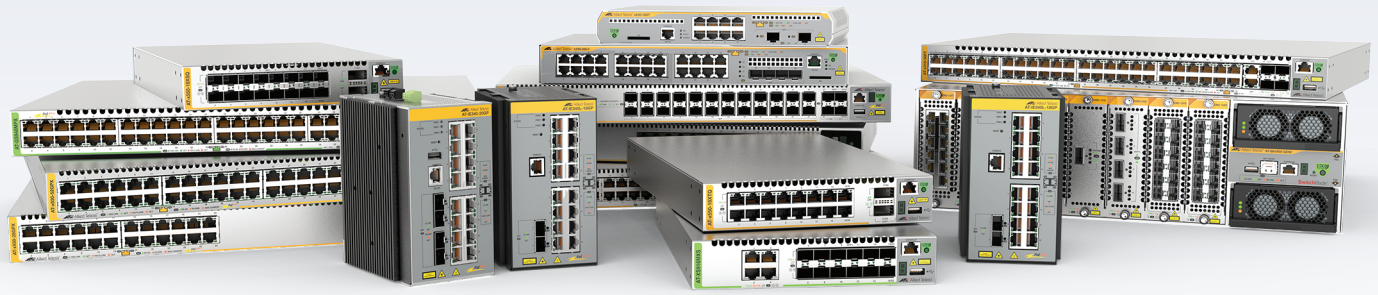
Release Note for AlliedWare Plus Software Version 5.5.2-0.x



AlliedWare Plus OPERATING SYSTEM

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

» 5.5.2-0.1 » 5.5.2-0.2 » 5.5.2-0.3

Acknowledgments

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

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

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

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

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

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

Getting the most from this Release Note

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

Contents

What's New in Version 5.5.2-0.3 1

Introduction 1

Enhancements in Version 5.5.2-0.3 5

Issues Resolved in Version 5.5.2-0.3 6

What's New in Version 5.5.2-0.2 12

Introduction 12

Enhancements in Version 5.5.2-0.2 16

Issues Resolved in Version 5.5.2-0.2 17

What's New in Version 5.5.2-0.1 22

Introduction 22

New Features and Enhancements 25

Important Considerations Before Upgrading 39

Obtaining User Documentation 47

Verifying the Release File 47

Licensing this Version on an SBx908 GEN2 Switch 48

Licensing this Version on an SBx8100 Series CFC960 Control Card 50

Installing this Software Version 52

Accessing and Updating the Web-based GUI 54

What's New in Version 5.5.2-0.3

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-0.3.

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 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		07/2022	vaa-5.5.2-0.3.iso (VAA OS) vaa-5.5.2-0.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-0.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	07/2022	SBx81CFC960-5.5.2-0.3.rel
SBx908 GEN2	SBx908 GEN2	07/2022	SBx908NG-5.5.2-0.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	07/2022	x950-5.5.2-0.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	07/2022	x930-5.5.2-0.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2022	x550-5.5.2-0.3.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	07/2022	x530-5.5.2-0.3.rel
x330-10GTX	x330	07/2022	x330-5.5.2-0.3.rel
x320-10GH x320-11GPT	x320	07/2022	x320-5.5.2-0.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2022	x230-5.5.2-0.3.rel
x220-28GS x220-52GT x220-52GP	x220	07/2022	x220-5.5.2-0.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	07/2022	IE340-5.5.2-0.3.rel
IE210L-10GP IE210L-18GP	IE210L	07/2022	IE210-5.5.2-0.3.rel
XS916MXT XS916MXS	XS900MX	07/2022	XS900-5.5.2-0.3.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	07/2022	GS980MX-5.5.2-0.3.rel

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

Models	Family	Date	Software File
GS980EM/10H GS980EM/11PT	GS980EM	07/2022	GS980EM-5.5.2-0.3.rel
GS980M/52 GS980M/52PS	GS980M	07/2022	GS980M-5.5.2-0.3.rel
GS970EMX/10	GS970EMX	07/2022	GS970EMX-5.5.2-0.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2022	GS970-5.5.2-0.3.rel
10G Virtual UTM Firewall		07/2022	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.2-0.3.app
AR4050S-5G	5G mobile broadband UTM firewall	07/2022	AR4050S-5.5.2-0.3.rel
AR4050S AR3050S	AR-series UTM firewalls	07/2022	AR4050S-5.5.2-0.3.rel AR3050S-5.5.2-0.3.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	07/2022	AR2050V-5.5.2-0.3.rel AR2010V-5.5.2-0.3.rel AR1050V-5.5.2-0.3.rel

Caution: Software version 5.5.2-0.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 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-0.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 47 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 49.

Unsupported devices

Version 5.5.2-0.x does not support:

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

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

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

The 5.5.2-0.3 software version is ISSU compatible with software version 5.5.2-0.1.

Enhancements in Version 5.5.2-0.3

This AlliedWare Plus maintenance version includes the following enhancements:

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	AMF Cloud
ER-4813	**User Management**	Update to the method used for hashing passwords Available on all AlliedWare Plus devices AlliedWare Plus devices store user passwords in configuration files in hashed form. From 5.5.2-0.3 onwards, the hash method for these passwords has been upgraded. 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-76571	**AWC Lite**	With this software update , it is now possible for tech support files to be stored to USB from devices that support AWC Lite.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	–	–	Y	Y	–

Issues Resolved in Version 5.5.2-0.3

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

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	AMF Cloud
CR-76820	**ACL, API**	Previously, ACL API could return incorrect information with IPv6 host groups. 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-76950	**ACL, API, Link Aggregation**	Previously, API could incorrectly add an ACL filter if **`send-to-vlan-port`** was an aggregator. 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-77077	**AMF**	Previously, the traffic for a node reachable via an AMF virtual link would not be passed through the virtual link as intended. 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-77080	**Authentication**	This software update addresses the Linux kernel vulnerabilities specified in the following CVEs: CVE-2022-22576, CVE-2022-27774, CVE-2022-27776, CVE-2022-27782, CVE-2022-27781, CVE-2022-27775, CVE-2022-27780, CVE-2022-27779, CVE-2022-30115. 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-76761	**AWC Lite**	Previously, the Passpoint security could not be used when 3gpp-info was not set. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	AMF Cloud
CR-76988	**AWC Lite**	Previously, when deleting an AP-profile that was using a channel blanket, the BSSID information that was being used would not be removed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	–
CR-77265	**AWC Lite**	Previously, the AP tech-support file could attempt to be stored to USB media, which was already removed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	–
CR-76951	**Boot**	Previously, on x330 Series, occassionally, external media would not be detected and autoboot configuration would be missed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-76595	**Cellular Modem**	Previously, deleting a modem's firmware could sometimes cause the modem to stop responding. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-76690	**Cellular Modem**	Previously, on rare occacions, the 5G modem would not operate correctly on startup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-72234	**Device Security**	Prior to this update it was possible to access internal Critical Security Parameter information. 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-76910	**LACP, SNMP**	Previously, a storm could occur when using multiple stack resiliency links that formed a loop. This was observed when **`no ip igmp snooping`** was configured. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	Y	–	Y	–	Y	Y	–	–	–	Y	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	AMF Cloud
CR-58712	**Logging**	Previously, if a terminal console timeout occured while the terminal monitor was enabled, it could cause the syslog process to restart abnormally. 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-76838	**Logging**	Previously, it was possible for the syslog process to restart abnormally. 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-77076	**Loop protection, VCStack**	Previously, if a stack member joined the stack as a late-joiner, the member's loop-protection configuration would not be present in the running-config. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	Y	–	Y	–	Y	Y	–	–	–	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-76364	**MRP**	Previously, ports were prematurely removed from STP before the MRP ring was complete and enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-76775	**OSPFv2**	Previously, it was not possible to configure the maximum number of ECMP routes. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-76984	**OSPFv2**	Previously, syncing OSPF Database Description packets could write values to unknown parts of memory. This could have potentially caused some random OSPF issues. 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-76909	**sFlow**	Previously, sflow sampled packets could be incorrectly forwarded. 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	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	AMF Cloud
CR-76063	**SSL**	This software update addresses the SSL security vulnerabilities specified in CVE-2022-1292 and CVE-2021-4160. 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-77060	**Switching**	Previously, using the SP10TM module at 2.5Gbps could result in a small amount of frame loss. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-76819	**System**	Previously, memory exhaustion could occur when processing some packets. 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-76907	**System**	This software update addresses the linux kernel vulnerability specified in CVE-2022-1353. 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-76929	**System**	This software update addresses the linux kernel vulnerability specified in CVE-2022-0847. 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-77010	**System**	This software update addresses the linux kernel vulnerability specified in CVE-2022-30594. 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-77012	**System**	This software update addresses the linux kernel vulnerability specified in CVE-2022-29581. 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-77100	**System**	This software update addresses the linux kernel vulnerability specified in CVE-2022-32250. 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	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AR4050S-5G	AMF Cloud
CR-77262	**USB Modem**	Previously, re-initialising the 5G modem WWAN interface would not remove the former DNS and route information. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-66523	**VCStack**	Previously, on the x530 Series, when ports were linked up using a DAC cable, it was possible for link flapping to occur. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-76264	**VCStack**	Previously, x330 Series stack ports using fibre SFP+ pluggables could sometimes fail to link up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-76299	**VCStack**	Previously, after a stack master failover went through a power cycle, it could occssionally fail to rejoin the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	Y	Y	–	–	–	–	Y	–	Y	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-76658	**VCStack**	Previously, after stack failover, a new master might cause traffic to not be forwarded correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–
CR-76872	**VCStack**	Previously, it was possible for the stack ports using 10G DAC cables to not linkup on the x530 Series. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-76933	**VCStack**	Previously, when a stack member with incompatible software attempted to join a stack, it could cause one of the existing stack members to restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	–	Y	Y	–	–	–	Y	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-76237	**VXLAN**	Previously, ECMP routes could cause traffic loss via VXLAN tunnels. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	Y	–	–	–	–	–	–

What's New in Version 5.5.2-0.2

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-0.2.

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 52.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 54. 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		06/2022	vaa-5.5.2-0.2.iso (VAA OS) vaa-5.5.2-0.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-0.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	06/2022	SBx81CFC960-5.5.2-0.2.rel
SBx908 GEN2	SBx908 GEN2	06/2022	SBx908NG-5.5.2-0.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	06/2022	x950-5.5.2-0.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	06/2022	x930-5.5.2-0.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2022	x550-5.5.2-0.2.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	06/2022	x530-5.5.2-0.2.rel
x330-10GTX	x330	06/2022	x330-5.5.2-0.2.rel
x320-10GH x320-11GPT	x320	06/2022	x320-5.5.2-0.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	06/2022	x230-5.5.2-0.2.rel
x220-28GS x220-52GT x220-52GP	x220	06/2022	x220-5.5.2-0.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	06/2022	IE340-5.5.2-0.2.rel
IE210L-10GP IE210L-18GP	IE210L	06/2022	IE210-5.5.2-0.2.rel
XS916MXT XS916MXS	XS900MX	06/2022	XS900-5.5.2-0.2.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	06/2022	GS980MX-5.5.2-0.2.rel

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

Models	Family	Date	Software File
GS980EM/10H GS980EM/11PT	GS980EM	06/2022	GS980EM-5.5.2-0.2.rel
GS980M/52 GS980M/52PS	GS980M	06/2022	GS980M-5.5.2-0.2.rel
GS970EMX/10	GS970EMX	06/2022	GS970EMX-5.5.2-0.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2022	GS970-5.5.2-0.2.rel
10G Virtual UTM Firewall		06/2022	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.2-0.2.app
AR4050S AR3050S	AR-series UTM firewalls	06/2022	AR4050S-5.5.2-0.2.rel AR3050S-5.5.2-0.2.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	06/2022	AR2050V-5.5.2-0.2.rel AR2010V-5.5.2-0.2.rel AR1050V-5.5.2-0.2.rel

Caution: Software version 5.5.2-0.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 5.5.2 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-0.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 48 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 50.

Unsupported devices

Version 5.5.2-0.x does not support:

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

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

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

The 5.5.2-0.2 software version is ISSU compatible with software version 5.5.2-0.1.

Enhancements in Version 5.5.2-0.2

This AlliedWare Plus maintenance version includes the following enhancement:

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-3282	**OSFPv2**	**Enhancement:** With this software update, OSPFv2 on routers now supports the **`distribute-list route-map <route-map-name> in`** command that was previously only available on Layer 3 switches. Also previously, in route-map configuration mode, the command **`no match interface [<interface>]`** could fail after initial system configuration load. These issues have been resolved. ISSU: CFCs Upgraded	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

Issues Resolved in Version 5.5.2-0.2

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

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM/	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75756	**AMF Cloud** **Virtual FW**	Previously, a configuration containing dot1q sub-interfaces might fail to correctly setup these interfaces following a reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-76458	**ACL**	Previously, executing the command **`show tech support`** might cause a device that had dynamic ACLs configured to restart. 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	–	–	–	–	–
CR-75908	**Aggregation - Static** **VCStack**	Previously, deleting a static aggregator could cause a stack break. This issue has been resolved.	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-60591	**EPSR**	Previously, there was a potential delay processing the link down event upon topology changes on an EPSR ring, resulting in slower EPSR convergence. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-76808	**Loop Protection**	Previously, when the **clear loop-protection counters** command was used, the VLAN information could be incorrectly cleared. 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-75041	**OSPFv2**	Previously, in networks where routing destinations were learned by both OSPF and BGP, significant topology changes in the network might cause OSPF and BGP events to become out of synchronisation, resulting in route mismatches. 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	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM/	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75712	**PoE**	Previously, PoE devices sometimes were not powered. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-76604	**Port Authentication** **ACL**	Previously, the output from the command: **`show access-list counters`** was incorrect when dynamic ACLs were enabled 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	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR-76621	**Port Authentication** **ACL**	Previously, the dynamic ACL could still be applied even after the supplicant had become unauthenticated. 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-75690	**Port Authentication**	Previously, when using Auth-web, it was possible to cause a system reboot if the HTTP headers were too large when accessing the login web page. With this software update, the supported size has been increased, and rather than causing a system reboot it will return an appropriate HTTP error code. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM/	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-75829	**Port Authentication**	Previously, when replacing a supplicant that was already authenticated via web authentication with a new device of the same IP address, it was possible for the device not to be authenticated. This issue has been resolved. Also, with this software update, a configuration option has been provided for web authentication such that if a new supplicant attempting to connect detects a conflicting (already existing) supplicant with the same IP address, you can configure such that it is the existing supplicant that is logged off to allow the new supplicant to connect. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76741	**QoS**	Previously, the command **`wrr-queue queue-limit`** would not work correctly when an identical set of queue weightings were applied to physical ports belonging to different switch instances (generally ports 1-24, 51-52 and ports 25-50 belong to different instances). This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-75757	**SNMP**	Previously, the SNMP discovery service was on by default even if it was not enabled, resulting in excessive logs. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-76582	**SNMP**	Previously, accessing the temperature sensors of the SBx8100 DC PSU via SNMP could result in a system restart. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM/	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76429	**System**	This software update addresses security vulnerability issues as specified in CVE-2022-0617. 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-76432	**System**	This software update addresses security vulnerability issues as specified in CVE-2021-20322. 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-76591	**System**	This software update addresses security vulnerability issues as specified in CVE-2020-36516. 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-76592	**System**	This software update addresses security vulnerability issues as specified in CVE-2021-3744. 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-76721	**System**	This software update addresses security vulnerability issues as specified in CVE-2021-3732. 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-76733	**System**	This software update addresses security vulnerability issues as specified in CVE-2022-1011. 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-76735	**System**	This software update addresses security vulnerability issues as specified in CVE-2021-4203. 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-76736	**System**	This software update addresses security vulnerability issues as specified in CVE-2021-4157. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	Y	Y	Y	–	Y	–	Y	–	Y	Y	–	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M/EMX	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM/	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-76737	**System**	This software update addresses security vulnerability issues as specified in CVE-2021-4197. 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-76779	**System**	This software update addresses security vulnerability issues as specified in CVE-2022-1055. 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-76816	**System**	This software update addresses security vulnerability issues as specified in CVE-2022-28391. 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-76209	**VCStack**	Previously, audit inconsistency errors could be logged immediately after a stack failover event caused by a disabled master in networks where LACP was configured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	Y	–	Y	Y	–	–	–	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-76722	**VCStack**	Previously, under rare circumstances, some stack links could link up incorrectly at startup, resulting in the stack not forming. This issue has been resolved.	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–
CR-75944	**VCStack** **ICMP**	Previously, when a member joined a stack that was already operating, some Layer 3 settings were not correctly synced to the new stack member. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	Y	–	–	–	–	–	–
CR-76725	**VLAN**	Previously, the MTU setting was not working correctly on the x330 Series. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–

What's New in Version 5.5.2-0.1

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

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.2-0.1.

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 52.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 54. 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		03/2022	vaa-5.5.2-0.1.iso (VAA OS) vaa-5.5.2-0.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.2-0.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	03/2022	SBx81CFC960-5.5.2-0.1.rel
SBx908 GEN2	SBx908 GEN2	03/2022	SBx908NG-5.5.2-0.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	03/2022	x950-5.5.2-0.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	03/2022	x930-5.5.2-0.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2022	x550-5.5.2-0.1.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	03/2022	x530-5.5.2-0.1.rel
x330-10GTX	x330	03/2022	x330-5.5.2-0.1.rel
x320-10GH x320-11GPT	x320	03/2022	x320-5.5.2-0.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	03/2022	x230-5.5.2-0.1.rel
x220-28GS x220-52GT x220-52GP	x220	03/2022	x220-5.5.2-0.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2022	IE340-5.5.2-0.1.rel
IE210L-10GP IE210L-18GP	IE210L	03/2022	IE210-5.5.2-0.1.rel
XS916MXT XS916MXS	XS900MX	03/2022	XS900-5.5.2-0.1.rel
GS980MX/10HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	03/2022	GS980MX-5.5.2-0.1.rel

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

Models	Family	Date	Software File
GS980EM/10H GS980EM/11PT	GS980EM	03/2022	GS980EM-5.5.2-0.1.rel
GS980M/52 GS980M/52PS	GS980M	03/2022	GS980M-5.5.2-0.1.rel
GS970EMX/10	GS970EMX	03/2022	GS970EMX-5.5.2-0.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	03/2022	GS970-5.5.2-0.1.rel
10G Virtual UTM Firewall		03/2022	ATVSTAPL-1.5.1.iso and vfw-x86_64-5.5.2-0.1.app
AR4050S AR3050S	AR-series UTM firewalls	03/2022	AR4050S-5.5.2-0.1.rel AR3050S-5.5.2-0.1.rel
AR2050V AR2010V AR1050 V	AR-series VPN routers	03/2022	AR2050V-5.5.2-0.1.rel AR2010V-5.5.2-0.1.rel AR1050V-5.5.2-0.1.rel

Caution: Software version 5.5.2-0.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 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.2 license installed, that license also covers all later 5.5.2 versions, including 5.5.2-0.x. Such switches do not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 48 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 50.

Unsupported devices

Version 5.5.2-0.x does not support:

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

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

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

The 5.5.2-0.1 software version is not ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.2-0.1:

- "Specify remote end of AMF virtual link by hostname" on page 26
- "AMF auto-recovery can replace some device series with similar devices" on page 26
- "Bi-directional Forwarding Detection (BFD)" on page 27
- "Enhanced DPI Web-categorization" on page 27
- "Support for TLS Crypt on OpenVPN" on page 28
- "Virtual UTM Firewall licensing made easier" on page 28
- "A long-press on the reset button now deletes the configuration file" on page 29
- "Port Authentication support for dynamic multiple VLAN assignment" on page 29
- "Port Based DHCP IP Address Assignment" on page 30
- "Improvement to "show stack detail"" on page 31
- "License no longer required for Media Redundancy Protocol (MRP) clients" on page 32
- "Enabling DHCP Snooping on individual VLANs" on page 32
- "Information about timed-out loop-detection packets for loop protection" on page 32
- "Removal of obsolete parameters from the SSH protocol" on page 33
- "Option to drop ICMP timestamp requests and responses" on page 34
- "Option to disable TCP timestamp responses" on page 34
- "Removal of a vulnerable MAC algorithm from secure algorithm list" on page 35
- "Prevention of ARP (foreign host route) poisoning" on page 35
- "Support for TQ6602 GEN2 and TQm6602 GEN2 APs in Vista Manager mini" on page 36
- "Obtain Access Point tech-support files via Vista Manager mini" on page 36
- "Passpoint (Hotspot 2.0) support" on page 37
- "Application proxy drop action support on AR Series" on page 38

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 47.

Specify remote end of AMF virtual link by hostname

Available on all devices that support AMF virtual links

From version 5.5.2-0.1 onwards, you can specify the remote end of an AMF virtual link by entering its domain name instead of its IP address (e.g. example.com). This allows you to create a virtual link when the IP address is unknown or dynamic.

To do this, use the new **remote-host** parameter in either of the following commands, instead of the existing **remote-ip** parameter:

```
awplus(config)# atmf virtual-link id <1-4094> ip <local-ip>
remote-id <1-4094> remote-host <domain-name>
```

```
awplus(config)# atmf virtual-crosslink id <1-4094> ip
<local-ip> remote-id <1-4094> remote-host <domain-name>
```

For more information about virtual links, see the AMF Feature Overview and Configuration Guide.

AMF auto-recovery can replace some device series with similar devices

Available on the devices listed in the table below

From version 5.5.2-0.1 onwards, you can use AMF's automatic node recovery to replace devices from one of the following series with a device from a similar, but not identical, series. This is in addition to replacements that have already been listed in the Node Recovery section of the AMF Feature Overview and Configuration Guide.

Original device type	Replacement device type
x310 Series	x530 Series and x530L Series
FS980M Series	GS970EMX Series and GS980MX Series
IE200 Series	IE340 Series and IE340L Series
IE300 Series	IE340 Series and IE340L Series
IE510-28GSX	x530 Series and x530L Series

For more information about node recovery, see the AMF Feature Overview and Configuration Guide.

Bi-directional Forwarding Detection (BFD)

Newly available on SBx908 GEN2, x950, and SBx8100 Series switches.
Previously available on x930 Series switches.

From version 5.5.2-0.1 onwards, Bi-direction Forwarding Detection (BFD) is now supported on SBx908 GEN2, x950, and SBx8100 Series switches, in addition to x930 Series.

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

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

- BFD supports profiles, defined via CLI or API, that are a collection of BFD session parameters. BFD profiles can be associated with BFD peers, OSPF peers, and BGP neighbors.
- BFD can monitor connections to OSPF peers and notify OSPF about connection events.
- BFD can monitor Static Route peers and notify NSM about connection events.

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

Enhanced DPI Web-categorization

Available on AR4050S, AR3050S, and vFW

From software release 5.5.2-0.1 onwards, you can access the enhanced Deep Packet Inspection (DPI) feature known as Web-categorization. Web-categorization helps protect users on the network based on the type of website they access.

The existing licensed feature called Web-categorization uses Digital Arts as a website categorization provider, to enable businesses to manage the types of website their staff can access. Now, as well as the previous proxy-based operation, Web-categorization can also be used with Deep Packet Inspection (DPI) as a second option for managing website access.

To use Web-categorization on your device, you need to configure a DPI provider, enable Web-categorization, and enable DPI. Hosts are categorized by type (if they are identified by the provider), or in the absence of a category by their usual DPI application. As always, you can view available applications using the **show application** command.

Web-categorization requires a Web Control subscription license.

To enable DPI Web-categorization and set the provider to Digital Arts, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
```

```
awplus(config-dpi)# web-categorization digital-arts
```

To enable DPI Web-categorization with no external provider, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# web-categorization
```

For a simple configuration example, see the Configuration section in the Application Awareness Feature Overview and Configuration Guide.

Support for TLS Crypt on OpenVPN

Available on all devices that support OpenVPN

From version 5.5.2-0.1 onwards, AlliedWare Plus firewalls and routers support TLS Crypt on OpenVPN. TLS Crypt uses a pre-shared key to secure the entire OpenVPN session from the first packet. It provides several potential benefits:

- It prevents detection of the OpenVPN connection start, which is helpful in some situations when the OpenVPN protocol signature is detected and blocked.
- It prevents TLS denial of service attacks. DoS attacks are possible with TLS-Auth, where the attacker can open thousands of TLS connections simultaneously but not provide a valid certificate, jamming the available ports. With TLS Crypt the server would reject the connection up front.
- Data is encrypted twice, once by TLS Crypt and once by the TLS session.

To use TLS Crypt, go into interface made for the OpenVPN tunnel and enter the command:

```
awplus(config-if)#tunnel openvpn tls-crypt <key-file>
```

The filename starts with "flash:/" (e.g. flash:/openvpn.key). All clients and the server must share the same key file. TLS Crypt will automatically create the configured key file if it doesn't exist.

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

Virtual UTM Firewall licensing made easier

Available on Virtual UTM Firewall (vFW)

When you purchase a feature license, you need to supply the serial number. From version 5.5.2-0.1 onwards, on vFW, you can now use the serial number of the Vista Manager Network Appliance (VST-APL). Previously, you had to use the serial number of your vFW instance.

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

A long-press on the reset button now deletes the configuration file

Available on all AR Series firewalls and VPN routers.

From version 5.5.2-0.1 onwards, when you press the reset button for more than 5 seconds, the device will delete the configuration file from flash memory, as well as everything else that the long-press used to delete. Therefore, from 5.5.2-01 onwards, long-pressing will delete:

- all NVS contents, and
- all flash content except for the boot firmware file, the latest GUI file, and any license files.

Port Authentication support for dynamic multiple VLAN assignment

Available on all products except the AR1050V, AMF Cloud, and the 10G Virtual UTM Firewall.

AlliedWare Plus **5.5.2-0.1** supports the dynamic assignment of a supplicant to multiple tagged VLANs. This means an authorized supplicant can access a number of tagged VLANs that have been assigned dynamically by a RADIUS server. The RADIUS server assigns these VLANs by including multiple RADIUS Egress-VLANID(56) and/or Egress-VLAN-Name(58) attributes in the Access-Accept or CoA (Change of Authorization) packets.

This feature requires that the port:

- be in trunk mode with egress filtering enabled (**switchport mode trunk ingress-filter enable)**,
- has dynamic VLAN assignment enabled (**auth dynamic-vlan-creation**),
- allows for packet forwarding on multiple VLANs (**auth multi-vlan-session**),
- and is configured with either **auth host-mode single-host** or **auth host-mode multi-host**.

This feature will not work:

- when a port has been configured to authenticate supplicants individually, i.e. when **auth host-mode multi-supplicant** is enabled on a port.
- if authentication roaming is enabled (**auth roaming enable**).

Allied Telesis recommend no more than 100 tagged VLANs are specified on a RADIUS server.

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

For more information on the local RADIUS server, see the Local RADIUS Server Feature Overview and Configuration Guide.

Port Based DHCP IP Address Assignment

Available on SBx8100, SBx908 GEN2, x950, x930, x550, x530, x330, x320, x230, IE210, IE340, GS980MX, GS970EMX, and GS970M Series switches

From version 5.5.2-0.1 onwards, you can configure DHCP port based IP address assignment.

The DHCP server port-based address allocation feature gives you the capability to ensure that the same IP address is always offered to a replacement device as it is being replaced. This IP address is always offered to the same connected port even as the client-identifier or client hardware address changes in the DHCP messages received on that port.

This feature is enabled by substituting a subscriber identifier (subscriber-id) for a client identifier (client-id) in all DHCP server internal transactions. To allow port based address assignment, the subscriber-id of a client needs to be associated with the physical port attachment. Subscriber-id for a remote client is included in the relay-agent information option on DHCP client packets relayed via a relay-agent. For a locally attached client, its subscriber-id is internally generated based on and associated with a port interface directly attached to the DHCP client.

The commands allow you to substitute a client-id with the subscriber-id associated to a client. This is either internally generated, by the ingress port receiving messages for a particular client, or an explicit subscriber-id obtained from a relay agent information option included in the messages from relayed client messages. You have the capability to add a subscriber-id sub-option to the relay agent information option it adds/replaces on client messages. Additionally, the DHCP server enables you to make an IP address reservation for a given client-id.

New commands

The **host** command:

To add a static host address reservation to the DHCP address pool you are configuring for the DHCP client with the given client identifier, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool <pool-name>
awplus(dhcp-config)# host <ip-address> client-id <identifier-id>
```

The **use-subscriber-id** command:

To configure the DHCP server to use subscriber identifier substitution for a client identifier on all DHCP packets for a given remote address, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool <pool-name>
awplus(dhcp-config)# use-subscriber-id
```

The **ip dhcp use-subscriber-id (conf)** command:

To configure the DHCP server to use subscriber identifier substitution on all DHCP packets coming from all switch ports, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp use-subscriber-id
```

The **ip dhcp use-subscriber-id (if)** command:

To configure the DHCP server to use subscriber identifier substitution for the client identifier on all DHCP packets coming from the DHCP client directly connected to an interface, use the commands:

```
awplus(config)# int <port-number>
awplus(config-if)# ip dhcp use-subscriber-id
```

The **ip dhcp-relay agent-option subscriber-id** command:

To set an ASCII string as a subscriber identifier for a port used by the relay agent, use the commands:

```
awplus# configure terminal
awplus(config)# interface <port-number>
awplus(config-if)# ip dhcp-relay agent-option subscriber-id
<subscriber-id>
```

For more information and configuration examples, see the DHCP Feature Overview and Configuration Guide

Improvement to “show stack detail”

Available on all devices that support VCStack

From version 5.5.2.-01 onwards, the output of the **show stack detail** command will list the ports on a Virtual Chassis Stacking neighbor, through which the stack members are connected. This will look like:

```
...
Stack port1.0.27 status        Learnt neighbor 3, connected port3.0.52
Stack port1.0.28 status        Learnt neighbor 2, connected port2.0.27
```

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

License no longer required for Media Redundancy Protocol (MRP) clients

Available on all devices that support MRP

From version 5.5.2-0.1 onwards, an MRP license is only required for running an MRP manager instance. Previously, an MRP license was required to run either MRP client or MRP manager.

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

Enabling DHCP Snooping on individual VLANs

Newly available on SBx8100, x530, x530L and x320 Series switches.
Previously supported on SBx908 GEN2, x950, x930, x510, x510L, IE510, IE340 and IE300 Series switches

From 5.5.2-0.1 onwards, you can optionally enable the DHCP snooping service on a per-VLAN basis on SBx8100, x530, x530L and x320 Series switches, instead of enabling the DHCP snooping service globally.

To do this, use the **per-vlan** parameter in the command:

```
awplus(config)# service dhcp-snooping per-vlan
```

This option only creates an ACL for the VLANs that you configure with the **ip dhcp snooping** command. This limits the amount of DHCP traffic that is forwarded to the CPU. However, using this option creates 2 ACLs for each VLAN that DHCP snooping is enabled on, so it is most suitable if you have a small number of VLANs. Use the **show platform classifier statistics utilization brief** command to see the number of ACLs available for your switch.

For more information about DHCP snooping, see the DHCP Snooping Feature Overview and Configuration Guide.

Information about timed-out loop-detection packets for loop protection

Available on all devices that support loop protection

Previously, some loop-detection packets would not be sent from the port in spite of loop-protection counters reporting the packets as transmitted. From version 5.5.2-0.1 onwards, this has been resolved and the packets are now more reliably sent. However, it is now possible for the sending of a packet to time out. Version 5.5.2-0.1 onwards includes counters to show when this happens and a new log message.

A new warning log message will occur if transmitting loop-detection packets takes much longer than expected. This can happen in some networks with large numbers of loop-protection instances with short loop-detection intervals. The log message is:

"Sending loop-detection frames taking longer than expected - too many instances?"

To prevent this log message, you can either:

- change the loop-detection frame interval to a higher value to reduce the number of packets that are sent in each block. To do this, use the command **loop-protection loop-detect ldf-interval <period>**, or
- reduce the number of instances by reducing the number of VLANs per port or by removing loop protection from some ports.

The following show commands now provide information about timeouts.

- **show loop-protection counters** now includes a 'Packet TX' timeout counter:

```
Switch Loop Detection Counter

 Interface   Tx         Rx         Tx Timeout Rx Invalid Last LDF Rx
-------------------------------------------------------------------------------
 port1.1.5
   vlan1     1          0          0          0          Wed Mar 02 00:47:05 2022
   vlan10    1          0          20         0          Wed Mar 02 00:47:05 2022
...
```

- **show loop-protection** now shows the total number of loop protection instances (one instance per vlan per port) and what that means for the number of packets that need to be transmitted by the device each second:

```
LDF Interval:    10
Fast Block:      Disabled
Total Instances: 29174 (2917 packets/s)
                                                          Timeout
  Int            Enabled  Action     Status    Timeout   Remain    Rx port
  ------------------------------------------------------------------------------
  port1.1.5      Yes      link-down  Normal    20        -         -
  port1.1.6      Yes      link-down  Normal    20        -         -
...
```

Removal of obsolete parameters from the SSH protocol

Available on all AlliedWare Plus devices

Since version 5.5.1-1.1, AlliedWare Plus no longer supports the following insecure options:

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

This improvement made a number of SSH parameters obsolete. In version 5.5.2-0.1, these changes have been made to the AlliedWare Plus CLI:

- Removed all references to RSA1 in configuration and show commands
- Removed all references to DSA in configuration and show commands
- Deprecated the **v1v2** and **v2only** parameters in the **ssh server** command. If you enter these, AlliedWare Plus prints a warning
- Set the RSA default key length to 2048 and the ECDSA default key size to 384

- Set the SSH version to always be 2
- Removed the version option from the **ssh** command
- Updated the RSA key generation commands to have a supported range of 1024-16384
- Updated the ECDSA key generation commands to support 521 bits.

You can still destroy unneeded RSA1 and DSA keys by using the commands:

- crypto key destroy userkey <*username*> dsa
- crypto key destroy userkey <*username*> rsa1

Option to drop ICMP timestamp requests and responses

Available on all AlliedWare Plus devices

From version 5.5.2-0.1 onwards, you can configure the device to drop all ICMP timestamp request and response packets. You may wish to do this because the ICMP timestamp response contains the device's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services. In addition, it may be possible to fingerprint devices by analyzing their responses to invalid ICMP timestamp requests.

By default, timestamp requests and responses are allowed. To drop them, use the new command:

```
awplus(config)# no ip icmp-timestamp
```

To allow them again, use the command:

```
awplus(config)# ip icmp-timestamp
```

Option to disable TCP timestamp responses

Available on all AlliedWare Plus devices

From version 5.5.2-0.1 onwards, you can disable TCP timestamp responses on the device. You may wish to do this because TCP timestamps may allow other parties to remotely calculate the system uptime and boot time of the device and the device's clock. To prevent this information leaking to potential attackers, we recommend you disable TCP timestamps on the device, unless you need to use them.

By default, timestamp responses are enabled. To disable them, use the new command:

```
awplus(config)# no ip tcp-timestamp
```

To enable them again, use the command:

```
awplus(config)# ip tcp-timestamp
```

Removal of a vulnerable MAC algorithm from secure algorithm list

Available on all AlliedWare Plus devices

From version 5.5.2-0.1 onwards, if you limit the SSH server so that it only uses secure Message Authentication Code (MAC) algorithms, it will prevent you from using 64-bit UMAC (umac-64@openssh.com). This is in addition to other already-prevented algorithms.

To limit SSH to secure MAC algorithms only, use either of the commands:

```
awplus(config)# ssh server secure-mac
awplus(config)# ssh server secure-algs
```

Prevention of ARP (foreign host route) poisoning

Available on all AlliedWare Plus devices

From version 5.5.2-0.1 onwards, ARP packet processing has been made stricter, to prevent ARP (foreign host route) poisoning. Now, AlliedWare Plus will only process ARP packets that are local to the incoming interface. This means the packets must have:

- a sender protocol address inside one of the incoming interface's local subnets, and
- a target protocol address equal to one of the incoming interface's IP addresses.

The new behavior is enabled by default. You can disable it and return to the earlier behavior by using the commands:

```
awplus(config)# interface <name>
awplus(config-if)#arp-loose-check
```

This new **arp-loose-check** command lets AlliedWare Plus process ARPs that have a sender protocol address from outside the interface's local subnets.

To return to the new strict behavior, use the command **no arp-loose-check**. You may need to clear the ARP cache after entering **no arp-loose-check**, to remove undesired existing ARPs.

The new behavior cannot be used at the same time as Proxy ARP. When Proxy ARP is enabled on an interface, the ARP behavior is the same as previously, instead of using the new strict behavior. Therefore, you cannot use the new command at the same time as Proxy ARP.

Support for TQ6602 GEN2 and TQm6602 GEN2 APs in Vista Manager mini

Available on all AlliedWare Plus products that support Vista Manager mini.

From version 5.5.2-0.1 and Device GUI 2.11.0 onwards, you can use the AWC Wireless Manager to manage the following additional APs in Vista Manager mini:

- TQ6602 GEN2
- TQm6602 GEN2

The APs must be running firmware version 8.0.1.-1.1 onwards.

For these APs, note that Channel Blanket, Smart Connect and Passpoint support on Vista Manager mini will be available with a later AlliedWare Plus version.

For more information on Vista Manager mini, see the Wireless Management (AWC) with Vista Manager mini User Guide.

Obtain Access Point tech-support files via Vista Manager mini

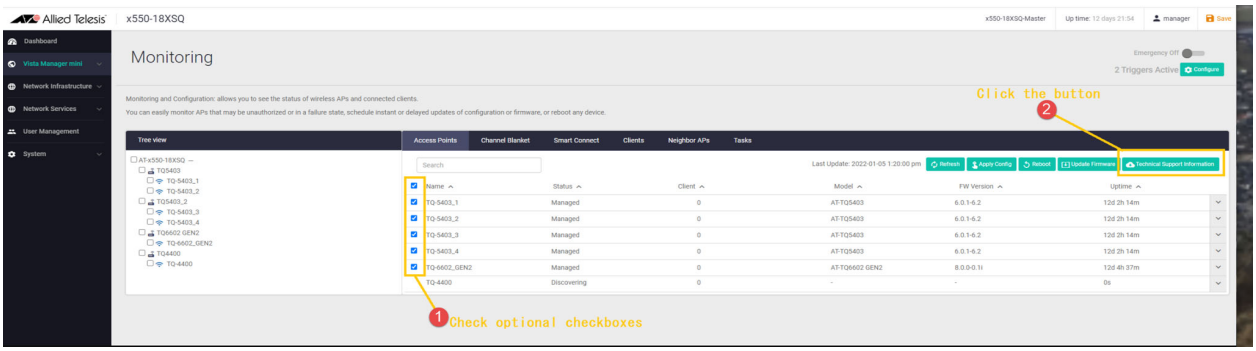
Available on all AlliedWare Plus products that support Vista Manager mini, when managing the following AP models:

Model	Firmware version
TQ6702 GEN2, TQm6702 GEN2	8.0.0-1.1 or later
TQ6602 GEN2, TQm6602 GEN2	8.0.1-1.1 or later
TQ6602	7.0.1-2.1 or later
TQ5403, TQm5403, TQ5403e, TQ1402, TQm1402	6.0.1-4.1 or later
TQ4600, TQ4400e	4.3.0 or later

From version 5.5.2-0.1 onwards, and Device GUI 2.11.0, you can get a tech-support file via Vista Manager mini from a single managed AP or all of the APs that belong to an AWC-CB or AWC-SC group.

To access this feature, go to **Vista Manager mini** > **Monitoring** and:

1. Use the checkboxes to select the AP or APs
2. Click Technical Support Information in either the Access Points, Channel Blanket, or Smart Connect tab.



New commands

The following tech-support commands are also available within the AlliedWare Plus CLI:

```
wireless get-tech ap {<ap-profile-id-range>|all} url <url>
wireless get-tech ap-profile {<ap-profile-id-range>|all} url <url>
wireless get-tech sc-profile {<sc-profile-id-range>|all} url <url>
wireless get-tech abort
```

Enhanced show command

The **show wireless ap** command **status** and **detail** parameters now include tech-support detail:

```
show wireless ap {<ap-id-range>|all} [brief|status|detail]
```

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

Passpoint (Hotspot 2.0) support

Available on all AlliedWare Plus products that support Vista Manager mini

From software release 5.5.2-0.1 onwards, the AWC Wireless Manager with Vista Manager mini supports wireless Hotspot version 2.0.

The following new commands are available:

- osu-providers service-desc lang desc
- osu-providers server-uri
- osu-providers nai
- osu-providers method-list
- osu-providers icon lang file
- osu-providers friendly-name lang name
- osu status enable
- osu ssid

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

Application proxy drop action support on AR Series

Available on AR1050V, AR2050V, AR3050S and AR4050S

From version 5.5.2-0.1 onwards, you can use the application proxy's threat protection feature to drop packets or take a link down on the switch ports on AR1050V, AR2050V, AR3050S and AR4050S firewalls and routers. Note that this doesn't apply to AR2010V routers.

This feature is part of AMF Security (AMF-Sec) and AMF Security mini (AMF-Sec mini).

To turn this feature on, go into interface made for the switchport or ports and enter the command:

```
awplus(config-if)#application-proxy threat-protection drop
```

or

```
awplus(config-if)#application-proxy threat-protection link-
down
```

With the drop action, the device will only drop packets that arrive at the port, not packets sent from the port.

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.2-x.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

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

- 5.5.1-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:

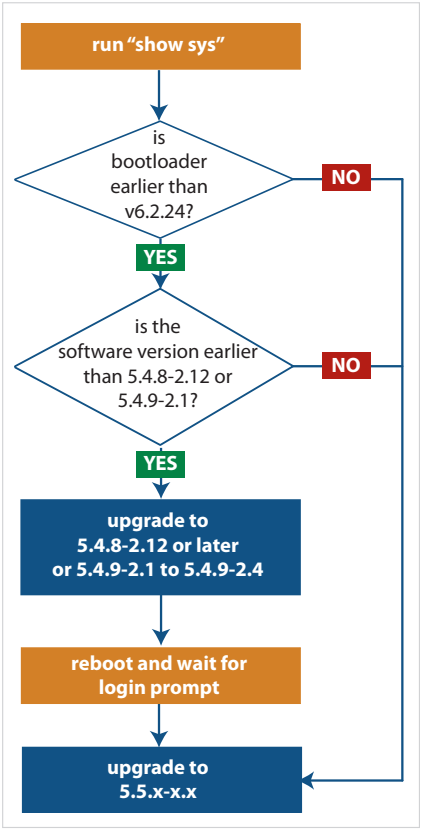
- 5.4.9-1.x
- 5.4.9-0.x
- any version before 5.4.8-2.12.

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:

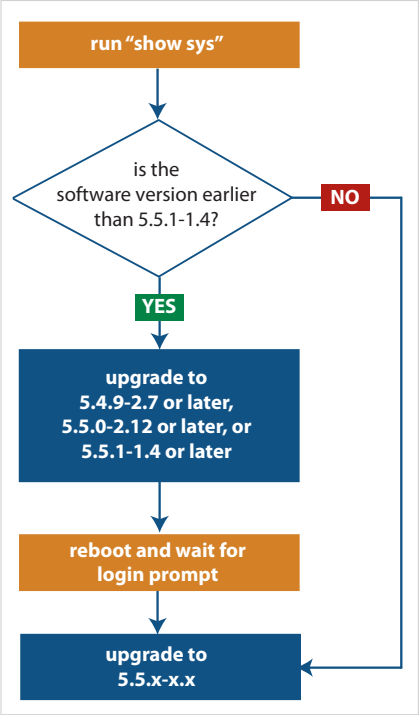



```
awplus# show system
```

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
Long-press on the reset button now deletes the configuration file	Available on all AR Series firewalls and VPN routers.	See "A long-press on the reset button now deletes the configuration file" on page 29.
Sending of loop-detection packets can now time out	All devices that support the Loop Protection feature	See "Information about timed-out loop-detection packets for loop protection" on page 32.
A number of SSH parameters have changed or become obsolete	All AlliedWare Plus devices	See "Removal of obsolete parameters from the SSH protocol" on page 33.
umac-64@openssh.com has been removed from the secure algorithm list	All AlliedWare Plus devices	See "Removal of a vulnerable MAC algorithm from secure algorithm list" on page 35.
ARP processing has become stricter	All AlliedWare Plus devices	See "Prevention of ARP (foreign host route) poisoning" on page 35.
Display of power-inline settings has changed for dual signature devices	x530L-10GHXm, GS980MX/10HSm, x530DP-28GHXm, and x530DP-52GHXm switches	When a dual signature PD is connected, from 5.5.2-0.1 onwards, the **show power-inline** command now displays the total port power on the data pair. The spare pair always displays the power as '-'.

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.2 license on your switch if you are upgrading to 5.5.2-x.x on your SBx908 GEN2 or SBx8100 switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- "Licensing this Version on an SBx908 GEN2 Switch" on page 48 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 50.

Upgrading a VCStack with rolling reboot

Applies to all stackable AlliedWare Plus switches, except SBx8100

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

For SBx908 GEN2, x950 and x550 Series switches

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

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

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

For x530 Series switches using DAC to stack

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

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

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

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

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

To use rolling reboot

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

Forming or extending a VCStack with auto-synchronization

Applies to all stackable AlliedWare Plus switches

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

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

For SBx908 GEN2, x950 and x550 Series switches

Auto-synchronization is supported between this version and:

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

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

For CFC960 cards in an SBx8100 system

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

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

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

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

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

For x530 Series switches using DAC to stack

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

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

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

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

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

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

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

If using an AMF controller

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

If using secure mode

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

If using Vista Manager EX

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

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

If using none of the above

If none of the above apply, then nodes running version this version are compatible with nodes running:

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

Upgrading all devices in an AMF network

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

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

2. Decide which AMF upgrade method is most suitable.

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

Obtaining User Documentation

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

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

Verifying the Release File

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

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

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

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

Caution

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

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

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

Licensing this Version on an SBx908 GEN2 Switch

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

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

1. Obtain the MAC address for a switch

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

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

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

2. Obtain a release license for a switch

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

3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

```
awplus#show license

Board region: Global

Index                          : 1
License name                   : Base License
Customer name                  : Base License
Type of license                : Full
License issue date             : 20-Mar-2021
Features included              : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                                 EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                                 L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VCStack, VRRP

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

Licensing this Version on an SBx8100 Series CFC960 Control Card

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

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

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

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

1. Obtain the MAC address for a control card

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

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

```
awplus#show system mac license

MAC address for licensing:


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

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

2. Obtain a release license for a control card

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

3. Apply a release license on a control card

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

```
awplus#show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2021
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

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

Installing this Software Version

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 48 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 50.

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

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

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

Product	Command
SBx8100 with CFC960	`awplus(config)# boot system SBx8100-5.5.2-0.3.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.2-0.3.rel`
x950 series	`awplus(config)# boot system x950-5.5.2-0.3.rel`
x930 series	`awplus(config)# boot system x930-5.5.2-0.3.rel`
x550 series	`awplus(config)# boot system x550-5.5.2-0.3.rel`
x530 series	`awplus(config)# boot system x530-5.5.2-0.3.rel`
x330-10GTX	`awplus(config)# boot system x330-5.5.2-0.3.rel`
x320 series	`awplus(config)# boot system x320-5.5.2-0.3.rel`
x230 series	`awplus(config)# boot system x230-5.5.2-0.3.rel`
x220 series	`awplus(config)# boot system x220-5.5.2-0.3.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.2-0.3.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.2-0.3.rel`

Product	Command
XS900MX series	`awplus(config)# boot system XS900-5.5.2-0.3.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.2-0.3.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.2-0.3.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.2-0.3.rel`
GS970EMX/10	`awplus(config)# boot system GS970EMX-5.5.2-0.3.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.2-0.3.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.2-0.3.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.2-0.3.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.2-0.3.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.5.2-0.3.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.5.2-0.3.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.2-0.3.rel`

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

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

6. Reboot using the new software version.

```
awplus# reload
```

Accessing and Updating the Web-based GUI

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

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

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

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

Browse to the GUI

Perform the following steps to browse to the GUI.

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

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

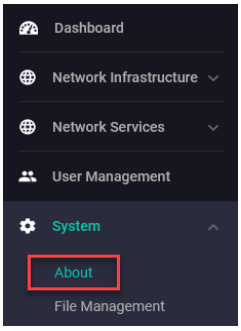
   Alternatively, on unconfigured devices you can use the default address, which is:

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

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

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

Check the GUI version



To see which version you have, open the **System** > **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.2-0.3 is 2.11.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 55 or "Update the GUI on AR-Series devices" on page 56.

Update the GUI on switches

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

1. Obtain the GUI file from our Software Download center. The GUI filename to use with AlliedWare Plus v5.5.2-x.x is awplus-gui_552_26.gui.

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

2. Log into the GUI:

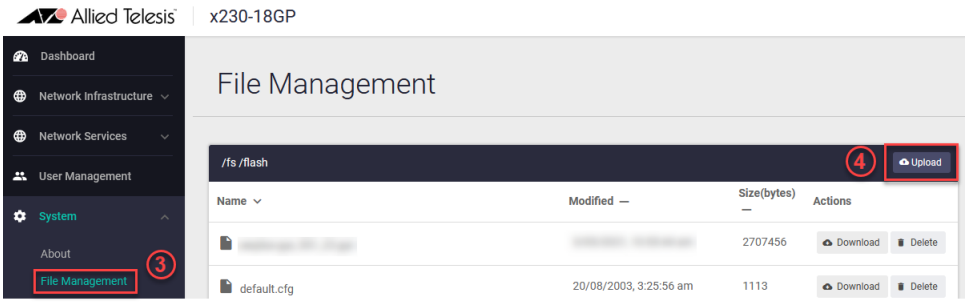
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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

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

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

4. Click **Upload**.



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

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

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

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

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

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

Update the GUI on AR-Series devices

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

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

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

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

3. Browse to the GUI and check that you have the latest version now, on the **System** > **About** page. You should have v2.11.0 or later.