export and import 2FA user data has been improved. You need this data if you replace a firewall and want to use the previous firewall's data. To export the user data, use the new command:

```
awplus#2fa export user-data
```

This exports the file to Flash with a filename like atl2fausers-20230215-2980.dat. Save the file to a suitable external location so it is available for later use.

To import the file onto a firewall, use the new command:

```
awplus#2fa import user-data source <file-location-and-name>
```

For example:

```
awplus#2fa import user-data source
tftp://192.168.1.1/atl2fausers-20230215-2890.dat
```

Note that you don't need to manually back this data up if you use AMF. AMF backs up this data and restores it as part of auto-recovery.

Support for IP multicast without UDP headers

Available on all AlliedWare Plus products that support multicast snooping

From version 5.5.3-0.1 onwards, AlliedWare Plus switches use IGMP or MLD snooping to process all unregistered multicast traffic. Previously, unregistered multicast traffic was only snooped if it had a UDP header.

Also, the switch will now drop IPv4 multicast packets that do not have a correctly matching MAC address and IPv4 address.

Support for the legacy ssh-rsa algorithm

Available on all AlliedWare Plus products

From version 5.5.3-0.1 onwards, a new command enables support for the legacy ssh-rsa algorithm. Support for this algorithm was removed in version 5.5.1-1.1 due to security concerns. Support for it is still disabled by default and you should only enable it if you cannot avoid using ssh-rsa. It cannot be enabled when in crypto secure mode.

To enable the ssh-rsa algorithm on the AlliedWare Plus SSH server, use the command:

```
awplus(config)#ssh server allow-legacy-ssh-rsa
```

To enable the ssh-rsa algorithm on the AlliedWare Plus SSH client, use the command:

```
awplus(config)#ssh client allow-legacy-ssh-rsa
```

Disabling use of the default route to resolve next hops in IP routing

Available on all AlliedWare Plus products that support BGP

From version 5.5.3-0.1 onwards, a new command allows you to stop BGP from using a default route to resolve next hops. This can be helpful when such use can lead to inappropriate next hops being incorrectly activated.

To disable use of the default route, use the command:

```
awplus(config)#no ip resolve-via-default
```

Use of the default route to resolve next hops is enabled by default.

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.3-0.x and may affect your device or network behavior if you upgrade:

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

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

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

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

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

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

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

The solution Before upgrading to the latest firmware version, upgrade to one of the specified older versions. See "Details for SBx908 GEN2 and x950 Series" on page 48 and "Details for x930 Series" on page 49 for details.

Affected Products

The following models could be affected:

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

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

Recovering from upgrading from an incompatible version

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

Details for SBx908 GEN2 and x950 Series

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

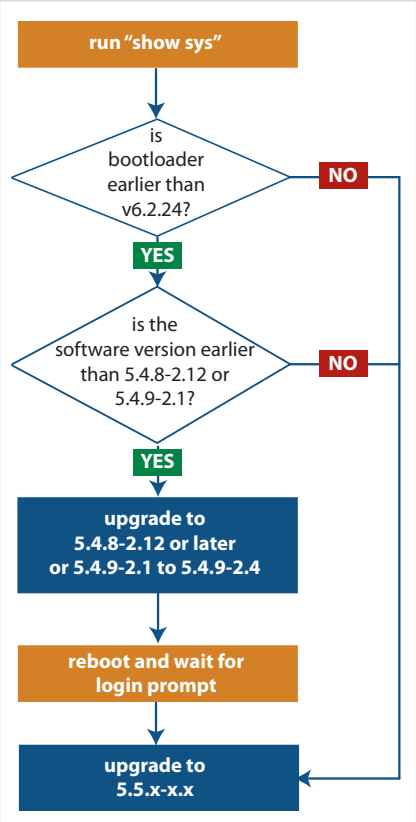
- 5.4.9-1.x
- 5.4.9-0.x
- any version before 5.4.8-2.12.

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

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

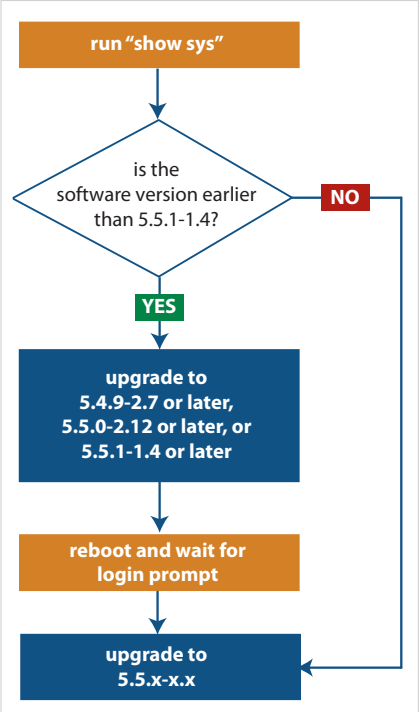
If it is not, upgrade to one of these versions before upgrading to the desired 5.5.x-x.x version.

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




```
awplus# show system
```

Details for x930 Series



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

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

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

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

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

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

```
awplus# show system
```

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.3 license on your switch if you are upgrading to 5.5.3-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 54 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 56.

Upgrading a VCStack with rolling reboot

Applies to all stackable AlliedWare Plus switches, except SBx8100

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

For SBx908 GEN2, x950 and x550 Series switches

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

- All versions from 5.5.0-x.x onwards

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

For x530 Series switches using DAC to stack

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

- All versions from 5.5.0-x.x onwards
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

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

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

- All versions from 5.4.5-x.x onwards
- 5.4.4-1.x

To use rolling reboot

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

Forming or extending a VCStack with auto-synchronization

Applies to all stackable AlliedWare Plus switches

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

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

For SBx908 GEN2, x950 and x550 Series switches

Auto-synchronization is supported between this version and:

- All versions from 5.5.0-x.x onwards

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

For CFC960 cards in an SBx8100 system

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

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

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

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

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

For x530 Series switches using DAC to stack

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

- All versions from 5.5.0-x.x onwards
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

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

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

- All versions from 5.4.7-x.x onwards
- 5.4.6-2.x
- 5.4.6-1.2 and all later 5.4.6-1.x versions.

It is not supported between this version and 5.4.6-1.1 or **any** earlier releases.

AMF software version compatibility

Applies to all AlliedWare Plus devices

We strongly recommend that all nodes in an AMF network run the same software release. However, if this is not possible, then nodes running this version are compatible with nodes running:

- All versions from 5.4.4-x.x onwards
- 5.4.3-2.6 or later.

Upgrading all devices in an AMF network

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

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

2. Decide which AMF upgrade method is most suitable.

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

Obtaining User Documentation

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

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

Verifying the Release File

On devices that **support crypto secure mode**, to ensure that the release file has not been corrupted or interfered with during download, you can verify the release file. To do this, enter Global Configuration mode and use the command:

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

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

This command compares the SHA256 hash of the release file with the correct hash for the file. The correct hash is listed in the table of Hash values below or in the release's sha256sum file, which is available from the Allied Telesis Download Center.

Caution

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

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

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

Table: Hash values

Product family	Software File	Hash
SBx8100	SBx81CFC960-5.5.3-0.4.rel	ac915a21063f15e4177a23ed35b8bf144465d2f030a9cf8b6bee3e7022520b2a
SBx908 GEN2	SBx908NG-5.5.3-0.4.rel	80f64d00c288e1ef106aca274b089116dbc48f7d9fc56585aad0b1b059a28e20
x950	x950-5.5.3-0.4.rel	80f64d00c288e1ef106aca274b089116dbc48f7d9fc56585aad0b1b059a28e20
x930	x930-5.5.3-0.4.rel	2c093bed003714b2840cd39d7beafdaeff5817ca8255d81fd2a7d4785efd83b2
x550	x550-5.5.3-0.4.rel	47413065a533ad05dd67b25208ac20e32d2b9076f4e4580878e122246b8f4a93
x530 & x530L	x530-5.5.3-0.4.rel	7d9142b24b092fe52ba02c8e48f2061d6fbcc90b4a46f8c8dbd03227fe533f0c
x330	x330-5.5.3-0.4.rel	e966b3984536817c737c6e8ef60a070258e2dc0ccbdd29cdf286772cff4a3b52
x320	x320-5.5.3-0.4.rel	7d9142b24b092fe52ba02c8e48f2061d6fbcc90b4a46f8c8dbd03227fe533f0c

Table: Hash values

Product family	Software File	Hash
x230 & x230L	x230-5.5.3-0.4.rel	60591efd4aa1b826d8c1732ec38761d5d960d50f232dc883e264a1a8fc5f52dc
x220	x220-5.5.3-0.4.rel	2e58fd83451c9bf0894144e92ed869c34892178746d28570b802ba4eccfc5e84
IE340 & IE340L	IE340-5.5.3-0.4.rel	7fa547c86f20c5c1dc4c91c41c92fc6ff6ddbfa020bd5d6709330ee5c7fd386a
IE220	IE220-5.5.3-0.4.rel	745122125975e7aeb8163fe05493545485a6f4aa806400eb8b13b342dd161903
XS900MX	XS900-5.5.3-0.4.rel	a06affb0b35d68b5bb495fbe127e8b680d77cbc78369363b0215ae769ca1f284
AR4050S-5G	AR4050S-5.5.3-0.4.rel	c100d63cea83a5c8290c9252bcef50af2e9d8ec3102154779e088d897a7d7836
AR4050S	AR4050S-5.5.3-0.4.rel	c100d63cea83a5c8290c9252bcef50af2e9d8ec3102154779e088d897a7d7836
AR3050S	AR3050S-5.5.3-0.4.rel	c100d63cea83a5c8290c9252bcef50af2e9d8ec3102154779e088d897a7d7836
AR2050V	AR2050V-5.5.3-0.4.rel	c100d63cea83a5c8290c9252bcef50af2e9d8ec3102154779e088d897a7d7836
AR2010V	AR2010V-5.5.3-0.4.rel	c100d63cea83a5c8290c9252bcef50af2e9d8ec3102154779e088d897a7d7836
AR1050V	AR1050V-5.5.3-0.4.rel	ea6654c05331fd365eb4a16cd5b3326adcb3dea8ed6d1592e078de5ae16e277c

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             : 30-Mar-2023
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                   : 5.5.3
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Aug-2023
License expiry date            : N/A
Release                        : 5.5.3
```

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             : 30-Mar-2023
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.5.3
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Aug-2023
License expiry date            : N/A
Release                        : 5.5.3
```

Installing this Software Version

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 54 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 56.

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

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

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

Product	Command
SBx8100 with CFC960	`awplus(config)# boot system SBx8100-5.5.3-0.4.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.3-0.4.rel`
x950 series	`awplus(config)# boot system x950-5.5.3-0.4.rel`
x930 series	`awplus(config)# boot system x930-5.5.3-0.4.rel`
x550 series	`awplus(config)# boot system x550-5.5.3-0.4.rel`
x530 series	`awplus(config)# boot system x530-5.5.3-0.4.rel`
x330-10GTX	`awplus(config)# boot system x330-5.5.3-0.4.rel`
x320 series	`awplus(config)# boot system x320-5.5.3-0.4.rel`
x230 series	`awplus(config)# boot system x230-5.5.3-0.4.rel`
x220 series	`awplus(config)# boot system x220-5.5.3-0.4.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.3-0.4.rel`
IE220 series	`awplus(config)# boot system IE220-5.5.3-0.4.rel`

Product	Command
IE210L series	`awplus(config)# boot system IE210-5.5.3-0.4.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.3-0.4.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.3-0.4.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.3-0.4.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.3-0.4.rel`
GS970EMX/10	`awplus(config)# boot system GS970EMX-5.5.3-0.4.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.3-0.4.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.3-0.4.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.3-0.4.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.3-0.4.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.5.3-0.4.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.3-0.4.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.3-0.4.rel`

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

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

6. Reboot using the new software version.

```
awplus# reload
```

Accessing and Updating the Web-based GUI

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

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

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

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

Browse to the GUI

Note: In version 5.5.2-2.1, AlliedWare Plus was enhanced so that only strong cipher suites can be used for accessing the Device GUI. This may prevent some very old browsers from accessing the GUI.

Perform the following steps to browse to the GUI.

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

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

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

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

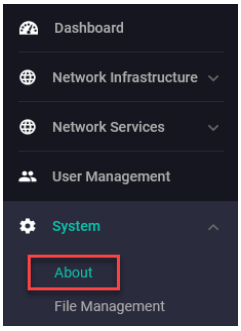
2. Open a web browser and browse to the IP address from step 1.

3. The GUI starts up and displays a login screen. Log in with your username and password. The default username is *manager* and the default password is *friend*.

Check the GUI version

To see which version you have, open the **System** > **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.3-0.4 is 2.15.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 61 or "Update the GUI on AR-Series devices" on page 62.



Update the GUI on switches

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

1. Obtain the GUI file from our Software Download center. The GUI filename to use with AlliedWare Plus v5.5.3-0.x is awplus-gui_553_29.gui.

   The file is not device-specific; the same file works on all devices. Make sure that the version string in the filename (e.g. 553) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

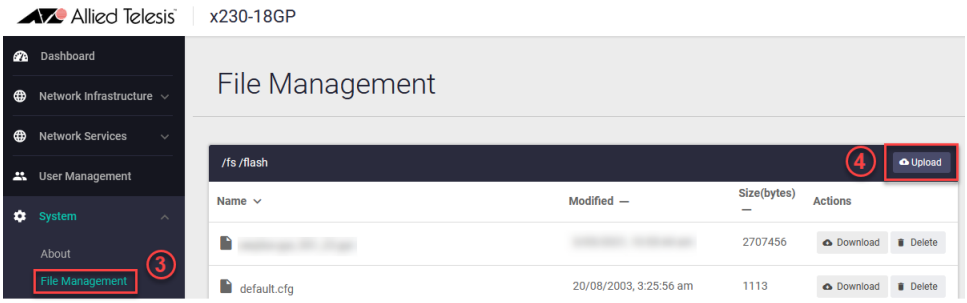
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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

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

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

4. Click **Upload**.



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

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

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

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

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

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

Update the GUI on AR-Series devices

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

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

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

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

3. Browse to the GUI and check that you have the latest version now, on the **System** > **About** page. You should have v2.15.0 or later.