Allied Telesis™

Release Note for AlliedWare Plus Software Version 5.5.3-2.x

AlliedWare Plus
OPERATING SYSTEM

AMF Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series

x330 Series
x320 Series
x250 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series

XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series

AR4000S-Cloud
10GbE UTM Firewall
AR4050S-5G
AR4050S
AR3050S
AR1050V
TQ6702 GEN2-R

» 5.5.3-2.1 » 5.5.3-2.3

Acknowledgments

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

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**.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

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/**

What’s New in Version 5.5.3-2.3

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x540 Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall[1]
AR4000S-Cloud[1]
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ6702 GEN2-R

[1] Please contact your customer support representative for more information about availability on this product

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-2.3.

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 35.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 37. 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 Plus Cloud		05/2024	vaa-5.5.3-2.3.iso (VAA OS) vaa-5.5.3-2.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-2.23vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	05/2024	SBx81CFC960-5.5.3-2.3.rel
SBx908 GEN2	SBx908 GEN2	05/2024	SBx908NG-5.5.3-2.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	05/2024	x950-5.5.3-2.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	05/2024	x930-5.5.3-2.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2024	x550-5.5.3-2.3.rel
x540L-28XTm x540L-28XHm x540L-52XTm x540L-52XHm x540L-28XS	x540L	05/2024	x540-5.5.3-2.3.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	05/2024	x530-5.5.3-2.3.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	05/2024	x330-5.5.3-2.3.rel
x320-10GH x320-11GPT	x320	05/2024	x320-5.5.3-2.3.rel
x250-10XTm x250-18XTm x250-28XTm x250-18XS x250-28XS	x250	05/2024	x250-5.5.3-2.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2024	x230-5.5.3-2.3.rel

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

Models	Family	Date	Software File
x220-28GS x220-52GT x220-52GP	x220	05/2024	x220-5.5.3-2.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	05/2024	IE340-5.5.3-2.3.rel
IE220-6GHX IE220-10GHX	IE220	05/2024	IE220-5.5.3-2.3.rel
IE210L-10GP IE210L-18GP	IE210L	05/2024	IE210-5.5.3-2.3.rel
XS916MXT XS916MXS	XS900MX	05/2024	XS900-5.5.3-2.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	05/2024	GS980MX-5.5.3-2.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	05/2024	GS980EM-5.5.3-2.3.rel
GS980M/52 GS980M/52PS	GS980M	05/2024	GS980M-5.5.3-2.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	05/2024	GS970EMX-5.5.3-2.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2024	GS970-5.5.3-2.3.rel
AR4000S-Cloud[1]		05/2024	AR-4000S-Cloud-5.5.3-2.3.iso
10GbE UTM Firewall[1]		05/2024	ATVSTAPL-1.9.1.iso and vfw-x86_64-5.5.3-2.3.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	05/2024	AR4050S-5.5.3-2.3.rel AR3050S-5.5.3-2.3.rel
AR1050V	AR-series VPN routers	02/2024	AR1050V-5.5.3-2.3.rel
TQ6702 GEN2-R	Wireless AP Router	02/2024	TQ6702GEN2R-5.5.3-2.3.rel

[1] Please contact your customer support representative for more information about availability on this product

Caution: Software version 5.5.3-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.3 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.3 license installed, that license also covers all later 5.5.3 versions, including 5.5.3-1.x and 5.5.3-2.x. Such switches will not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 31 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 33.

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

The 5.5.3-2.3 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.3-2.3:

ER-5795 *Available on: x530 / x530L, x550, x930, x950, SBx908Gen2, and SBx81CFC960 Series switches.*

Previously, a VCStack failover would cause a new BFD session to be created on the new Master, resulting in the remote end peer to detect session down. This enhancement introduces support for seamless synchronization of BFD sessions to the new VCStack Master during a failover.

ISSU: Effective when CFCs upgraded.

ER-5890 *Available on: GS970EMX, GS980MX, XS900MX, x330, x530 / x530L, x550, x930, x950, SBx908Gen2, and SBx81CFC960 Series switches.*

Improvements to rolling reboot have been implemented to allow routes from dynamic routing protocols such as OSPF, BGP, and RIP to be retained by the stack master across the rolling reboot operation. This helps to minimize network disruption caused by the rolling reboot.

ISSU: Effective when CFCs upgraded.

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

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

ISSU: Effective when ISSU complete.

ER-5591 *Available on: GS970M, GS970EMX, XS900MX, x230/x230L, x330, x550, x930, x950, and SBx908Gen2 Series switches.*

A new option has been added for VLAN translations which aren't specified by explicit rules. Previously, the options were to either 'drop' the packets or 'accept' them (pass them through without any translation). Now you can optionally add an outer-vlan tag to these packets. The command is:

```
switchport vlan translation default [drop|outer-vlan <vid>]
```

For example, to configure an outer-vlan on po1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface po1
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 1000,2000
awplus(config-if)# switchport trunk native vlan 10
awplus(config-if)# switchport vlan translation default outer-
   vlan 2000
```

ER-5803 *Available on: x530 / x530L, x930, x950, SBx908Gen2, SBx81CFC960, AR4050S,AR4050S-5G and AR3050S Series.*

Previously, if a saved configuration was pasted in to a console with VRF and certain VRF management configuration, if the management functionality was configured before the VRF creation, the config could fail.

This issue has been resolved.

The running config now has the VRF creation happening before the management functionality.

ISSU: Effective when CFCs upgraded.

Issues Resolved in Version 5.5.3-2.3

This AlliedWare Plus maintenance version includes the following resolved issues:

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	TQ6702 GEN2-R	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81125	**802.1x**	Previously, if two-step authentication was configured, re-authentication could fail. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	–	–
CR-80477	**AMF**	Previously, it was possible for a provisioned AMF node to include a copy of a UUID, if the **copy** or **clone** commands were used during the provisioning process. This could result in problems identifying the device after recovery when Vista Manager was in use. 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-82753	**AMF**	Previously, when attempting to use an AMF backup command on a device that did not support backups, the error message provided suggested that the problem was due to incorrect configuration. The error message has been changed so that it is clear the hardware platform does not support AMF backup. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–
CR-79525	**ARP** **Neighbor Discovery**	Previously, ARP learning was causing memory exhaustion. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	Y	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	TQ6702 GEN2-R	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81208	**BFD**	Previously, changing the BFD configuration from multi-hop to single-hop did not work as expected. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	–
CR-81867	**BGP**	Previously, BGP peers could get stuck in ‘Connect’ when both ends were configured with a VRF and an md5 password. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	Y	Y	–	–
CR-81762	**CLI, VLAN**	Previously, on rare occasions, logging into the AlliedWare Plus device via Telnet, could cause an unexpected disconnection. 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-82069	**CLI, VLAN**	Previously, running the **`show interface switchport vlan transport interface`** command on an interface with a default VLAN translation of outer-vlan, could incorrectly display the VLAN ID in the middle field. This issue has been resolved, and the VLAN ID now correctly displays in the right hand field.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–
CR-82498	**Device Security**	Previously, on platforms with **`crypto secure-mode`** enabled, on-demand algorithm self-tests may not have worked. This issue has been resolved. SSU: Effective when CFCs upgraded.	–	Y	–	–	–	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	TQ6702 GEN2-R	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81870	**Device Security, Encryption**	Previously, the command `show running-config unencrypted` could be used when the device was configured to run in crypto secure-mode. This has been changed. Now, the command is not permitted when secure-mode is enabled. This is to prevent disclosure of clear-text passwords and keys stored in the configuration.	–	Y	–	–	–	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-82014	**Device Security, HTTP service, Logging**	CBC and CCM based TLS ciphers have been removed, because they are now considered less secure and are not allowed by some security certifications. In addition, more TLS ciphers are also supported for TLSv1.2 and TLSv1.3 for web GUI HTTPS connections. 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-82798	**DHCP Snooping**	Previously, the DHCP snooping module could restart when handling a bootp packet. 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-81922	**Environmental Monitoring**	Previously, on AT-x530DP, the temperature limits applied when using a combination of AT-PWR150, AT-PWR250, AT-PWR250 v2, or AT-PWR250R were incorrect. This only occurred when both PSU slots had PSUs installed. This issue has been resolved. An error message will be displayed if certain unsupported PSUs (PWR150 together with PWR250 or PWR250DC) are used together. The PSU fans will run at full speed when an unsupported combination of PSUs is detected.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	TQ6702 GEN2-R	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81881	**IDS/IPS**	Previously, when activating a UTM stream feature such as IPS or IP Reputation, an unnecessary warning log was produced. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-81703	**IPSec**	Previously, on devices supporting AES-GCM IPSEC tunnels, the default profile could include invalid combinations of GCM with 3DES. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–
CR-81830	**Logging, WebAPI**	Previously, the log message did not provide details of the username or remote host when a login failure via HTTP(S) occurred. This issue has been resolved by including the extra details in the log message. 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-81577	**Memory Management**	Previously, on virtual firewall and AMF containers, debug-low-memory files weren't being generated when crossing the critical low memory threshold. This issue has been resolved. Now, if free memory becomes very low a debug-low-memory file will be generated, and if free memory is below the critical level, the container will reboot automatically.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y
CR-81827	**OSPFv2, WebAPI**	Previously, certain multicast reserve range packets were not correctly being trapped to the CPU. This issue has been resolved.	Y	Y	–	–	–	Y	–	–	–	Y	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-81797	**Pluggable Transceivers**	Previously, the **`limited-reach-mode`** command could fail to be executed on the x550 platform. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	TQ6702 GEN2-R	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-81716	**Pluggable Transceivers**	Previously, when an SFP was disabled then re-enabled (via {{shutdown}}/{{no shutdown}}), there was a possibility it may not link up. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	Y	Y	–	–	–	Y	Y	Y	–	Y	–	–	–	Y	–	–	–	–	–	–	–
CR-82679	**Pluggable Transceivers**	Previously, 1G SFPs (e.g. AT-SPSX) installed in the x530-28GSX, could fail to link up when configured for 100M-BASE-FX mode. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-78955	**SNMP**	Previously, in SNMP traps for MAC thrashing, the VLAN ID was set to 0. This is now resolved and the VLAN ID is set to the VLAN the thrashing was detected on. ISSU: Effective when CFCs upgraded.	Y	–	Y	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	–	–
CR-81948	**SSH**	This software update addresses the SSH vulnerabilities specified in CVE-2023-48795	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-82780	**SSH**	Previously, SSH known hosts which used non-standard port numbers could fail to be removed. 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-81609	**VCStack**	Previously, when VCS traps were enabled, a VCS stack would send a VCS resiliency link trap if the link status changed from shutdown to up, or from up to shutdown. This behaviour is now changed. A resiliency link trap can be generated only if both VCS traps and VCS resiliency link traps are enabled. ISSU: Effective when CFCs upgraded.	Y	Y	–	Y	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	GS970M/EMX	XS900MX	GS980M	GS980MX	GS980EM	IE340	IE220	IE210L	x220	x230, x230L	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	TQ6702 GEN2-R	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud
CR-82163	**VCStack, Loop Protection**	Previously, if Loop Protection Frame (LDF) packets from a neighbor device caused a storm, it could cause a stack separation on the x330 platform. This issue has been resolved by setting the storm control level of LDF broadcast to 50% of port speed by default.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-79890	**VRF, RADIUS Server**	Previously, when configuring the RADIUS server, when a VRF was specified the configuration was in the wrong order when it was saved. This resulted in the server not being configured when the configuration was re-run (e.g. reboot). This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	–	Y	Y	–	–
CR-82678	**VRRP**	Previously, an overlap in the settings for trapping reserve multicast packets to the CPU, could result in short periods of packet loss during a rolling reboot, if the stack was the VRRP master. This issue has been resolved.	Y	Y	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	–	–	–

What’s New in Version 5.5.3-2.1

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall[1]
AR4000S-Cloud[1]
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ6702 GEN2-R

[1] Please contact your customer support representative for more information about availability on this product

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.3-2.1.

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 35.

For instructions on how to update the web-based GUI, see “Accessing and Updating the Web-based GUI” on page 37. 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 Plus Cloud		11/2023	vaa-5.5.3-2.1.iso (VAA OS) vaa-5.5.3-2.1.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.3-2.1.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2023	SBx81CFC960-5.5.3-2.1.rel
SBx908 GEN2	SBx908 GEN2	11/2023	SBx908NG-5.5.3-2.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	11/2023	x950-5.5.3-2.1.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	11/2023	x930-5.5.3-2.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2023	x550-5.5.3-2.1.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	11/2023	x530-5.5.3-2.1.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	11/2023	x330-5.5.3-2.1.rel
x320-10GH x320-11GPT	x320	11/2023	x320-5.5.3-2.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2023	x230-5.5.3-2.1.rel
x220-28GS x220-52GT x220-52GP	x220	11/2023	x220-5.5.3-2.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	11/2023	IE340-5.5.3-2.1.rel
IE220-6GHX IE220-10GHX	IE220	11/2023	IE220-5.5.3-2.1.rel
IE210L-10GP IE210L-18GP	IE210L	11/2023	IE210-5.5.3-2.1.rel

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

Models	Family	Date	Software File
XS916MXT XS916MXS	XS900MX	11/2023	XS900-5.5.3-2.1.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	11/2023	GS980MX-5.5.3-2.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2023	GS980EM-5.5.3-2.1.rel
GS980M/52 GS980M/52PS	GS980M	11/2023	GS980M-5.5.3-2.1.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	11/2023	GS970EMX-5.5.3-2.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2023	GS970-5.5.3-2.1.rel
AR4000S-Cloud[1]		11/2023	AR-4000S-Cloud-5.5.3-2.1.iso
10GbE UTM Firewall[1]		11/2023	ATVSTAPL-1.9.1.iso and vfw-x86_64-5.5.3-2.1.app
AR4050S AR4050S-5G AR3050S	AR-series UTM firewalls	11/2023	AR4050S-5.5.3-2.1.rel AR3050S-5.5.3-2.1.rel
AR1050V	AR-series VPN routers	11/2023	AR1050V-5.5.3-2.1.rel
TQ6702 GEN2-R	Wireless AP Router	11/2023	TQ6702GEN2R-5.5.3-2.1.rel

[1] Please contact your customer support representative for more information about availability on this product

Caution: Software version 5.5.3-2.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.3 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.3 license installed, that license also covers all later 5.5.3 versions, including 5.5.3-1.x and 5.5.3-2.x. Such switches will not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 31 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 33.

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

The 5.5.3-2.1 software version is not ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.3-2.1:

- "Support for NETCONF and RESTCONF" on page 16
- "Denial of Service (DoS) attack protection added to some switches" on page 18
- "Support for Precision Time Protocol in VCStack configurations" on page 19
- "Support for IPv6 routing with longest prefix length for prefixes from 0-128 bits" on page 20
- "Support for AES-GCM for IPsec" on page 20
- "Additional features for the TQ6702 GEN2-R wireless router" on page 20
- "Setting the lifetime of X.509 certificates" on page 21
- "Disable local RADIUS server users" on page 21
- "Passwords are now displayed in encrypted form in running configuration" on page 22
- "OSPFv3 support for VRF-lite with IPv6" on page 23
- "Support for AR4000S-Cloud on more virtual environments" on page 23
- "Increase to log storage size on virtual platforms" on page 23

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 30.

Support for NETCONF and RESTCONF

Available on IE340, IE220 and x530 Series switches

From version 5.5.3-2.1 onwards, AlliedWare Plus supports NETCONF (Network Configuration Protocol) and RESTCONF (RESTful Network Configuration Protocol) network management protocols. NETCONF and RESTCONF are both protocols used for configuring and managing network devices. They are considered model-driven protocols, meaning they leverage data models to define the structure and behavior of network configurations.

Data models are conventionally written in YANG (Yet Another Next Generation), although any formatted standard way of expressing the same information is potentially acceptable. If some other expression is desired, it is normal to start with the YANG model, then apply transformations to convert to another format. All data models supported by the AlliedWare Plus implementations of NETCONF and RESTCONF will have expressions written in YANG.

YANG data models are the foundation for both NETCONF and RESTCONF, as they define the structure and semantics of the data exchanged between network management systems and network devices. These models make it possible to manage network configurations and gather operational data in a consistent, standardized, and vendor-agnostic way, facilitating efficient network management and automation.

NETCONF and RESTCONF provide robust, predictable, and consistent programmatic management of networks. They offer a structured and standardized approach to network configuration and management, allowing for automation, interoperability, and ease of integration with various network devices and systems. The use of data models helps ensure consistency and reliability in the management of network configurations and operations.

The benefits of using NETCONF and RESTCONF

Traditionally, configuration and monitoring of network devices was carried out using the CLI. One drawback of using the CLI is that it lacks standardization. Managing multi-vendor environments with different syntaxes can become difficult, especially when you want to introduce automation.

SNMP (Simple Network Management Protocol) was developed as a standard protocol for obtaining management information and performing configuration tasks through software. It has been widely used for network management and monitoring.

NETCONF and RESTCONF, on the other hand, were created as an attempt to provide a next-generation protocol to replace SNMP. NETCONF aims to improve upon the limitations of SNMP by offering a more structured and programmatic approach to network configuration and management. It provides a standardized way to communicate and interact with network devices, enabling automated configuration and management capabilities. Use of standard protocols and standard data models means that software written to use these protocols can be reused in many different networks.

New commands

This software version introduces two new commands:

```
awplus(config)#service restconf
awplus(config)#ssh server netconf
```

Example To enable the HTTP and RESTCONF servers, use the following commands:

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

Note: to enable RESTCONF functionality, it is necessary to enable the HTTP service.

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

Denial of Service (DoS) attack protection added to some switches

Added to x530, x530L, x320, GS980MX and GS980EM series switches

From version 5.5.3-2.1 onwards, x530, x530L, x320, GS980MX and GS980EM series switches can defend against a range of attacks. Six different attacks can be detected: IP Options, Land, Ping-of-Death, Smurf, Synflood and Teardrop. When an attack is detected, the switch can shut the port down, send an SNMP trap, or do both.

DoS attack protection is available on switch ports, but not on aggregated links.

To configure this defense, use the following command on the desired switch interfaces:

```
awplus(config-if)# dos {ipoptions|land|ping-of-death|smurf
broadcast <ip-address>|synflood|teardrop} action [shutdown]
[trap]
```

Type of attack	Description
ipoptions *(x530, x530L and GS980MX series only)*	This type of attack occurs when an attacker sends packets containing bad IP options to a victim node. There are many different types of IP options attacks and this software does not try to distinguish between them. Rather, if this defense is activated, the number of ingress IP packets containing IP options is counted. If the number exceeds 20 packets per second, the switch considers this a possible IP options attack.
land	This type of attack occurs when the Source IP and Destination IP address are the same. This can cause a target host to be confused. Since packets with the same source and destination addresses should never occur, these packets are dropped when this attack is enabled. Note that on x530, x530L, x320, GS980MX and GS980EM Series switches, this defense requires the CPU to monitor packets. However, it sends packets to the CPU at a controlled and limited rate, so it will not heavily load the CPU. If multiple ports receive problematic traffic as the same, this rate-limiting may delay detection of the attack.
ping-of-death	This type of attack results from a fragmented packet which, when reassembled, would exceed the maximum size of a valid IP datagram. To detect this attack, the fragments of ICMP packets have to be sent to the CPU for inspection. Therefore, this defense can load the CPU.
smurf	This type of attack is an ICMP ping packet to a broadcast address. Although routers should not forward packets to local broadcast addresses anymore (see RFC2644), the Smurf attack can still be explicitly discarded with this command. In order for the Smurf attack to work, the broadcast IP address is required. Any ICMP Ping packet with this destination address is considered an attack.

Type of attack	Description
synflood	In this type of attack, an attacker, seeking to overwhelm a victim with TCP connection requests, sends a large number of TCP SYN packets with bogus source addresses to the victim. The victim responds with SYN ACK packets, but since the original source addresses are bogus, the victim node does not receive any replies. If the attacker sends enough requests in a short enough period, the victim may freeze operations once the requests exceed the capacity of its connections queue.
teardrop	In this DoS attack, an attacker sends a packet in several fragments with a bogus offset value, used to reconstruct the packet, in one of the fragments to a victim. This results in the victim being unable to reassemble the packet, possibly causing it to freeze operations. Note that this defense requires the CPU to monitor packets. Therefore, this defense can load the CPU.

Note that:

- DoS protection takes precedence over ACL rules. This can stop the switch from blocking traffic that would be blocked by an ACL. For example, teardrop protection requires the switch to count fragmented packets, so fragmented packets will be forwarded even if there is an ACL to drop them.
- Protection from IP options attacks is not available on x320 or GS980EM series switches.

Support for Precision Time Protocol in VCStack configurations

Added to SBx908 GEN2, x950 and x550 Series switches. Previously available on x530L Series switches.

From version 5.5.3-2.1 onwards, SBx908 GEN2, x950 and x550 Series switches support Transparent Clock for Precision Time Protocol (PTP) in VCStack configurations. PTP is an Ethernet or IP-based protocol for synchronizing time clocks on a collection of network devices. The transparent clock computes the variable delay as the PTP packets pass through the switch or the router.

Note that 100G interfaces are not supported for stacking with PTP. If you need to use PTP on an SBx908 GEN2 or x950 Series stack, the stack links need to be 40G rather than 100G.

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

Support for IPv6 routing with longest prefix length for prefixes from 0-128 bits

Added to SBx908 GEN2, x950 and x930 Series switches. Previously available on most other AlliedWare Plus switches.

From version 5.5.3-2.1 onwards, SBx908 GEN2, x950 and x930 Series switches support Layer 3 IPv6 switching with longest prefix match (LPM) with prefix lengths from 0 to 128 bits. Previously, they only supported LPM with 0-64 and 128 bit prefixes.

These switches now comply with RFC-7608/BCP-198 requirements.

For more information, see the IPv6 Feature Overview and Configuration Guide.

Support for AES-GCM for IPsec

Available on all AlliedWare Plus firewalls that support IPsec.

From version 5.5.3-2.1 onwards, AlliedWare Plus supports Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) for IPsec authentication and encryption. AES-GCM is a highly secure option for providing confidentiality and data origin authentication.

AlliedWare Plus supports three different integrity check value (ICV) lengths: 8, 12 and 16 bytes.

To use AES-GCM with IPsec, use the following options in the **transform** command in IPsec Profile Configuration mode:

```
awplus(config-ipsec-profile)# transform <1-255> protocol esp
integrity {gcm8|gcm12|gcm16} encryption {aes128|aes192|aes256}
```

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

Additional features for the TQ6702 GEN2-R wireless router

From software version 5.5.3-2.1 onwards, AlliedWare Plus supports the following new features for the TQ6702 GEN2-R wireless router:

- AMF-Sec application proxy on wireless interfaces
- Application Aware Deep Packet Inspection (DPI) (using the built-in application list only). See the Application Awareness Feature Overview and Configuration Guide for step-by-step configuration details
- Ethernet Bonding
- Policy Based Routing (PBR) - see the Policy-Based Routing Feature Overview and Configuration Guide for step-by-step configuration details
- SD-WAN - see the Policy-Based Routing Feature Overview and Configuration Guide for step-by-step configuration details

- Eco-friendly LED. This lets you turn the device's LED off, to save power.
- Additional Captive Portal features:
  - using a secondary RADIUS server if the primary one fails
  - Walled Garden (including use of wildcards)
  - a reauthentication timer (3600 hour (1 hour) by default)
  - redirection to an external URL such as a third-party Captive Portal vendor page
- WEP for wireless security. WEP is available when the radio mode is 'legacy', the radios are using vap0, and radio 1 is set to 802.11bg and radio 2 is set to 802.11a. Only use WEP if you can't use WPA Personal, WPA Enterprise, or WPA3.

Setting the lifetime of X.509 certificates

Applies to all AlliedWare Plus devices

From version 5.5.3-2.1 onwards, you can specify the lifetime of self-signed X.509 certificates as part of configuring the trustpoint. You can specify the certificate lifetime in days (1-1825), months (1-60) or years (1-5).

To do this, use the following new command in Trustpoint Configuration mode for a trustpoint:

```
awplus(ca-trustpoint)# lifetime {days <1-1825>|months <1-60>|
years <1-5>}
```

The default lifetime is unchanged at 5 years.

Note that this change does not apply to the default self-signed certificate generated by each AlliedWare Plus device when it is first booted up (named 'default-selfsigned'). The lifetime for that certificate will remain at 50 years.

The default certificate is used by various applications when they first start up. If you need to use a shorter certificate lifetime for any of those applications, create a trustpoint with the appropriate lifetime and apply it to the application, using the commands:

- For the web-based device GUI: http trustpoint <*trustpoint-name*>
- For web-based authentication: auth-web-server trustpoint <*trustpoint-name*>
- For device discovery using STOAT: stoat collector trustpoint <*trustpoint-name*>
- For wireless: trustpoint <*trustpoint-name*>
(use in Wireless Configuration mode)

For more information, see the Public Key Infrastructure (PKI) Feature Overview and Configuration Guide.

Disable local RADIUS server users

Applies to all devices that support the local RADIUS server

From version 5.5.3-2.1 onwards, you can disable and re-enable users in the device’s local RADIUS server. This means you can prevent users from authenticating through the local RADIUS server without deleting their settings in the server, which is useful if you need to temporarily disable them, for example.

To disable a user, use the following new command:

```
awplus(config-radsrv)# user <name> reject
```

To enable the user again, use the following new command:

```
awplus(config-radsrv)# no user <name> reject
```

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

See the last tunnel connection time for OpenVPN tunnel users

Applies to all devices that support OpenVPN

From version 5.5.3-2.1 onwards, you can see the last tunnel connection time for users of OpenVPN tunnels. To display this, use the following new command:

```
awplus# show tunnel connections history
```

The last connection time is shown in local time.

```
awplus#show tunnel connections history
Interface: tunnel0

Username                                                    Last connection time
--------------------------------------------------------------------------------
user_a                                                      2023-09-01 10:31:09
```

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

Passwords are now displayed in encrypted form in running configuration

Applies to all AlliedWare Plus devices

From version 5.5.3-2.1 onwards, a number of features will now have their passwords displayed in running configuration in encrypted form, instead of in plain text. For example, if you enter the following CLI command:

```
radius-server key <cleartext>
```

It will be displayed in running configuration as:

```
radius-server key <ciphertext> encrypted
```

The **encrypted** parameter shows that the password is encrypted. Do not use this parameter when you enter a password in the CLI.

If you need to display the passwords in unencrypted form, use the new command:

```
awplus# show running-config unencrypted
```

This command can only be entered by users with privilege level 15.

OSPFv3 support for VRF-lite with IPv6

Available on products that support VRF-lite: SBx8100, SBx908 GEN2, x950, x930, and x530 Series switches and AR-Series firewalls (except AR1050V)

From version 5.5.3-2.1 onwards, VRF-lite support with IPv6 includes support for OSPFv3.

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

Support for AR4000S-Cloud on more virtual environments

From version 5.5.3-2.1 onwards, AR4000S-Cloud can be deployed on:

- Microsoft Azure
- Oracle Cloud

For more information, see the appropriate AR4000S-Cloud Installation Guide.

Increase to log storage size on virtual platforms

From version 5.5.3-2.1 onwards, the sizes of the buffered and permanent logs have been increased.

On AMF Plus Cloud and AR4000S-Cloud, the sizes have increased to:

- maximum: 50 MB
- default: 5 MB

The increased default size only applies to virtual platforms with at least 4GB RAM for the buffered log and 4GB flash for the permanent log.

On VST-APL, VST-VRT and the 10G UTM Firewall, the sizes have increased from 50KB to 5MB. It is not possible to change the size on these platforms.

For more information about logging, see the Logging Feature Overview and Configuration Guide.

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that may affect your device or network behavior if you upgrade:

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

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

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

Please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.2-2.x version, please check the 5.5.3-0.x and 5.5.3-1.x release notes. Release notes are available from our website, including:

- 5.5.3-1.x release notes
- 5.5.3-0.x release notes
- 5.5.2-x.x release notes
- 5.5.1-x.x release notes
- 5.5.0-x.x release notes
- 5.4.9-x.x release notes
- 5.4.8-x.x release notes
- 5.4.7-x.x release notes
- 5.4.6-x.x release notes

Web Control interface matching no longer supported on 10GbE UTM Firewall

From version 5.5.3-2.1 onwards, interface matching in Web Control is not supported in the Firewall app on the 10GbE UTM Firewall.

In a web control entity configuration like the one below, the **interface eth** portion of the **ip subnet** command will have no effect.

```
awplus(config-web-control)#exit
awplus(config)#zone private
awplus(config)#network engineering
awplus(config-network)#ip subnet 192.168.1.0/24 interface eth1
```

If you configure a rule using the **rule (web control)** command, the device generates this CLI and log message:

```
% Entity "private.engineering" contains interface matches - only
the subnet portion is used by Web Control
```

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 26 and "Details for x930 Series" on page 26 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.

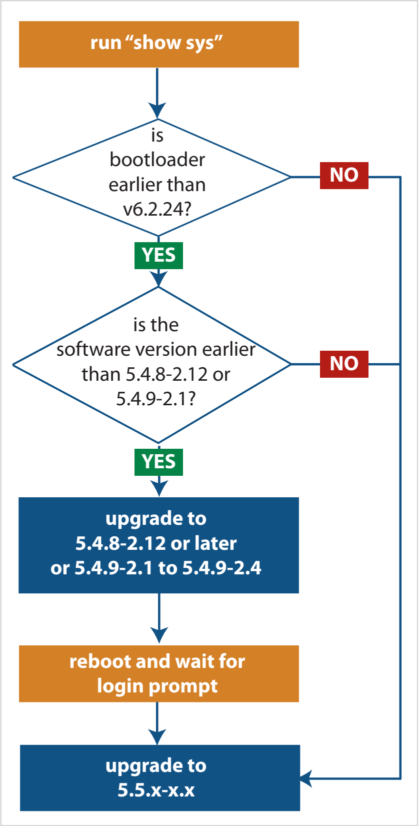
Instead, before upgrading from one of those versions to 5.5.0-0.1 or later, make sure your switch is running one of these specified versions:

- 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
```


run “show sys”
is bootloader earlier than v6.2.24?
NO
YES
is the software version earlier than 5.4.8-2.12 or 5.4.9-2.1?
NO
YES
upgrade to 5.4.8-2.12 or later or 5.4.9-2.1 to 5.4.9-2.4
reboot and wait for login prompt
upgrade to 5.5.x-x.x

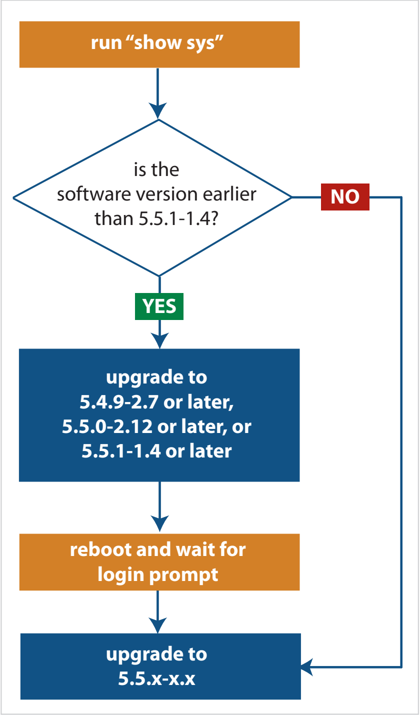
Details for x930 Series

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.


run “show sys”
is the software version earlier than 5.5.1-1.4?
NO
YES
upgrade to 5.4.9-2.7 or later, 5.5.0-2.12 or later, or 5.5.1-1.4 or later
reboot and wait for login prompt
upgrade to 5.5.x-x.x

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

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

```
awplus# show system
```

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.3 license on your switch if you are upgrading to 5.5.3-x.x on your SBx908 GEN2 or SBx8100 switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- “Licensing this Version on an SBx908 GEN2 Switch” on page 31 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 33.

Upgrading a VCStack with rolling reboot

Applies to all stackable AlliedWare Plus switches, except SBx8100

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

For SBx908 GEN2, x950 and x550 Series switches

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

- All versions from 5.5.0-x.x onwards

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

For x530 Series switches using DAC to stack

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

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

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

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

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

To use rolling reboot

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

Forming or extending a VCStack with auto-synchronization

Applies to all stackable AlliedWare Plus switches

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

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

For SBx908 GEN2, x950 and x550 Series switches

Auto-synchronization is supported between this version and:

- All versions from 5.5.0-x.x onwards

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

For CFC960 cards in an SBx8100 system

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

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

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

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

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

For x530 Series switches using DAC to stack

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

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

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

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

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

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

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

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

Upgrading all devices in an AMF network

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
    a. create a working-set of the nodes you want to upgrade
    b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
    c. Check the console messages to make sure that all nodes are “release ready”. If they are, follow the prompts to perform the upgrade.

Obtaining User Documentation

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

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

Verifying the Release File

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

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

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

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

Caution

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

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

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

Table: Hash values

Product family	Software File	Hash
AMF Cloud-	vaa-5.5.3-2.3.rel	927e31e032db8e6a44a6c6687d030f3b6e02ea4b4e87a2eb0146e62827ab1137
SBx8100-	SBx81CFC960-5.5.3-2.3.rel	fa0e8fb01b4672f1dd972a547833588e8c36c6410cc0d1dbb7ec6d45ca461241
SBx908 GEN2-	SBx908NG-5.5.3-2.3.rel	d6c40a9397cc51cd28d6b674738a95d78c3267ac6c94ea7922bae5ca3d8c6213
x950-	x950-5.5.3-2.3.rel	d6c40a9397cc51cd28d6b674738a95d78c3267ac6c94ea7922bae5ca3d8c6213
x930-	x930-5.5.3-2.3.rel	ea751e18c61cad156eab7fc01e2dcca27259c70d06322925dac4522dcf3b0af7
x550-	x550-5.5.3-2.3.rel	51557ddea291989265f57163065c4242c90fec12cb11bbe53ff231ee460e5a12
x540L-	x540-5.5.3-2.3.rel	3198e77bc3796c8b311fd7968ef1b253c707927add70c49f2ea3bcd70c5001b5
x530 & x530L-	x530-5.5.3-2.3.rel	8be66142cddc9305899226fbd30edc5342d6d77460b4795f7089cf4551d18821

Table: Hash values

Product family	Software File	Hash
x330	x330-5.5.3-2.3.rel	df38487cd2a8dc815f41be5f65e3e38a0281a9e9e1c08c4437ed99bcb1e80c1f
x320	x320-5.5.3-2.3.rel	8be66142cddc9305899226fbd30edc5342d6d77460b4795f7089cf4551d18821
x250	x250-5.5.3-2.3.rel	b72fdf062a66761424b6c0730aca477336f94652d27c433872c55dca99a7854a
x230 & x230L	x230-5.5.3-2.3.rel	2ac014a18f974322a3d0775b5cb794024c17873cd8f92766d60c1209abe288cf
x220	x220-5.5.3-2.3.rel	cba39f7492f7e03c8e62203368b864b4133638d7228bd69ee3c53671ad5a1798
IE340 & IE340L	IE340-5.5.3-2.3.rel	097fa102de6cdccde89c80e86c83f844b6700f5ff9cdb5d81e0cb3d3483e24b0
IE220	IE220-5.5.3-2.3.rel	ca70a03fb27d96214586c28db9d7994d34c17dbcbd50da81a1f7f870e36724b3
IE210L	IE210-5.5.3-2.3.rel	2ac014a18f974322a3d0775b5cb794024c17873cd8f92766d60c1209abe288cf
XS900MX	XS900-5.5.3-2.3.rel	a84c9c2c3b316ba0a0c90b77b5e838471ef4912965c643dd746ed07cd0ca40c0
GS980MX	GS980MX-5.5.3-2.3.rel	8be66142cddc9305899226fbd30edc5342d6d77460b4795f7089cf4551d18821
GS980EM	GS980EM-5.5.3-2.3.rel	8be66142cddc9305899226fbd30edc5342d6d77460b4795f7089cf4551d18821
GS980M	GS980M-5.5.3-2.3.rel	cba39f7492f7e03c8e62203368b864b4133638d7228bd69ee3c53671ad5a1798
GS970EMX	GS970EMX-5.5.3-2.3.rel	df38487cd2a8dc815f41be5f65e3e38a0281a9e9e1c08c4437ed99bcb1e80c1f
GS970M	GS970-5.5.3-2.3.rel	2ac014a18f974322a3d0775b5cb794024c17873cd8f92766d60c1209abe288cf
AR4050S-5G	AR4050S-5.5.3-2.3.rel	2990ffc427566e78981cffb8723ec9b2ce3969f024556141062956e69a4c2de5
AR4050S	AR4050S-5.5.3-2.3.rel	2990ffc427566e78981cffb8723ec9b2ce3969f024556141062956e69a4c2de5
AR3050S	AR3050S-5.5.3-2.3.rel	2990ffc427566e78981cffb8723ec9b2ce3969f024556141062956e69a4c2de5
AR1050V	AR1050V-5.5.3-2.3.rel	0d6a793a6cab94d10030213f13d756e37c29e3be2ffbab1fef492c8aac6c37df
TQ6702 GEN2-R	TQ6702GEN2R-5.5.3-2.3.rel	b8c7692aec881db9a3e2d0b43976baf0a72b94c96b7aacc79d285601fec2b505

Licensing this Version on an SBx908 GEN2 Switch

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

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

1. **Obtain the MAC address for a switch**

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

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

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

2. Obtain a release license for a switch

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

3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

```
awplus#show license

Board region: Global

Index                         : 1
License name                  : Base License
Customer name                 : Base License
Type of license               : Full
License issue date            : 30-Mar-2023
Features included             : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                                EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                                L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                                RADIUS-100, RIP, VCStack, VRRP

Index                         : 2
License name                  : 5.5.3
Customer name                 : ABC Consulting
Quantity of licenses          : 1
Type of license               : Full
License issue date            : 20-Aug-2023
License expiry date           : N/A
Release                       : 5.5.3
```

Licensing this Version on an SBx8100 Series CFC960 Control Card

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

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

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

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

1. Obtain the MAC address for a control card

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

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

```
awplus#show system mac license

MAC address for licensing:

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

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

2. Obtain a release license for a control card

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

3. Apply a release license on a control card

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

```
awplus#show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 30-Mar-2023
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

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

Installing this Software Version

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 31 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 33.

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

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

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

Product	Command
SBx8100 with CFC960	`awplus(config)# boot system SBx8100-5.5.3-2.3.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.3-2.3.rel`
x950 series	`awplus(config)# boot system x950-5.5.3-2.3.rel`
x930 series	`awplus(config)# boot system x930-5.5.3-2.3.rel`
x550 series	`awplus(config)# boot system x550-5.5.3-2.3.rel`
x540L series	`awplus(config)# boot system x540-5.5.3-2.3.rel`
x530 series	`awplus(config)# boot system x530-5.5.3-2.3.rel`
x330 series	`awplus(config)# boot system x330-5.5.3-2.3.rel`
x320 series	`awplus(config)# boot system x320-5.5.3-2.3.rel`
x250 series	`awplus(config)# boot system x250-5.5.3-2.3.rel`
x230 series	`awplus(config)# boot system x230-5.5.3-2.3.rel`
x220 series	`awplus(config)# boot system x220-5.5.3-2.3.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.3-2.3.rel`

Product	Command
IE220 series	`awplus(config)# boot system IE220-5.5.3-2.3.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.3-2.3.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.3-2.3.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.3-2.3.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.3-2.3.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.3-2.3.rel`
GS970EMX series	`awplus(config)# boot system GS970EMX-5.5.3-2.3.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.3-2.3.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.3-2.3.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.3-2.3.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.3-2.3.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.3-2.3.rel`
TQ6702 GEN2-R	`awplus(config)# boot system TQ6702GEN2R-5.5.3-2.3.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

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

Perform the following steps to browse to the GUI.

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

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

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

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

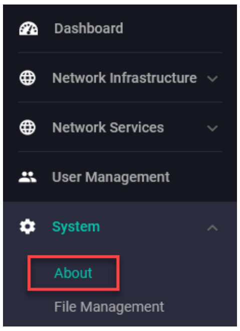
2. Open a web browser and browse to the IP address from step 1.

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

Check the GUI version

To see which version you have, open the **System** > **About** page in the GUI and check the field called **GUI version**. The version to use with 5.5.3-2.3 is 2.16.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 38 or "Update the GUI on AR-Series devices" on page 39.



Update the GUI on switches

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

1. Obtain the GUI file from our Software Download center. The GUI filename to use with AlliedWare Plus v5.5.3-2.x is awplus-gui_553_31.gui.

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

2. Log into the GUI:

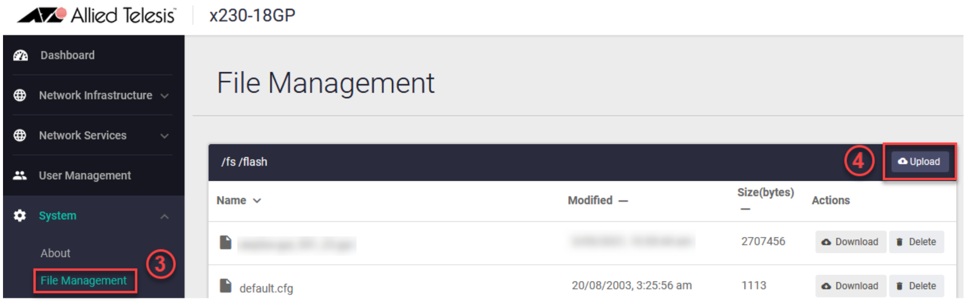
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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

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

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

4. Click **Upload**.



Name	Modified	Size(bytes)	Actions
[redacted]	[redacted]	2707456	Download Delete
default.cfg	20/08/2003, 3:25:56 am	1113	Download Delete

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.

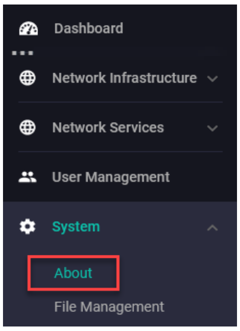
Perform the following steps if you have been running an earlier version of the GUI and need to update it.

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 v2.16.0 or later.


Dashboard
Network Infrastructure
Network Services
User Management
System
About
File Management