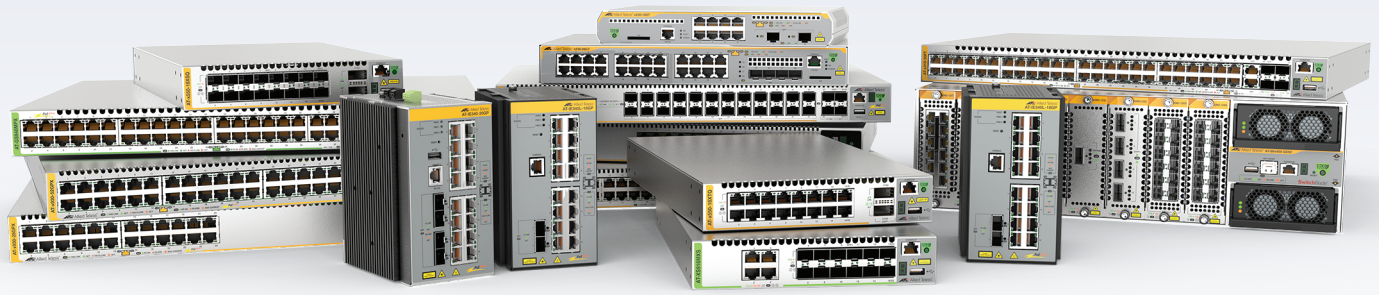
Release Note for AlliedWare Plus Software Version 5.5.3-1.x



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
AR1050V
TQ6702 GEN2-R

» 5.5.3-1.1 » 5.5.3-1.2 » 5.5.3-1.3 » 5.5.3-1.4

Acknowledgments

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

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

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

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

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

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

Getting the most from this Release Note

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

Contents

What's New in Version 5.5.3-1.4

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
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
AR1050V
TQ6702 GEN2-R

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-1.4.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 51.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 53. 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		12/2023	vaa-5.5.3-1.4.iso (VAA OS) vaa-5.5.3-1.4.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-1.4.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	12/2023	SBx81CFC960-5.5.3-1.4.rel
SBx908 GEN2	SBx908 GEN2	12/2023	SBx908NG-5.5.3-1.4.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	12/2023	x950-5.5.3-1.4.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	12/2023	x930-5.5.3-1.4.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	12/2023	x550-5.5.3-1.4.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	12/2023	x530-5.5.3-1.4.rel
x330-10GTX x330-20GTX x330-28GTX	x330	12/2023	x330-5.5.3-1.4.rel
x320-10GH x320-11GPT	x320	12/2023	x320-5.5.3-1.4.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	12/2023	x230-5.5.3-1.4.rel
x220-28GS x220-52GT x220-52GP	x220	12/2023	x220-5.5.3-1.4.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	12/2023	IE340-5.5.3-1.4.rel
IE220-6GHX IE220-10GHX	IE220	12/2023	IE220-5.5.3-1.4.rel
IE210L-10GP IE210L-18GP	IE210L	12/2023	IE210-5.5.3-1.4.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	12/2023	XS900-5.5.3-1.4.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	12/2023	GS980MX-5.5.3-1.4.rel
GS980EM/10H GS980EM/11PT	GS980EM	12/2023	GS980EM-5.5.3-1.4.rel
GS980M/52 GS980M/52PS	GS980M	12/2023	GS980M-5.5.3-1.4.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	12/2023	GS970EMX-5.5.3-1.4.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	12/2023	GS970-5.5.3-1.4.rel
AR4000S-Cloud		12/2023	AR-4000S-Cloud-5.5.3-1.4.iso
10GbE UTM Firewall		12/2023	ATVSTAPL-1.8.3.iso and vfw-x86_64-5.5.3-1.4.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	12/2023	AR4050S-5.5.3-1.4.rel AR3050S-5.5.3-1.4.rel
AR1050 V	AR-series VPN routers	12/2023	AR1050V-5.5.3-1.4.rel
TQ6702 GEN2-R	Wireless AP Router	12/2023	TQ6702GEN2R-5.5.3-1.4.rel

Caution: Software version 5.5.3-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.3 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 47 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 49.

Unsupported devices

Version 5.5.3-1.x does not support:

- AR2050V VPN routers
- AR2010V VPN routers

The last version to support the above devices is 5.5.3-0.x.

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

The 5.5.3-1.4 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the features and enhancements available in 5.5.3-1.4:

CR-81569 *Applies to: XS900MX, x230/x230L, x930, SBx81CFC960, AR3050S, and AR4050S*

Starting from version 5.5.3-1, AlliedWare Plus utilizes OpenSSL 3. On devices using the local RADIUS server with the default local trustpoint, and were initially booted with version 5.4.6-0.1 or earlier, the RADIUS server may fail to start. This is due to the certificate's incompatibility with OpenSSL 3, as it uses sha1WithRSAEncryption for signing, which is now deprecated. On certain platforms, this issue may result in a boot loop when the RADIUS server is enabled in the startup configuration.

This issue has been resolved, but corrective action is also required by the system administrator. Instead of failing to start, the RADIUS server will start without EAP/TLS support enabled and will emit critical log messages as follows:

user.crit awplus IMI[740]: RADIUS server certificate is not compatible with OpenSSL3.
user.crit awplus IMI[740]: RADIUS server TLS config will not be generated.
user.crit awplus IMI[740]: RADIUS server trustpoint must be regenerated.

If these log messages are emitted, the following commands can be run to regenerate the trustpoint:

```
configure terminal
radius-server local
no server trustpoint local
no crypto pki trustpoint local
crypto pki trustpoint local
radius-server local
server trustpoint local
end
crypto pki enroll local
```

Any client certificates that were signed with the RADIUS server's certificate will also need to be regenerated.

The command **show crypto pki certificates** has also been updated to include the algorithm information:

```
Certificates with the following lines are incompatible:

   Algorithms : Public Key : rsaEncryption, 1024 bits
              : Signature : sha1WithRSAEncryption

Certificates with the following lines are compatible:

   Algorithms : Public Key : rsaEncryption, 2048 bits
              : Signature : sha256WithRSAEncryption
```

ISSU: Effective when CFCs upgraded.

ER-5383 *Applies to: AR3050S, AR4050S, and AR4050S-5G*

This software release provides improved behavior when DPI in combination with NAT are under load.

ER-5604 *Applies to: GS970EMX, GS970M, XS900MX, IE340, IE210L, x230/x230L, x330, x550, x930, x950, SBx908Gen2, and IE220*

This software release provides improved stack reboot times. Previously, when adding a large number of ACL filters, especially when loading configuration, the process could take a considerable amount of time. This time has been reduced in most cases.

ER-5841 *Applies to: GS970EMX, GS970M, GS980EM, GS980M, GS980MX, XS900MX, IE340, IE210L, x220, x230/x230L, x240/SE240, x330, x530 / x530L, x550, x930, x950, SBx908Gen2, SBx81CFC960, AR3050S, AR1050V, AR4050S, x320, AR4050S-5G, and IE220*

Previously, user logins and logouts via the device GUI were not logged. These events are now logged at Notice level.

ISSU: Effective when ISSU complete

ER-5502 *Applies to: x530 / x530L*

Denial of Service (DoS) detection is now supported on the x530 Series. A Denial of Service attack is a malicious attempt to disrupt the normal functioning of a network, service, or website by overwhelming it with a flood of traffic, making it difficult or impossible for legitimate users to access the resources.

Issues Resolved in Version 5.5.3-1.4

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	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81208	**BFD**	Previously, changing the BFD configuration from multi-hop to single-hop did not work correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-81206	**BFD, BGP**	Previously, a BGP neighbour configured with BFD fallback could take too long to establish. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–
CR-50066	**BGP**	When using BGP on a stacked device that has multiple BGP neighbors configured for graceful restart, after a stack failover event that results in BGP graceful restart occurring, it was possible for one or more BGP peers to get stuck in the graceful restart state. This would prevent the device from ever leaving the graceful restart mode, which in turn could prevent it from properly learning or announcing BGP routes from neighbors until the BGP process was manually reset. This issue has been resolved. Now, when a BGP graceful restart occurs following a stack failover, the graceful restart mode will always eventually exit and normal BGP route convergence will resume. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	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	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81202	**BGP, VCStack**	Previously, when the VCStack master resets, routes going via the master were not deleted from the new master. BGP graceful restart, which is enabled by default on devices which are capable of running VCStacking, did not appear in the running-configuration, and could not be disabled from the CLI. This issue has now been resolved. BGP graceful restart is now enabled by default for all AlliedWare Plus products. This setting will appear in the running configuration when BGP is configured. If required, graceful restart can be disabled by using the command **`no bgp graceful-restart`**. BGP graceful restart capability also needs to be configured manually for each BGP peer, using the command **`neighbor [addr] capability graceful-restart`**. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-81175	**BGP, VCStack, VRF-lite**	Previously, when using **BGP** in a **VRF** on a stacked device that has multiple BGP neighbors configured for graceful restart, after a stack failover event that results in BGP graceful restart occurring, it was possible for one or more BGP peers to get stuck in the graceful restart state. This would prevent the device from ever leaving the graceful restart mode, which in turn could prevent it from properly learning or announcing BGP routes from neighbors until the BGP process was manually reset. This issue has been resolved. Now when a BGP graceful restart occurs following a stack failover, the graceful restart mode will always eventually exit and normal BGP route convergence will resume. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	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	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81247	**CLI**	Previously, after enabling 802.1q encapsulation on an Ethernet/ tunnel/bridge/WAN interface, the default MTU of this newly created sub-interface was displayed in the running-config. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-81342	**CLI**	Previously, If multiple commands were entered rapidly (e.g. using a script) into the command line interface, it was possible for the mode of the CLI session to change to EXEC mode unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-81665	**Crypto Secure Mode**	Previously, certificate processing may have failed when the device was in crypto secure-mode. This issue has been resolved.	–	Y	–	–	–	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR-81144	**Environmental Monitoring**	Previously, on the x930 Series, the supported PSU combination of AT-PWR250v2 and AT-PWR150 would set the fans to run at full speed, which is done for unsupported PSU combinations. Conversely, the unsupported combination of AT-PWR150 and AT-PWR250DC will now cause the fans to run at full speed, which it didn't previously. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-81622	**IDS/IPS**	Previously, when under load with TCP connections starting and closing traffic, throughput may have been unstable or lowered due to the TCP segments staying in memory longer. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-79697	**IPv6** **CLI**	Previously, the command **`no ipv6 forwarding`** did not stop the device from routing IPv6 traffic. 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	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81618	**MAP-E**	Previously, under certain conditions, traffic being transmitted in a softwire tunnel would not be masqueraded correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-77098	**Multicast**	Previously, a memory leak could occur if a switch received packet fragments from unregistered multicast streams and was configured with the command: **`ip multicast allow-register-fragments`**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-79792	**Multicast**	Previously, it was possible in some circumstances for Layer 3 multicast routing to fail after repeated unicast route changes. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-81015	**NAT**	Previously, if a NAT port forwarding rule for FTP, including a port translation, was configured, the first connection to the FTP server from a client would work but subsequent connections could fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-81050	**NAT**	Previously, an unexpected reboot could occur when disabling NAT while the router was processing a large amount of UTM traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-80541	**PoE**	Previously, it was possible for stacked PoE switches under heavy load to encounter the following error "apteryxd: No response from provider for path "/poe/running". This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	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	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-80866	**Port Authentication**	Previously, when an Ethernet interface was configured to be protected by auth-web and the auth web server DHCP IP address was set, connecting a host to the eth port could cause a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-80698	**PPP**	Previously, if a remote PPP server required CHAP authentication but the final 'outcome' message from the server was lost, the PPP connection could hang. This meant it wouldn't fail and wouldn't fully establish. This issue has been resolved. Now, if the 'outcome' message is not received after 60 seconds, the PPP will behave as though the outcome was 'Failure'. The PPP will be brought down and restarted.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-80332	**SFP**	Previously, when a SFP+ port with a SP10Tm or SP10Ta module was oversubscribed, CRC errors were observed in the traffic received on the link partner. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-80930	**SMNP**	Previously, configuring an AlliedWare Plus device with users having names longer than 40 characters could lead to an unexpected system reboot when repeatedly performing SNMP walk on the AT private MIB tree. 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-81126	**SNMP** **PoE**	Previously, the **`snmp restart power-inline`** command wasn't executing correctly on the platforms which supported PoE. 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	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81438	**SNMP**	Previously, run snmp long walk might cause free memory decrease on the backup member of an x330 VCStack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-81449	**SSL, Encryption**	This software update addresses the OpenSSL vulnerability specified in: CVE-2023-5363. 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-81507	**STOAT**	Previously, there was STOAT information missing from tech-support. This issue has been resolved. With this software update, the STOAT information is now included in the tech-support. 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-80674	**System**	Previously, on occassion after a system reboot, the TQ6702 GEN2 Router could hang instead of rebooting. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-81269	**Traffic Control**	Previously, when shutting down or restarting it was possible for the traffic control daemon to fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-81012	**Triggers**	Previously, it was possible for Log Triggers to get into a state where further activations of the trigger would not occur. This issue could occur on any device with this feature, however it was more prevalent with vFW on the AT-NFVAPL/AT-VSTAPL. 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-81268	**Tunneling**	Previously, when shutting down or restarting it was possible for the tunnel daemon to fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81185	**UTM**	Previously, in the 5.5.3-1.x releases of vFW and AR-Cloud, instances using stream-based UTM features (IPS, Malware Protection, IP-Reputation, DPI, URL Filtering) could unexpectedly stop passing packets when experiencing heavy traffic load. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-81550	**VCStack**	Previously, following a VCStack failover, static IP routes may have been lost. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	Y	–	–	–	–	–	–
CR-80993	**VCStack, RADIUS**	Previously, on a VCStack, when setting up a connection to a RADIUS server using a domain name, the user interface could experience a 30-second lockup. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-81383	**VRRP**	Previously, when shutting down VRRPd, memory could be accessed after it was freed resulting in an unexpected system reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	Y

What's New in Version 5.5.3-1.3

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
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
AR1050V
TQ6702 GEN2-R

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-1.3.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 51.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 53. 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-5.5.3-1.3.iso (VAA OS) vaa-5.5.3-1.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-1.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2023	SBx81CFC960-5.5.3-1.3.rel
SBx908 GEN2	SBx908 GEN2	10/2023	SBx908NG-5.5.3-1.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	10/2023	x950-5.5.3-1.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	10/2023	x930-5.5.3-1.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2023	x550-5.5.3-1.3.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	10/2023	x530-5.5.3-1.3.rel
x330-10GTX x330-20GTX x330-28GTX	x330	10/2023	x330-5.5.3-1.3.rel
x320-10GH x320-11GPT	x320	10/2023	x320-5.5.3-1.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2023	x230-5.5.3-1.3.rel
x220-28GS x220-52GT x220-52GP	x220	10/2023	x220-5.5.3-1.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	10/2023	IE340-5.5.3-1.3.rel
IE220-6GHX IE220-10GHX	IE220	10/2023	IE220-5.5.3-1.3.rel
IE210L-10GP IE210L-18GP	IE210L	10/2023	IE210-5.5.3-1.3.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	10/2023	XS900-5.5.3-1.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	10/2023	GS980MX-5.5.3-1.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2023	GS980EM-5.5.3-1.3.rel
GS980M/52 GS980M/52PS	GS980M	10/2023	GS980M-5.5.3-1.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	10/2023	GS970EMX-5.5.3-1.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2023	GS970-5.5.3-1.3.rel
AR4000S-Cloud		10/2023	AR-4000S-Cloud-5.5.3-1.3.iso
10GbE UTM Firewall		10/2023	ATVSTAPL-1.8.3.iso and vfw-x86_64-5.5.3-1.3.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	10/2023	AR4050S-5.5.3-1.3.rel AR3050S-5.5.3-1.3.rel
AR1050 V	AR-series VPN routers	10/2023	AR1050V-5.5.3-1.3.rel
TQ6702 GEN2-R	Wireless AP Router	10/2023	TQ6702GEN2R-5.5.3-1.3.rel

Caution: Software version 5.5.3-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.3 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 47 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 49.

Unsupported devices

Version 5.5.3-1.x does not support:

- AR2050V VPN routers
- AR2010V VPN routers

The last version to support the above devices is 5.5.3-0.x.

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

The 5.5.3-1.3 software version is **not** ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.3-1.3

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	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
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	–
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	–	–	–	Y	–	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–
CR-72577	**Pluggable Transceivers**	Previously, under some circumstancwes, 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	–	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-79906	**Port Authentication**	Previously, with a surge of packets from many unauthorized supplicants, the port authentication process could take longer than expected to process. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–
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	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-79290	**Syslog, Bootup**	Previously, there was an internal issue with syslog, resulting in slow initialization. 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-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-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-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	–	–	–	–	–	–	–	–

What's New in Version 5.5.3-1.2

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
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
AR1050V
TQ6702 GEN2-R

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-1.2.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 51.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 53. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		09/2023	vaa-5.5.3-1.2.iso (VAA OS) vaa-5.5.3-1.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-1.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	09/2023	SBx81CFC960-5.5.3-1.2.rel
SBx908 GEN2	SBx908 GEN2	09/2023	SBx908NG-5.5.3-1.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	09/2023	x950-5.5.3-1.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	09/2023	x930-5.5.3-1.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	09/2023	x550-5.5.3-1.2.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	09/2023	x530-5.5.3-1.2.rel
x330-10GTX x330-20GTX x330-28GTX	x330	09/2023	x330-5.5.3-1.2.rel
x320-10GH x320-11GPT	x320	09/2023	x320-5.5.3-1.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	09/2023	x230-5.5.3-1.2.rel
x220-28GS x220-52GT x220-52GP	x220	09/2023	x220-5.5.3-1.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	09/2023	IE340-5.5.3-1.2.rel
IE220-6GHX IE220-10GHX	IE220	09/2023	IE220-5.5.3-1.2.rel
IE210L-10GP IE210L-18GP	IE210L	09/2023	IE210-5.5.3-1.2.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	09/2023	XS900-5.5.3-1.2.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	09/2023	GS980MX-5.5.3-1.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	09/2023	GS980EM-5.5.3-1.2.rel
GS980M/52 GS980M/52PS	GS980M	09/2023	GS980M-5.5.3-1.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	09/2023	GS970EMX-5.5.3-1.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	09/2023	GS970-5.5.3-1.2.rel
AR4000S-Cloud		09/2023	AR-4000S-Cloud-5.5.3-1.2.iso
10GbE UTM Firewall		09/2023	ATVSTAPL-1.8.3.iso and vfw-x86_64-5.5.3-1.2.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	09/2023	AR4050S-5.5.3-1.2.rel AR3050S-5.5.3-1.2.rel
AR1050 V	AR-series VPN routers	09/2023	AR1050V-5.5.3-1.2.rel
TQ6702 GEN2-R	Wireless AP Router	09/2023	TQ6702GEN2R-5.5.3-1.2.rel

Caution: Software version 5.5.3-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.3 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 47 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 49.

Unsupported devices

Version 5.5.3-1.x does not support:

- AR2050V VPN routers
- AR2010V VPN routers

The last version to support the above devices is 5.5.3-0.x.

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

The 5.5.3-1.2 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the enhancement available in 5.5.3-1.2:

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.

What's New in Version 5.5.3-1.1

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
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
AR1050V
TQ6702 GEN2-R

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-1.1.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 51.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 53. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		08/2023	vaa-5.5.3-1.1.iso (VAA OS) vaa-5.5.3-1.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-1.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	08/2023	SBx81CFC960-5.5.3-1.1.rel
SBx908 GEN2	SBx908 GEN2	08/2023	SBx908NG-5.5.3-1.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	08/2023	x950-5.5.3-1.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	08/2023	x930-5.5.3-1.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	08/2023	x550-5.5.3-1.1.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	08/2023	x530-5.5.3-1.1.rel
x330-10GTX x330-20GTX x330-28GTX	x330	08/2023	x330-5.5.3-1.1.rel
x320-10GH x320-11GPT	x320	08/2023	x320-5.5.3-1.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	08/2023	x230-5.5.3-1.1.rel
x220-28GS x220-52GT x220-52GP	x220	08/2023	x220-5.5.3-1.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	08/2023	IE340-5.5.3-1.1.rel
IE220-6GHX IE220-10GHX	IE220	08/2023	IE220-5.5.3-1.1.rel
IE210L-10GP IE210L-18GP	IE210L	08/2023	IE210-5.5.3-1.1.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	08/2023	XS900-5.5.3-1.1.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	08/2023	GS980MX-5.5.3-1.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	08/2023	GS980EM-5.5.3-1.1.rel
GS980M/52 GS980M/52PS	GS980M	08/2023	GS980M-5.5.3-1.1.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	08/2023	GS970EMX-5.5.3-1.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2023	GS970-5.5.3-1.1.rel
AR4000S-Cloud		08/2023	AR-4000S-Cloud-5.5.3-1.1.iso
10GbE UTM Firewall		08/2023	ATVSTAPL-1.8.3.iso and vfw-x86_64-5.5.3-1.1.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	08/2023	AR4050S-5.5.3-1.1.rel AR3050S-5.5.3-1.1.rel
AR1050 V	AR-series VPN routers	08/2023	AR1050V-5.5.3-1.1.rel
TQ6702 GEN2-R	Wireless AP Router	08/2023	TQ6702GEN2R-5.5.3-1.1.rel

Caution: Software version 5.5.3-1.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.3 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 47 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 49.

Unsupported devices

Version 5.5.3-1.x does not support:

- AR2050V VPN routers
- AR2010V VPN routers

The last version to support the above devices is 5.5.3-0.x.

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

The 5.5.3-1.1 software version is not ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.3-1.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 46.

Support for AMF Cloud and AMF Plus Cloud on more virtual environments

From version 5.5.3-1.1 onwards, AMF Cloud and AMF Plus Cloud can be deployed on:

- VMWare vSphere Hypervisor (ESXi) 8.0
- Nutanix AHV 6.5

For more information, see the AMF Cloud on Nutanix AHV Installation Guide.

Device Discovery using STOAT

Available on: Vista Manager EX and all AMF and AMF Plus capable products

From version 5.5.3-1.1 onwards, AlliedWare Plus devices support Device Discovery using STOAT (Standardized Topology Organizer and Transport). STOAT is a feature used to create an accurate overview of a customer's network topology. Devices are discovered using LLDP and DHCP Snooping protocols and information about the devices is organized into a standard format and transported to a central location for Vista Manager EX to extract and use to create a topology map. This feature will be available from Vista Manager EX version 3.11.0 onwards.

Prior to this version, Vista Manager EX created an integrated map using information from AMF and other plug-ins such as AWC and SNMP. Device Discovery using STOAT enhances the topology information present in the integrated map by providing Vista Manager EX with additional information about devices and the links between them.

Device Discovery using STOAT provides a more accurate representation of the network since it is not limited to only AMF devices

Enhancing network visibility with STOAT

STOAT devices actively record information about themselves, including details about the system/environment and their interfaces. These devices may include IP cameras, IP phones, PCs, laptops, Wi-Fi access points, printers, and so on. Additionally, Vista Manager EX merges any AMF and AMF Plus topology data with STOAT data, resulting in an enhanced and optimal view of the network.

Licensing

Device discovery using STOAT is part of the standard feature set of the device software, so there are no special licensing requirements.

New commands

You can configure STOAT using the following new commands:

```
awplus(config)# service stoat
awplus(config)# stoat dicovery
awplus(config)# stoat collector enable
awplus(config)# stoat collector key secretkey
awplus(config)# stoat destination
awplus(config-stoat-dest)# key
awplus(config)# stoat collector trustpoint
awplus(config)# stoat collector expiry-period
awplus(config)# show stoat collector
```

For more information, see the Device Discovery using STOAT Feature Overview and Configuration Guide.

Change for Advanced IPS rulesets

Applies to Advanced IPS on UTM firewalls

Version 5.5.3-1.1 onwards supports a new mechanism for users of Advanced IPS to receive updated rulesets. The previous mechanism has been discontinued, so users of Advanced IPS must upgrade their UTM firewalls to version 5.5.3-1.1 or later, to keep receiving updated rulesets.

Also, two new categories have been added to the IPS category list:

- **Phishing**: Signatures that detect credential phishing activity. This includes landing pages exhibiting credential phishing as well as successful submission of credentials into credential phishing sites.
- **Flowbits**: Signatures to match metadata to flows used by other IPS categories. Do not disable this category. If it is disabled, other IPS categories will not function correctly.

For more information about Advanced IPS, see the Advanced Network Protection Feature Overview and Configuration Guide.

Enhancements to AR1050V

From version 5.5.3-1.1 onwards, AR1050V supports:

- 1024 static routes
- Telnet server
- SSH server and client

For more information, see the following guides:

- Route Selection Feature Overview and Configuration Guide
- Secure Shell (SSH) Feature Overview and Configuration Guide

MAC Address Filter for Firewalls and VPN Routers

Applies to AR4000S-Cloud, 10GbE UTM Firewall, AR4050S, AR3050S, AR1050V

From version 5.5.3-1.1 onwards, these devices let you filter packets that come from specified hosts, by specifying the host's MAC address. Filtering by MAC address is useful if the host's IP address is allocated dynamically.

You can use this feature, for example, to increase security by preventing internal sensors from sending information out to the Internet.

There are two ways to configure this.

1. Specify a MAC address to discard

This is not available on AR4000S-Cloud or 10GbE UTM Firewalls

To have the firewall or router discard all traffic from a host, use the command:

```
awplus(config)# mac address-table static <mac-addr>
discard-src interface <port> [vlan <vid>]
```

If you do not specify a VLAN, it applies to VLAN 1.

2. Use the MAC address in firewall rules

First add the MAC address to an entity, using commands like these:

```
awplus(config)# zone example
awplus(config-zone)# network cameras
awplus(config-network)# host door
awplus(config-host)# mac-address 00:00:cd:11:22:33
```

Then block traffic from the entity to the Internet, using commands like these:

```
awplus(config)# firewall
awplus(config-firewall)# rule deny any from
example.cameras.door to inet
awplus(config-firewall)# protect
```

For more information, see the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

VRF support for PIM Source Specific Multicast (PIM-SSM)

Available on products that support PIM-SSM and VRF-lite: SBx8100, SBx908 GEN2, x950, x930, and x530 Series switches

From version 5.5.3-1.1 onwards, PIM-SSM VRF is supported. This means that VRF-lite capability is enabled for the **ip pim** commands relevant to SSM.

VRF-lite (Virtual Routing and Forwarding Lite) is a simple form of VRF. It allows multiple routing tables to co-exist within the same router/switch at the same time. Because the routing instances are independent, the same or overlapping IP address space can be used without conflicting with each other.

Command changes

These commands now all support VRF:

```
ip pim [vrf <name>] ssm default
ip pim [vrf <name>] ssm range {<acl>|<named-acl>}
no ip pim [vrf <name>] ssm
```

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

VRF support for IPv6

Available on: AlliedWare Plus devices that support VRF-lite

From software version 5.5.3-1.1 onwards, AlliedWare Plus supports VRFs with IPv6 unicast. Earlier AlliedWare Plus versions support VRFs with IPv4.

The following features are affected:

Ping, Traceroute, and SSH client

- Ping supports specification of a VRF in combination with an IPv6 address or a hostname resolving to an IPv6 address.
- Traceroute supports specification of a VRF in combination with an IPv6 address or a hostname resolving to an IPv6 address.
- SSH client supports specification of a VRF in combination with an IPv6 address or a hostname resolving to an IPv6 address.

IPv6

Now supports:

- In-hardware routing of IPv6 VRF traffic on switch platforms.
- In-CPU routing of IPv6 VRF traffic on router platforms.
- Static routing with VRF.
- Neighbor Discovery on interfaces assigned to a VRF.
- Router Advertisements on interfaces assigned to a VRF.
- SLAAC on interfaces assigned to a VRF.

DNS Now supports:

- Specifying a VRF in combination with an IPv6 address with the command **ip name-server**.
- DNS Relay queries via IPv6 in combination with a VRF.

DHCP Now supports:

- DHCPv6 Client on interfaces assigned to a VRF.

BGP Now supports:

- VRF with IPv6.

BFD Now supports:

- VRF with IPv6.
- Static routes with VRF and IPv6.
- BGP with VRF and IPv6.

sFlow Now supports:

- sFlow Agent - specification of a VRF in combination with an IPv6 collector address.

New commands

This software release introduces the following new commands.

```
ipv6 route vrf
ipv6 route bfd
ipv6 route bfd all-interfaces
show bgp ipv6 vrf
show bgp ipv6 vrf community
show bgp ipv6 vrf community-list
show bgp ipv6 vrf longer-prefixes
show bgp ipv6 vrf regexp
show bgp ipv6 vrf filter-list
show bgp ipv6 vrf neighbors routes
show bgp ipv6 vrf dampening
address-family ipv6 vrf
```

Updated commands

Syntax changed to use either disable or profile option but not both together:

```
ip route bfd [disable | profile <profilename>]
ip route <subnet&mask> <gateway-ip> fall-over bfd [disable |
profile <profilename> ]
```

Adds BFD session support to IPv6 static routes:

```
ipv6 route <dest-prefix/length> fall-over bfd [disable |
profile <profilename> ]
```

Adds BFD fall-over support to a BGP IPv6 neighbor under VRF:

```
neighbor {<ip-address>|<ipv6-address>|<peer-group>} fall-over
bfd [multihop] [profile <profilename>]
```

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

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

Support for Private VLAN UFO on More Switches

Added to SBx908 GEN2, x950, x550, x320, x230, x230L, and x220 Series switches. Previously available on SBx8100, x930, x530, x530L, x330, IE340, IE340L, IE220, and IE210L Series switches.

From version 5.5.3-1.1 onwards, the list of switches above support Upstream Forwarding Only (UFO) on private VLANs. UFO lets you restrict selected Ethernet hosts so that they can only communicate with designated upstream devices. It does this by blocking forwarding of Ethernet frames amongst designated VLAN member ports.

For more information about UFO, see the Virtual LANs (VLANs) Feature Overview and Configuration Guide.

Support for Precision Time Protocol Transparent Clock on More Switches

Added to SBx908 GEN2 (standalone only), x950 (standalone only), and x530L (both standalone and VCStack configurations) Series switches. Previously available on x930, x550, x230, x230L, IE340, IE340L, and IE210L Series switches.

From version 5.5.3-1.1 onwards, SBx908 GEN2, x950, and x530L Series switches support Transparent Clock for Precision Time Protocol (PTP). PTP is an Ethernet or IP-based protocol for synchronizing time clocks on a collection of network devices. The transparent clock computes the variable delay as the PTP packets pass through the switch or the router.

For SBx908 GEN2 and x950 Series switches, transparent clock is only available when the switch is a standalone unit, not when it is stacked.

For more information, see the Precision Time Protocol (PTP) and Transparent Clock Feature Overview and Configuration Guide.

Improvements to multicast recovery time when VCStacks failover

Added to SBx8100, SBx908 GEN2, x950, x930, x550, x530, x530L, x330, XS900MX, GS980MX, and GS970EMX Series switches.

From version 5.5.3-1.1 onwards, multicast traffic will recover more quickly if a VCStack master switch fails and the backup switch takes over.

For more information about VCStack, see the Virtual Chassis Stacking Feature Overview and Configuration Guide. For more information about multicast, see:

- Protocol Independent Multicast - Sparse Mode (PIM-SM) Feature Overview and Configuration Guide
- PIM-DM Feature Overview and Configuration Guide
- PIM Sparse Mode for IPv6 (PIM-SMv6) Feature Overview and Configuration Guide

Trigger for PoE PSE related events

Applies to all devices that support PoE

From version 5.5.3-1.1 onwards, two new trigger types have been added for PoE related events:

- **main-pse** - this monitors the switch's total PoE power budget. It activates if the total amount of power being drawn exceeds the switch's power budget.
- **pse-port** - this monitors individual ports. It activates if the amount of power being drawn by a port exceeds the capabilities of the port.

You can also activate these trigger types when the amount of power drops to within the limit again. Note that the switch will take corrective action when the power budget or port limit is exceeded, such as shutting down the affected port. This means the amount of power will drop soon after the fault occurs.

To create a trigger that monitors the total PoE power budget, use the command:

```
awplus(config-trigger)# type main-pse {up|down|any}
```

On switches that are in a VCStack, that trigger will activate if any stack member meets its conditions. You can monitor a specific stack member by using the command:

```
awplus(config-trigger)# type main-pse member <id> {up|down|
any}
```

To create a trigger that monitors a particular port, use the command:

```
awplus(config-trigger)# type pse-port <port-number> {up|down|
any}
```

In all of these commands:

- **up** means the trigger activates when the power becomes too high
- **down** means the trigger activates when the power drops low enough again
- **any** means it activates both times - when the power becomes too high and when it drops low enough again.

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

More ciphersuites supported by TLSv1.3

Applies to all AlliedWare Plus devices

From version 5.5.3-1.1 onwards, TLSv1.3 on AlliedWare Plus supports more ciphersuites, including:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

Note that the supported minimum TLS version is 1.2 in AlliedWare Plus. TLS versions 1.0 and 1.1 have been deprecated.

802.1X retransmission mechanism

Applies to all devices that support 802.1X

From version 5.5.3-1.1 onwards, AlliedWare Plus supports a retransmission mechanism for 802.1X. If an EAP Request packet is lost between the authenticating device and the supplicant, the authenticator now resends the EAP Request packet. Previously, if the supplicant did not respond on an EAP Request within the supplicant timeout period, the authenticator would treat the authentication process as a failure.

With this enhancement, the authenticator resends the EAP request packet up to a specified maximum number of times. If the supplicant has not responded after the maximum number of retransmissions is reached, then the supplicant fails the authentication process.

The default number of retransmissions is 2. This means by default, the authenticator sends the original attempt and 2 more attempts, which is 3 attempts in total. To change the maximum number of retransmissions for one or more switch ports, use the following new command in Interface mode:

```
awplus(config-if)# dot1x max-req <1-10>
```

You can also apply the maximum number of transmissions to only a particular supplicant on the specified port or ports, using one of the following commands:

```
awplus(config-if)# auth supplicant-mac <mac-addr> max-req
<1-10>
awplus(config-if)# auth supplicant-ip <ip-addr> max-req <1-10>
```

For more information about 802.1X, see the AAA and Port Authentication Feature Overview and Configuration Guide.

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.3-1.x and may affect your device or network behavior if you upgrade:

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

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

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

Please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.2-2.x version, please check the 5.5.3-0.x release note. Release notes are available from our website, including:

- 5.5.3-0.x release notes
- 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 40 and "Details for x930 Series" on page 41 for details.

Affected Products

The following models could be affected:

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

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

Recovering from upgrading from an incompatible version

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

Details for SBx908 GEN2 and x950 Series

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

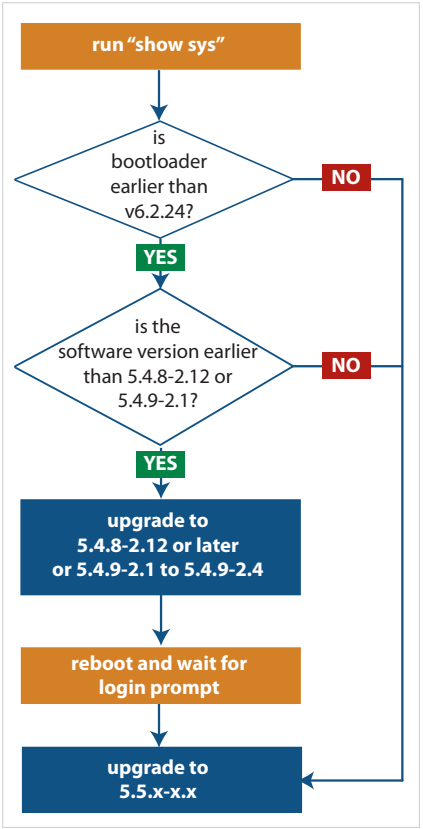
- 5.4.9-1.x
- 5.4.9-0.x
- any version before 5.4.8-2.12.

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

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

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

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

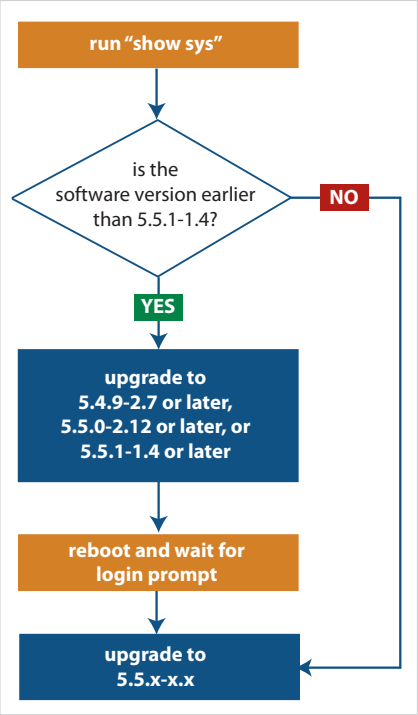



```
awplus# show system
```

Details for x930 Series

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

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



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

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

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

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

```
awplus# show system
```

Changes that may affect device or network configuration

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

Summary	Affected devices	Detail
Disable strict user process control before returning a product to a factory default state	All AlliedWare Plus devices	From 5.5.3-1.1 onwards, you cannot run the commands **atmf cleanup** or **erase factory-default** when strict user process control is enabled. You must disable strict user process control first, using the command **no strict-user-process-control**.
Diffie-Hellman based cipher suites have been disabled	All AlliedWare Plus devices	From 5.5.3-1.1 onwards, to improve the security of communication between browsers and the HTTP service within the AlliedWare Plus devices, all Diffie-Hellman based cipher suites have been disabled. Older browsers that support only Diffie-Hellman based cipher suites will no longer be able to communicate with AlliedWare Plus devices via HTTP. If you are affected by this, please use a newer browser.

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 47 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 49.

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
AMF Cloud	vaa-5.5.3-1.4.rel	f6bf1b827f7723cc4cd857b5cb558941745541ada15c765999dc94152022844b
SBx8100	SBx81CFC960-5.5.3-1.4.rel	db95ebc5e585c423207b3493540eee1550aabd2e370ca3a34739b3177ca150a9
SBx908 GEN2	SBx908NG-5.5.3-1.4.rel	4b43668477111e4226978aa41fa564d97a745e7c8eacd24525be3cd3b39edaf6
x950	x950-5.5.3-1.4.rel	4b43668477111e4226978aa41fa564d97a745e7c8eacd24525be3cd3b39edaf6
x930	x930-5.5.3-1.4.rel	284600671ebc93fae5b11e63feed006e446a408b0eb707b64ec72269ade0316e
x550	x550-5.5.3-1.4.rel	77df609433a7ff7ed4f399b1b93c46bb0cec15eac31284ca4cfcb693a21cda28
x530 & x530L	x530-5.5.3-1.4.rel	7c8ba310800270ea2b454e8ebae5c8eac5b3c6de4af14d84fe1bcd710161b600
x330	x330-5.5.3-1.4.rel	cd8b652d0203dc6677fd16d02bd542840699e3273622a81a354d69153b83aee3

Table: Hash values

Product family	Software File	Hash
x320	x320-5.5.3-1.4.rel	7c8ba310800270ea2b454e8ebae5c8eac5b3c6de4af14d84fe1bcd710161b600
x230 & x230L	x230-5.5.3-1.4.rel	fc0e5fa606a43ede924fd3880e8c0f8bbe50b45b8784c59ed893b249e620bff2
x220	x220-5.5.3-1.4.rel	fc0e5fa606a43ede924fd3880e8c0f8bbe50b45b8784c59ed893b249e620bff2
IE340 & IE340L	IE340-5.5.3-1.4.rel	537f8d3ca67c94880a10e51c3c226947e8eff065a8f45162219ef4bd46fd1ed1
IE220	IE220-5.5.3-1.4.rel	74987bd52700e344a607ccaa1ee9f0216fa47f75b9aef25dfb6cbedd252a8e95
IE210L	IE210-5.5.3-1.4.rel	b147beaf4c422028368a242f8015d8aac4955a46499b45e7183b7e441cab70f2
XS900MX	XS900-5.5.3-1.4.rel	7249d452cb4c7028b98b65e1d260b851e2ab5e6e256428b6ae45f588f08bb13e
GS980MX	GS980MX-5.5.3-1.4.rel	7c8ba310800270ea2b454e8ebae5c8eac5b3c6de4af14d84fe1bcd710161b600
GS980EM	GS980EM-5.5.3-1.4.rel	7c8ba310800270ea2b454e8ebae5c8eac5b3c6de4af14d84fe1bcd710161b600
GS980M	GS980M-5.5.3-1.4.rel	fc0e5fa606a43ede924fd3880e8c0f8bbe50b45b8784c59ed893b249e620bff2
GS970EMX	GS970EMX-5.5.3-1.4.rel	cd8b652d0203dc6677fd16d02bd542840699e3273622a81a354d69153b83aee3
GS970M	GS970-5.5.3-1.4.rel	b147beaf4c422028368a242f8015d8aac4955a46499b45e7183b7e441cab70f2
AR4050S-5G	AR4050S-5.5.3-1.4.rel	d2da08db3b903a4c9070619900c2759cb805551f5f531c5ac9d203f7ffcaa7fc
AR4050S	AR4050S-5.5.3-1.4.rel	d2da08db3b903a4c9070619900c2759cb805551f5f531c5ac9d203f7ffcaa7fc
AR3050S	AR3050S-5.5.3-1.4.rel	d2da08db3b903a4c9070619900c2759cb805551f5f531c5ac9d203f7ffcaa7fc
AR1050V	AR1050V-5.5.3-1.4.rel	32f04a7a434dcb48739794b1fe78121a55ad974edaab4eb0eeca0bf430c7c88b
TQ6702 GEN2-R	TQ6702GEN2R-5.5.3-1.4.rel	7afd32b7afe5fb9f776d2245a570cdff14d7a0b2374f5b2cedf4f41de7364ce7

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 47 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 49.

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 SBx8100-5.5.3-1.4.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.3-1.4.rel`
x950 series	`awplus(config)# boot system x950-5.5.3-1.4.rel`
x930 series	`awplus(config)# boot system x930-5.5.3-1.4.rel`
x550 series	`awplus(config)# boot system x550-5.5.3-1.4.rel`
x530 series	`awplus(config)# boot system x530-5.5.3-1.4.rel`
x330 series	`awplus(config)# boot system x330-5.5.3-1.4.rel`
x320 series	`awplus(config)# boot system x320-5.5.3-1.4.rel`
x230 series	`awplus(config)# boot system x230-5.5.3-1.4.rel`
x220 series	`awplus(config)# boot system x220-5.5.3-1.4.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.3-1.4.rel`
IE220 series	`awplus(config)#boot system IE220-5.5.3-1.4.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.3-1.4.rel`

Product	Command
XS900MX series	`awplus(config)# boot system XS900-5.5.3-1.4.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.3-1.4.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.3-1.4.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.3-1.4.rel`
GS970EMX series	`awplus(config)# boot system GS970EMX-5.5.3-1.4.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.3-1.4.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.3-1.4.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.3-1.4.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.3-1.4.rel`
AR1050V	`awplus(config)4# boot system AR1050V-5.5.3-1.4.rel`
TQ6702 GEN2-R	`awplus(config)# boot system TQ6702GEN2R-5.5.3-1.4.rel`

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

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

6. Reboot using the new software version.

```
awplus# reload
```

Accessing and Updating the Web-based GUI

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

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

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

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

Browse to the GUI

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

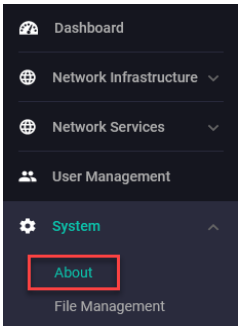
2. Open a web browser and browse to the IP address from step 1.

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 5.5.3-1.4 is 2.15.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 54 or "Update the GUI on AR-Series devices" on page 55.



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 v5.5.3-1.x is awplus-gui_553_30.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:

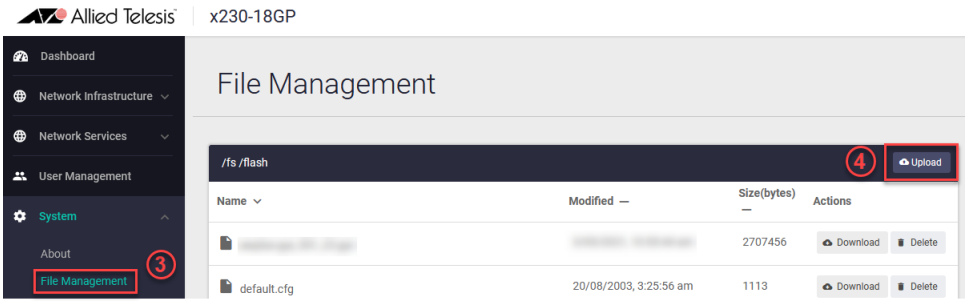
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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.