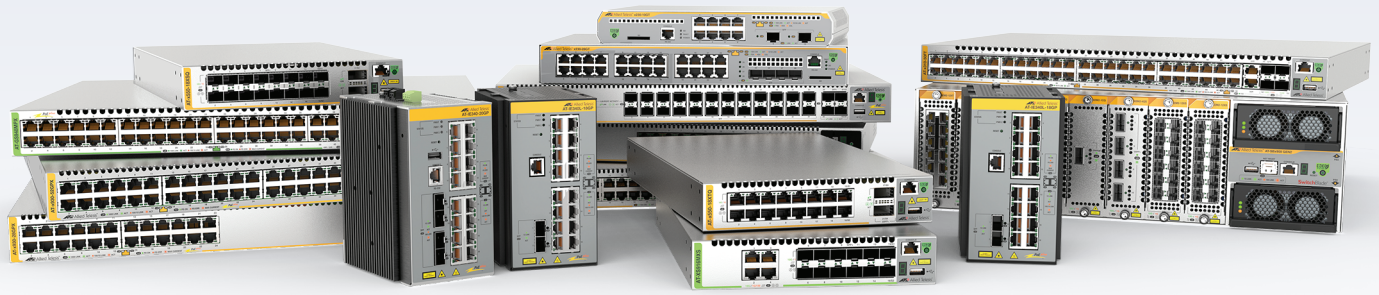
Release Note for AlliedWare Plus Software Version 5.5.4-1.x



AlliedWare Plus OPERATING SYSTEM

AMF Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x240 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE240 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

» 5.5.4-1.1 » 5.5.4-1.2 » 5.5.4-1.5 » 5.5.4-1.6 » 5.5.4-1.7

Acknowledgments

Getting the most from this Release Note

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

Content

What's New in Version 5.5.4-1.7

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
X540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series*
SE240L Series*
SE240 Series*
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ6702 GEN2-R

1. * Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-1.7.

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 47.

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 current datecurrent datefor this version:

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		01/2025	vaa-5.5.4-1.7.iso (VAA OS) vaa-5.5.4-1.7.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-1.7.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	01/2025	SBx81CFC960-5.5.4-1.7.rel
SBx908 GEN2	SBx908 GEN2	01/2025	SBx908NG-5.5.4-1.7.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	01/2025	x950-5.5.4-1.7.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	01/2025	x930-5.5.4-1.7.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	01/2025	x550-5.5.4-1.7.rel
x540L-28XTm x540L-28XS	x540L	01/2025	x540-5.5.4-1.7.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	01/2025	x530-5.5.4-1.7.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	01/2025	x330-5.5.4-1.7.rel
x320-10GH x320-11GPT	x320	01/2025	x320-5.5.4-1.7.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	01/2025	x240-5.5.4-1.7.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	01/2025	x230-5.5.4-1.7.rel
x220-28GS x220-52GT x220-52GP	x220	01/2025	x220-5.5.4-1.7.rel

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

Models	Family	Date	Software File
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	01/2025	IE340-5.5.4-1.7.rel
IE220-6GHX IE220-10GHX	IE220	01/2025	IE220-5.5.4-1.7.rel
IE210L-10GP IE210L-18GP	IE210L	01/2025	IE210-5.5.4-1.7.rel
SE540L-28XTm SE540L-28XS	SE540L	01/2025	SE540-5.5.4-1.7.rel
SE250-18XTm SE250-28XTm SE250-28XS	SE250	01/2025	SE250-5.5.4-1.7.rel
SE240-10GTXm SE240-10GHXm	SE240	01/2025	SE240-5.5.4-1.7.rel
XS916MXT XS916MXS	XS900MX	01/2025	XS900-5.5.4-1.7.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	01/2025	GS980MX-5.5.4-1.7.rel
GS980EM/10H GS980EM/11PT	GS980EM	01/2025	GS980EM-5.5.4-1.7.rel
GS980M/52 GS980M/52PS	GS980M	01/2025	GS980M-5.5.4-1.7.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	01/2025	GS970EMX-5.5.4-1.7.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	01/2025	GS970-5.5.4-1.7.rel
AR4000S-Cloud		01/2025	AR-4000S-Cloud-5.5.4-1.7.iso
10GbE UTM Firewall		01/2025	ATVSTAPL-1.9.3.iso and vfw-x86_64-5.5.4-1.7.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	01/2025	AR4050S-5.5.4-1.7.rel AR3050S-5.5.4-1.7.rel
AR1050V	AR-Series VPN routers	01/2025	AR1050V-5.5.4-1.7.rel
TQ6702 GEN2-R	Wireless AP Router	01/2025	TQ6702GEN2R-5.5.4-1.7.rel

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

The 5.5.4-1.7 software version is ISSU compatible with previous software versions.

New features and Enhancements

Stricter process control

Available on all AlliedWare Plus devices

CR-77554 This software update provides a new feature where edit, activate and several other associated commands have more strict process control. Shell scripts are now prevented from accessing certain sensitive system files, and the edit command is also prevented from accessing sensitive system files.

File and directory manipulation commands, show file commands, copy, move, delete file commands, show command redirections, and trigger scripting may also be put under strict user process control.

The affected commands and command types are:

- activate <script-name>
- copy [force] <source-name> <destination-name>
- copy FILE zmodem
- copy FILE startup-config
- copy current-software FILE
- copy running-config FILE
- copy startup-config FILE
- copy buffered-log FILE
- copy permanent-log FILE
- delete FILE
- edit (FILE|)
- move <source-name> <destination-name>
- mkdir FILE
- rmdir FILE
- show file FILE
- show commands with output redirection
- trigger running shell scripts

New command In order to maintain backward compatibility, the functionality is disabled by default and enabled using a new command. This command prompts for a new password before it takes effect. This password is then required in order to disable the functionality. Privileged system managers will not be able to access sensitive system files without access to this password.

The new command is:

```
awplus(config)# (no) strict-user-process-control
```

Command usage

When the command is configured to enable the feature it will prompt for a password and a password confirmation. A new password, separate from any existing privileged management passwords, should be entered. This password should be stored carefully and securely as it will be required to disable the feature using the 'no' form of the command.

This command must be entered from a physical console. Adding/deleting the 'strict-user -process- control ' command to/from saved configuration file will not affect the running status of the feature. For additional security, entering the command from a remote login session is not allowed.

Use the command **show running-config** to confirm the status of the feature. If the feature is running, the output will contain the command **strict-user-process-control**.

ISSU: Effective when CFCs upgraded

Issues Resolved in Version 5.5.4-1.7

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

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340\IE340L	SE540L	SE250	SE240L	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-64117	**AMF**	Previously, long CLI commands (in excess of 319 characters) via AMF would fail to be executed on remote nodes. 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-82953	**AMF**	Previously, when multiple AMF guest nodes were connected using 'agent' discovery, and static addresses within the same subnet, Layer 3 communication issues could result which would impact the ability to perform AMF auto recovery. 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	Y
CR-85200	**AMF**	Previously, executing 'show' commands within a working-set that generated verbose output could result in incomplete output when traffic was actively being processed. 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	Y

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340\IE340L	SE540L	SE250	SE240L	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-83935	**ARP, Neighbor Discovery**	Previously, when Proxy ARP, Local Proxy ARP or Limited Local Proxy ARP was configured on an interface, there was no validity checking done on the source IP of ARP requests received on the interface. Now, when any of these features are enabled, ARP requests are checked to see if the source address matches the subnet of one of the addresses configured on that interface. If it does not, the ARP request is dropped. 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
CR-82331	**CLI, AMF**	Previously, AMF agent links were not being removed when using the command: **`no switchport atmf-agentlink`** This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y
CR-85429	**CLI, AMF**	Previously, on a device configured for AMF which also had **`security-password forced-change`** enabled, if an SSH or Telnet connection was terminated while a password change was in progress, after approximately 10 minutes the device could experience an unnecessary system reboot. 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	Y
CR-85696	**Device Security**	This software change enhances the **`strict-user-process-control`** command, providing tighter control over internal processes and enforcing stricter access restrictions to files intended for internal use only. 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	Y

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340\IE340L	SE540L	SE250	SE240L	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82923	**EPSR**	Previously, when an EPSR ring transitioned to a 'complete' state after a failure, transit nodes could start receiving traffic on the alternate EPSR port. In some cases, host entries were not correctly updated to reflect the old port, causing traffic to be forwarded through the wrong interface. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-85199	**Firewall**	Previously, when moving an ICMP/ICMPv6 firewall rule to a different identifier, an error message would appear, and the rule would be duplicated, leaving two copies at both the old and new identifiers. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y
CR-83972	**Firewall, VRF-Lite**	Previously, using firewall rules inside a named VRF could result in traffic generated by the router for this VRF to be discarded. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–
CR-85024	**Flow Control**	Previously, flow control was incorrectly enabled on copper combo ports on the x930-GSTX which were link up during switch boot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-85390	**IPV6 Neighbour discovery**	Previously, if a router was booted with the command: **`tunnel provision upstream-interface`** configured on a VAP interface, the command was rejected during config replay. This was due to the tunnel configuration being executed before the VAP interface had been created. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340\IE340L	SE540L	SE250	SE240L	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-84950	**Logging**	Previously, when logging parity errors, it was possible for the device to undergo a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-85215	**MAC authentication, 802.1x Authentication**	Previously, two-step authentication could fail when the auth order was ***auth-mac*** followed by ***dot1x***. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y
CR-84250	**MLD Snooping**	Previously, there was an issue which caused IPv6 multicast traffic to be flooded. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–
CR-84414	**PIM-DM v4, Multicast Routing**	Previously, in rare cases, it was possible for a system reboot to occur when processing very large numbers of port state changes. For example, when multiple ports were flapping. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–	–
CR-82935	**PIM-SM**	Previously, multicast packets could be lost during multicast route updates. This issue has been resolved.	Y	Y	–	–	–	Y	Y	Y	–	–	–	–	Y	–	–	–	Y	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-83464	**PIM, VCStack**	Previously, in rare cases, it was possible for the PIMv6 background process to fail during a VCStack failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340\IE340L	SE540L	SE250	SE240L	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82949	**PIM. L3 Multicast**	When multicast join/leave operations were done synchronously among stack members using the command "platform sync-mc-ops" introduced under CR-82036, occasionally an error log message "ERROR: The multicast index does not exist" might be produced by the system. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-85302	**Pluggable Transcievers**	Previously, on rare occasions a pluggable transceiver could fail to link up after re-powering the device.	Y	Y	–	–	–	Y	Y	Y	–	–	–	–	Y	–	–	–	Y	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-83874	**PTP**	Previously, on switches supporting PTP, PTPv1, traffic could be dropped if it ingressed a port configured as a 'clock-port'. This issue has been resolved.	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–		–	–	–	–	Y	Y	–	–	Y	–	–	–	–	–	–
CR-85450	**QoS HW**	Previously, the egress queue drop and transmit counters specifically for port1.0.3 was showing incorrect values, as output by the command: **`show mls qos interface port1.0.3 queue-counters`** This was due to those counters being incorrectly mapped to another port on the switch. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-84379	**SSL**	This software update addresses the SSL vulnerabilities stated in CVE-2023-6129 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-84037	**Switching**	Previously, when a 5G port linked up, in some instances it would report an error and no longer pass traffic until the device was rebooted. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	Y	–	–	Y	Y	–	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M/GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340\IE340L	SE540L	SE250	SE240L	x220	x230, x230L	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-85542	**Unicast Routing**	Previously, in some situations it was possible for an ECMP entry to fail to be written to the hardware table. This resulted in traffic loss and an error message being generated. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-84890	**VCStack, LACP**	Previously, audit inconsistencies could occur for dynamic LACP interfaces when a backup member containing a member port of the dynamic aggregator rejoined the VCStack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	Y	–	–	–	–	–
CR-82806	**VCStack, Multicast Routing**	Previously, following a VCStack failover on affected platforms, some multicast traffic loss could be seen while the backup member was syncing. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–

What's New in Version 5.5.4-1.6

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
x240 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ6702 GEN2-R

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-1.6.

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 47.

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		11/2024	vaa-5.5.4-1.6.iso (VAA OS) vaa-5.5.4-1.6.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-1.6.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	11/2024	SBx81CFC960-5.5.4-1.6.rel
SBx908 GEN2	SBx908 GEN2	11/2024	SBx908NG-5.5.4-1.6.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	11/2024	x950-5.5.4-1.6.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	11/2024	x930-5.5.4-1.6.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2024	x550-5.5.4-1.6.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	11/2024	x530-5.5.4-1.6.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	11/2024	x330-5.5.4-1.6.rel
x320-10GH x320-11GPT	x320	11/2024	x320-5.5.4-1.6.rel
x240-10GTXm x240-10GHXm	x240	11/2024	x240-5.5.4-1.6.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	11/2024	x230-5.5.4-1.6.rel
x220-28GS x220-52GT x220-52GP	x220	11/2024	x220-5.5.4-1.6.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	11/2024	IE340-5.5.4-1.6.rel
IE220-6GHX IE220-10GHX	IE220	11/2024	IE220-5.5.4-1.6.rel

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

Models	Family	Date	Software File
IE210L-10GP IE210L-18GP	IE210L	11/2024	IE210-5.5.4-1.6.rel
SE240-10GTXm SE240-10GHXm	SE240	11/2024	SE240-5.5.4-1.6.rel
XS916MXT XS916MXS	XS900MX	11/2024	XS900-5.5.4-1.6.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	11/2024	GS980MX-5.5.4-1.6.rel
GS980EM/10H GS980EM/11PT	GS980EM	11/2024	GS980EM-5.5.4-1.6.rel
GS980M/52 GS980M/52PS	GS980M	11/2024	GS980M-5.5.4-1.6.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	11/2024	GS970EMX-5.5.4-1.6.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2024	GS970-5.5.4-1.6.rel
AR4000S-Cloud		11/2024	AR-4000S-Cloud-5.5.4-1.6.iso
10GbE UTM Firewall		11/2024	ATVSTAPL-1.9.3.iso and vfw-x86_64-5.5.4-1.6.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	11/2024	AR4050S-5.5.4-1.6.rel AR3050S-5.5.4-1.6.rel
AR1050V	AR-Series VPN routers	11/2024	AR1050V-5.5.4-1.6.rel
TQ6702 GEN2-R	Wireless AP Router	11/2024	TQ6702GEN2R-5.5.4-1.6.rel

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

The 5.5.4-1.6 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.4-1.6

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

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340/IE340L	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-83599	**Device GUI, Web API**	This update allows users to make sure that all the Web-GUI HTTP/HTTPS requests coming into the device have the expected Content-Type HTTP header set to 'application/json'. This ensures more secure HTTP request processing by the device. ■ By default, the checking is disabled. To enable the checking, and ensure that all the Web-GUI HTTP/HTTPS requests coming into the device have the expected Content-Type HTTP header set to 'application/json', use the command: **http check-content-type-header** ■ We recommend that HTTP header checking is enabled. However, to enable this feature, you must load a Web-GUI file version newer than release 2.18.0 onto the device. ■ To show the status of the Web-GUI HTTP/HTTPS requests header checking, use the command: **show http** ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-82188	**Device Security**	Previously, strong password rules were only enforced on privileged users. Now, the same password check is done for all users regardless of privilege levels. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340/IE340L	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-84302	**Logging**	With this software version, additional log messages have been added to CLI handlers. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-84502	**Port Authentication**	Previously, when a supplicant roamed from port A to port B, the count of tagged and untagged supplicants was not updated correctly on port A. 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-82431	**RADIUS**	Previously, the AlliedWare Plus local RADIUS server did not support TLSv1.3. Support for TLSv1.3 has now been added. 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-84010	**Telnet**	Previously, unprivileged users could access SSH and Telnet clients in **crypto secure-mode**. This has been modified so that only privileged users are allowed to use SSH and Telnet clients when crypto secure-mode is enabled. ISSU: Effective when CFCs upgraded	–	–	Y	–	–	–	Y	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–

What's New in Version 5.5.4-1.5

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x240 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ6702 GEN2-R

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-1.5.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 47.

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		10/2024	vaa-5.5.4-1.5.iso (VAA OS) vaa-5.5.4-1.5.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-1.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2024	SBx81CFC960-5.5.4-1.5.rel
SBx908 GEN2	SBx908 GEN2	10/2024	SBx908NG-5.5.4-1.5.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	10/2024	x950-5.5.4-1.5.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	10/2024	x930-5.5.4-1.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2024	x550-5.5.4-1.5.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	10/2024	x530-5.5.4-1.5.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	10/2024	x330-5.5.4-1.5.rel
x320-10GH x320-11GPT	x320	10/2024	x320-5.5.4-1.5.rel
x240-10GTXm x240-10GHXm	x240	10/2024	x240-5.5.4-1.5.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2024	x230-5.5.4-1.5.rel
x220-28GS x220-52GT x220-52GP	x220	10/2024	x220-5.5.4-1.5.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	10/2024	IE340-5.5.4-1.5.rel
IE220-6GHX IE220-10GHX	IE220	10/2024	IE220-5.5.4-1.5.rel

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

Models	Family	Date	Software File
IE210L-10GP IE210L-18GP	IE210L	10/2024	IE210-5.5.4-1.5.rel
SE240-10GTXm SE240-10GHXm	SE240	10/2024	SE240-5.5.4-1.5.rel
XS916MXT XS916MXS	XS900MX	10/2024	XS900-5.5.4-1.5.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	10/2024	GS980MX-5.5.4-1.5.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2024	GS980EM-5.5.4-1.5.rel
GS980M/52 GS980M/52PS	GS980M	10/2024	GS980M-5.5.4-1.5.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	10/2024	GS970EMX-5.5.4-1.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2024	GS970-5.5.4-1.5.rel
AR4000S-Cloud		10/2024	AR-4000S-Cloud-5.5.4-1.5.iso
10GbE UTM Firewall		10/2024	ATVSTAPL-1.9.3.iso and vfw-x86_64-5.5.4-1.5.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	10/2024	AR4050S-5.5.4-1.5.rel AR3050S-5.5.4-1.5.rel
AR1050V	AR-Series VPN routers	10/2024	AR1050V-5.5.4-1.5.rel
TQ6702 GEN2-R	Wireless AP Router	10/2024	TQ6702GEN2R-5.5.4-1.5.rel

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

The 5.5.4-1.5 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in AlliedWare Plus version 5.5.4-1.5:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 41.

TQ6702 GEN2-R enhancements

For the TQ6702 GEN2-R, AlliedWare Plus version 5.5.4-1.5 onwards supports:

ER-6421 Auto-negotiation to 10M full duplex with a partner advertising 10MFULL on both Ethernet interfaces. Manually fixing speed to 10M full or half-duplex is not supported on Ethernet interfaces.

ER-6288 DoS protection support on the TQ6702 GEN2-R. DoS protection is designed to detect, prevent, or mitigate Denial of Service (DoS) attacks. DoS attacks can include Ping of Death, Smurf, SYN Flood, and Teardrop.

Issues Resolved in Version 5.5.4-1.5

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

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340/IE340L	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-84141	**ACL**	Previously, if a VLAN filter with a large number of entries (e.g. one with many VLANs, VLAN maps, or access-lists) was modified, it could take a long time to process. The long process time could result in a healthcheck failure and a system reboot of the switch. This issue has now been resolved. Now, while the VLAN filter update is being processed, the system will periodically check and process health check messages to allow the command to complete correctly without causing healthcheck failure.	Y	Y	Y	–	–	–	Y	–	Y	–	Y	–	–	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-84131	**ARP, Neighbor Discovery**	Previously, in some cases, flooding next-hop entries for static ARPs on dynamic (LACP) aggregators did not correctly add the entries to hardware. This issue has been resolved.	Y	Y	Y	–	–	–	Y	Y	Y	–	Y	–	–	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-84171	**DHCP Server**	Previously, DHCP could stop working on TQ6702-R APs running AlliedWare plus and using a configuration file containing 30 or more VAP interfaces. This could only occur if interfaces were transitioning between up and down frequently. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340/IE340L	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-84006	**DPI, IDS/IPS, IP Reputation, Web Control**	Previously, when stream-based UTM features (IPS, IP-Rep, DPI, Malware Protection, URL Filtering and Web-control from version 5.5.4-1) were enabled, activity involving data flowing onto or off the device via IPv6 could be slower than equivalent via IPv4. This could include such things as copying files on or off the device, AMF backups and Web-Control (prior to 5.5.4-1). This issue is now resolved, and these operations are performed at equivalent speeds to the same operation via IPv4.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y
CR-83988	**HTTPS Service**	This software update addresses the vulnerability specified in CVE-2023-46724.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y
CR-83354	**PIM-SM**	Previously, on affected VCStacks, following a VCS master failover, some multicast streams could fail to recover. This issue has been resolved	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	–	–	–	–	–	–
CR-84386	**Port Configuration**	Previously, in certain situations it was possible for one or more LIFs (Line Interface Cards) to cause a continuous system reboot on start-up. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–

What's New in Version 5.5.4-1.2

Product families supported by this version:

AMF Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x550 Series
x530 Series
x530L Series
x330 Series
x320 Series
x240 Series
x230 Series
x220 Series
IE340 Series
IE220 Series
IE210L Series
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ6702 GEN2-R

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-1.2.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 47.

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		10/2024	vaa-5.5.4-1.2.iso (VAA OS) vaa-5.5.4-1.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.4-0.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	10/2024	SBx81CFC960-5.5.4-1.2.rel
SBx908 GEN2	SBx908 GEN2	10/2024	SBx908NG-5.5.4-1.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	10/2024	x950-5.5.4-1.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	10/2024	x930-5.5.4-1.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	10/2024	x550-5.5.4-1.2.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530 and x530L	10/2024	x530-5.5.4-1.2.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	10/2024	x330-5.5.4-1.2.rel
x320-10GH x320-11GPT	x320	10/2024	x320-5.5.4-1.2.rel
x240-10GTXm x240-10GHXm	x240	10/2024	x240-5.5.4-1.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	10/2024	x230-5.5.4-1.2.rel
x220-28GS x220-52GT x220-52GP	x220	10/2024	x220-5.5.4-1.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	10/2024	IE340-5.5.4-1.2.rel
IE220-6GHX IE220-10GHX	IE220	10/2024	IE220-5.5.4-1.2.rel

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

Models	Family	Date	Software File
IE210L-10GP IE210L-18GP	IE210L	10/2024	IE210-5.5.4-1.2.rel
SE240-10GTXm SE240-10GHXm	SE240	10/2024	SE240-5.5.4-1.2.rel
XS916MXT XS916MXS	XS900MX	10/2024	XS900-5.5.4-1.2.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	10/2024	GS980MX-5.5.4-1.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	10/2024	GS980EM-5.5.4-1.2.rel
GS980M/52 GS980M/52PS	GS980M	10/2024	GS980M-5.5.4-1.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	10/2024	GS970EMX-5.5.4-1.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	10/2024	GS970-5.5.4-1.2.rel
AR4000S-Cloud		10/2024	AR-4000S-Cloud-5.5.4-1.2.iso
10GbE UTM Firewall		10/2024	ATVSTAPL-1.9.3.iso and vfw-x86_64-5.5.4-1.2.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	10/2024	AR4050S-5.5.4-1.2.rel AR3050S-5.5.4-1.2.rel
AR1050V	AR-Series VPN routers	10/2024	AR1050V-5.5.4-1.2.rel
TQ6702 GEN2-R	Wireless AP Router	10/2024	TQ6702GEN2R-5.5.4-1.2.rel

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

The 5.5.4-1.2 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in AlliedWare Plus version 5.5.4-1.2:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 41.

Stream-based Web Control

Available on: AR-Series UTM firewalls and VPN routers, AR4000-Cloud, and the 10GbE UTM Firewall.

From AlliedWare Plus version 5.5.4-1.2 onwards, stream-based Web Control includes a few small functional changes:

- **No block page for denied HTTP traffic**

Previously, for HTTP traffic, if a Web Control rule denied a request, a notification page would be returned to the web client. This is no longer the case; the request is now simply dropped. This behavior was only ever supported for HTTP traffic. For HTTPS, the request was always just dropped. In practice, the vast majority of web traffic these days is HTTPS, so this change is unlikely to seriously impact customers.

- **Firewall Entities no longer match against interface**

Previously, in Firewall Entities, it was possible to specify an interface along with a particular subnet as part of the network configuration, ensuring it matched a particular subnet traversing a specific interface. Web Control rules included this interface in the match criteria when applying rules. From AlliedWare Plus version 5.5.4-1.1, this interface information is ignored, and only the subnet is used.

You may need to change your configuration if you utilize interface matching, particularly when using a network entity such as **ip subnet 0.0.0.0/0 interface <*interface-name*>**. To achieve equivalent matching, you will need to specify a subnet or multiple subnets that cover the hosts sending traffic through that interface.

- **Bypass rules now match on source and destination**

Previously, bypass rules matched against the destination of web traffic in order to allow traffic to certain remote servers to be exempt from filtering. Now, they can also match against the **source** of web traffic, in order to allow web requests from certain hosts to be exempt from filtering. For example, to create a Web Control bypass for entity 'server.my.box', use the following commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# bypass-web-control server.my.box
```

By default all traffic is processed by Web Control.

NAT64 and DNS64

Available on: AR-Series UTM firewalls and VPN routers, AR4000-Cloud, the 10GbE UTM firewall, and TQ6702 GEN2-R

AlliedWare Plus version 5.5.4-1.2 onward supports NAT64.

The main idea behind NAT64 is it allows providers and customers connected to that provider to be running IPv6 only, yet still be able to connect to IPv4 only services out on other networks such as, of course, the Internet.

Here's how it works:

NAT64 and DNS64 work together to enable an IPv6-only client to communicate with an IPv4-only server.

- **DNS64**: When an IPv6-only client sends a DNS query for an IPv6 address (AAAA record), DNS64 adds a query for the IPv4 address (A record) if necessary. It then translates the IPv4 address from the response into an IPv6 address using a predefined IPv6 prefix, ensuring the client can use an IPv6 address to reach an IPv4-only server.
- **NAT64**: When the client sends packets to the server's IPv6 address, NAT64 translates the IPv6 packet headers into IPv4 packet headers. The server responds with IPv4 packets, and NAT64 translates these back into IPv6 packets for the client.

This combination allows seamless communication between IPv6 clients and IPv4 servers.

New command

There is a new command available with this feature:

```
ip dns forwarding dns64 <map4to6-instance> [translate-all]
```

Configuration example

Let's assume you have a network where you want to enable IPv6-only clients to resolve and access IPv4-only services. You'll configure a DNS64 service with a mapping instance named 'example6to4'.

Basic steps:

1. Configure DNS64 on the Router:
   - « Enable DNS forwarding with DNS64 using the map4to6-instance named 'example6to4'.
2. Define the DNS64 Prefix:
   - « Specify the IPv6 prefix that DNS64 will use to translate IPv4 addresses.
3. Enable NAT64:
   - « Set up NAT64 to handle the translation between IPv6 and IPv4 packets.

Full configuration:

```
zone inet
 network all
  ip subnet 0.0.0.0/0 interface eth2
!
zone lan
 network all
  ip subnet 0.0.0.0/0
!
nat
 rule masq any from lan to inet
 enable
!
4to6-mapping example6to4
  map6to4 subnet 2001:db8::/96 0.0.0.0/0
  map4to6 subnet 0.0.0.0/0 64:ff9b::/96
!
ipv6 dhcp pool lanv6
 address range 2001:db8::192.0.2.100 2001:db8::192.0.2.150
 dns-server 2001:db8::192.0.2.1
!
service dhcp-server
!
interface eth1
 ipv6 address 2001:db8::192.0.2.1/64
 no ipv6 nd suppress-ra
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd dns-server 2001:db8::192.0.2.1
 ipv6 dhcp server lanv6
!
interface eth2
 ip address 203.0.113.1/24
!
interface tunnel0
 tunnel 4to6-mapping example6to4
 tunnel mode map4to6
 ip address 198.51.100.1/32
 ipv6 enable
!
ipv6 forwarding
!
ip route 192.0.2.0/24 tunnel0
!
ipv6 route 64:ff9b::/96 tunnel0
!
ip dns forwarding
ip dns forwarding dns64 example6t
```

For more information, see the Transitioning IPv4 to IPv6 Feature Overview and Configuration Guide.

Support for IPFIX network management standard

Available on: x530 Series switches only

AlliedWare Plus version 5.5.4-1.2 onwards supports the network management standard IPFIX (Internet Protocol Flow Information Export).

IPFIX, as defined by the IETF in RFC 7011, provides a flexible and extensible method for monitoring network traffic. Its primary purpose is to collect data about IP traffic flows for various purposes, including network management, security analysis, and performance monitoring.

In IPFIX, a flow is defined as a set of IP packets passing through an observation point in the network during a certain time interval, which share a set of common properties (e.g., source IP address, destination IP address, source port, destination port, protocol). IPFIX utilizes a template-based approach to define the structure of flow records, allowing customization of the collected data.

Flow records are sent and collected using two main components:

- **Exporter**: A device (such as a router or switch) that collects flow data and sends it to a collector.
- **Collector**: A system that receives flow information from one or more exporters and processes it for analysis.

New commands

The new commands available with this feature are:

```
description(flow exporter)
description(flow monitor)
destination(flow exporter)
exporter(flow monitor)
flow exporter
flow monitor
flow monitor-map
flow record
match ipv4(flow record)
match transport(flow record)
record(flow monitor)
service flow
show flow exporter
show flow monitor
show flow record
show flow
transport(flow exporter)
```

AMF node count increase to 350

Available on: IE340 and IE340L Series switches only

From AlliedWare Plus version 5.5.4-1.2 onwards, the maximum number of AMF member nodes supported in a single area increases from 300 to 350.

Increase Radius Proxy NAS limit to 1000 nodes

Available on: SBx908GEN2

From AlliedWare Plus version 5.5.4-1.2 onwards, the maximum number of Network Access Servers (NAS) supported by RADIUS Proxy is increased to 1000.

VCStacking supported on the x240 Series switch

Available on: x240 Series switches

From AlliedWare Plus version 5.5.4-1.2 onwards, VCStacking is supported on the x240 Series switch (up to two devices).

Stacking is disabled by default, and no stack ports are configured. Any ports can be configured for stacking, but stacking links of different speeds are not supported.

For information on VCStacking and how to configure a stack, see the VCStack Feature Overview and Configuration Guide.

Support for PTP on VCStack and Link Aggregation

Available on: x950, x930, x530/x530L Series, and SBx908 GEN2 switches

AlliedWare Plus version 5.5.4-1.2 onwards supports PTP on VCStack and Link Aggregation.

PTP and Link Aggregation

PTP with Link Aggregation is supported with End-to-End Transparent Clock (E2E TC). PTP accuracy can be compromised when packets traverse different paths in the send and receive directions across an aggregator. With this in mind, there are some considerations to consider to help maintain PTP accuracy:

When PTP packets traverse the switch over an aggregated link, the individual link that the packet is sent on is determined in hardware by the switch chip. For this reason, the characteristics of links used in the aggregated link should be as similar as possible.

For example, all links in the aggregated link should have the same:

- link type, e.g. all fiber
- cable distance

This helps to ensure that PTP packets traversing the aggregated link share similar characteristics in both the TX and RX direction, and in turn helps to minimize error introduced during the PTP calculation.

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

RADIUS local server TLSv1.2

Available on: TQ6702-GEN2-R

AlliedWare Plus version 5.5.4-1.2 onward supports RADIUS local server TLS v1.2 on the TQ6702 GEN2-R.

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

VLAN Translation upgrade

Available on: IE340 and IE340L Series

From AlliedWare Plus version 5.5.4-1.2 onward, the software base license supports VLAN Translation Full. This means that a license is not required and you can now translate more VLANs. The recommended maximum is now 500 VLANs.

Previously, only the VLAN Translation Lite version was supported.

Allow console login on locked accounts

Available on: All AlliedWare Plus devices with a console port

From AlliedWare Plus version 5.5.4-1.2 onwards, it is possible to allow users to login via the physical console port even when the account is locked because of reaching the maximum number of failed remote login attempts.

To allow this, use the command **aaa local authentication attempts max-fail remote-login-only**. This command restricts account lockout only to remote logins (GUI, Telnet, SSH); logins on the physical console (ttyS0) with valid credentials are still allowed.

This command applies to all local users. This command does not interfere with the fail delay mechanism. Brute-force attacks on console logins are still mitigated by the fail delay mechanism.

Example To configure account lock-out to remote login only, use the command:

```
awplus(config)# aaa local authentication attempts max-fail
remote-login-only
```

Removing stability delay on linkup

On some switches, a short delay (500 ms) occurs before sending packets after linkup, to make sure that the link is stable. From version 5.5.4-1.2 onwards, you can remove this delay if necessary. This change applies to the following switches:

- x530 Series
- GS980MX Series
- x240 Series

To remove the delay, use the new command **no linkflap enable-stable-time**. Only remove the delay if it causes network problems, because removing it may cause link flapping. The command is enabled by default.

Example

```
awplus(config)# no linkflap enable-stabel-time
```

Airtime fairness on the TQ6702 GEN2-R

Available on: TQ6702 GEN2-R

Previously, the TQ6702 GEN2-R supported the command **airtime-fairness enable**. This command has been made hidden and when you enter it, it will behave as if you had entered **airtime-fairness mode evenly**.

Anyone using airtime fairness in version 5.5.4-0 or earlier will have their startup configuration accepted and automatically mapped to the command **airtime-fairness mode evenly**.

Airtime fairness is a feature designed to enhance network throughput by fairly distributing airtime among wireless clients. It addresses the issue where older Wi-Fi standards (e.g., 802.11a, g, n) consume more airtime due to slower transmission speeds, impacting overall network efficiency. By enabling airtime fairness, the device's radio allocates airtime proportionally, giving faster clients more airtime and reducing time spent on slower clients.

There are two modes for airtime fairness:

Evenly mode: Airtime is equally divided among Virtual Access Points (VAPs) and then among the clients within each VAP.

Manual mode: You can manually adjust airtime distribution between VAPs, but airtime among clients within each VAP is still evenly split.

Example To configure radio 1 to operate in 'evenly' mode for airtime fairness, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# airtime-fairness mode
evenly
```

Change to default setting for 'platform port-tx-recovery'

Available on: x220, x320, x530, GS980MX, GS980EM, and GS980M Series switches

Previously, when a switch had ports connected at half duplex, there was a chance of an instability issue occurring.

From AlliedWare Plus version 5.5.4-1.2 onwards, to increase stability of switches, the command **platform port-tx-recovery** is enabled by default on the following platforms:

- x220 Series
- x320 Series
- x530 Series
- GS980MX Series
- GS980EM Series
- GS980M Series

You can check whether it is disabled or enabled by looking at the *port-tx-recovery* field in the command **show platform**.

```
awplus#show platform
Routing ratio                 IPv4 and IPv6
Route Weighting               balanced
Load Balancing                src-dst-mac,src-dst-ip
Control-plane-prioritization  Max 1000 Mbps
Fdb-chain-length              8
L2MC overlapped group check   off
port-tx-recovery              on  <<<<------
fdb-l3-hosts mode             Disabled
acls to vlanclassifiers       more-vlan-classifiers
stop-unreg-mc-flooding        off
MC address mismatch action    Drop
Extended ACL VLAN actions     Disabled
Jumboframe support            off
Vlan-stacking TPID            0x8100
Hardware Filter Size          basic
```

You can disable it if necessary by using the command **no platform port-tx-recovery**.

NOTE: This command was first supported in AlliedWare Plus software version 5.5.2-2.

Issues Resolved in Version 5.5.4-1.2

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

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340/IE340L	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-82861	**BFD, BGP**	Previously, a BFD session Down event following a port link down was deleting the BFD session, which could result in incorrect OSPF/BGP neighbour states when the port linked Up again. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR-84064	**CLI**	Previously, the **`show platform port counter`** output was not being included in the **`show tech-support`** output. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y
CR-83675	**Device Security**	Previously, an existing non-privileged user could be promoted to Administrator (Privilege 15) without conforming to strong password settings. This has been addressed by disallowing privilege level promotion to 15 when password requirements are set.	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-83663	**DOS Detection**	Previously, on the x320, DOS rules were triggered on interfaces that were not configured for those rules. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-81763	**HTTP**	This software update addresses the vulnerability specified in CVE-2023-38545 ISSU: This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340/IE340L	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-83417	**ISSU Upgrade**	This maintenance release resolves an issue with ISSU compatibility. Previously, traffic failed to recover after ISSU upgrade from software version 5.5.4-0.2 to 5.5.4-0.3. As a result, traffic flow did not recover, including after rebooting the line-cards. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
CR-83877	**LLDP**	Previously, eth port neighbor information was missing from **`lldp show neighbour`** output on router platforms which include one or more eth ports. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–
CR-81426	**Multicast Routing**	Previously, disabling and re-enabling PIM-SM or PIM-DM after routes were learned could cause traffic loss. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–	–
CR-83958	**OSPFv2**	Previously, during boot, up the software could reject the **`passive-interface tunnel`** command and fail to set a tunnel interface as an OSPF or OSPFv2 passive-interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–
CR-84018	**RIP, RIPng**	Previously, during bootup, the command parameter '*passive-interface*' was rejected, resulting in the corresponding tunnel interface failing to be configured as a RIP or RIP6 passive-interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–
CR-82822	**SNMP**	Previously, under certain extreme conditions, there was a very low probability that the SNMP daemon could cause a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	GS970M	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE200/IE220	IE210L	IE340/IE340L	x220	x230, x230L	x240	x320	x330	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	TQ6702 GEN2-R
CR-83715	**System Logging**	Previously, in rare situations, log messages generated by NSM might be incorrectly dropped by rate-limiting. 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

What's New in Version 5.5.4-1.1

Product families supported by this version: TQ6702 GEN2-R

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.4-1.1.

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

For instructions on how to upgrade to this version, see "Installing this Software Version" on page 47.

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: Model and software file name

Models	Family	Date	Software File
TQ6702 GEN2-R	Wireless AP Router	08/2024	TQ6702GEN2R-5.5.4-1.1.rel

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.4-1.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 41.

AlliedWare Plus enhancements

From version 5.5.4-1.1 onwards, the following AlliedWare Plus features have been added to the TQ6702 GEN2-R Wi-Fi 6 (802.11ax) Wireless AP Router.

GRE over IPv4 and IPv6 - tunneling

Version 5.5.4-1.1 onwards supports standard point-to-point GRE tunnels on the TQ6702 GEN2-R.

GRE is a mechanism for encapsulating any network layer protocol over any other network layer. It allows hosts in one private IP network to communicate with hosts in another private IP network by providing a VPN between two routers across the Internet.

For more information, see the GRE and Multipoint VPNs Feature Overview and Configuration Guide.

Traffic control/QoS

Version 5.5.4-1.1 onwards supports Traffic Control on the TQ6702 GEN2-R. This means that the device supports the same QoS features as the current AR Router series.

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

L2TPv3 Ethernet pseudowire - tunneling

Version 5.5.4-1.1 onwards supports L2TPv3 Ethernet pseudowire tunnel mode on the TQ6702 GEN2-R. L2TPv3 Ethernet Pseudowires can be used to transport Ethernet frames across an IP backbone network, which connects Ethernet LANs together. A pseudowire is an emulation of a point-to-point connection over a Packet Switched Network (PSN).

For more information, see the L2TPv3 Ethernet Pseudowire Feature Overview and Configuration Guide.

Procera support added

Version 5.5.4-1.1 onwards supports Procera's Network Application Visibility Library (NAVL) for the TQ6702 GEN2-R wireless AP router.

Procera is an option available for the Application Control feature. It uses Deep Packet Inspection (DPI) to provide application-specific information based on a client device's activity. Administrators can choose to create rules by using this information to allow or block application traffic to a device.

The license names for using Procera application control on the TQ6702 GEN2-R are as follows:

- AT-TQR-APP-1YR
- AT-TQR-APP-5YR

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

RADIUS local server TLSv1.2

Version 5.5.4-1.1 onwards supports RADIUS local server TLS v1.2 on the TQ6702 GEN2-R.

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

AWC enhancements

From version 5.5.4-1.1 onwards, and using Device GUI version 2.18.0, the following AWC features have been added to the TQ6702 GEN2-R Wi-Fi 6 (802.11ax) Wireless AP Router.

Passpoint

Version 5.5.4-1.1 onwards supports Passpoint™, also known as Hotspot 2.0. Passpoint is the open standard for public Wi-Fi, introduced by the Wi-Fi Alliance™. Passpoint brings seamless, secure Wi-Fi connectivity to any network employing Passpoint enabled Wi-Fi hotspots. It also provides user connections with WPA3™ security.

More Radio mode options

Version 5.5.4-1.1 onwards supports the following additional radio modes and bandwidth options:

Radio modes

- Radio1 - b/g/n
- Radio2 - a/n, a/n/ac

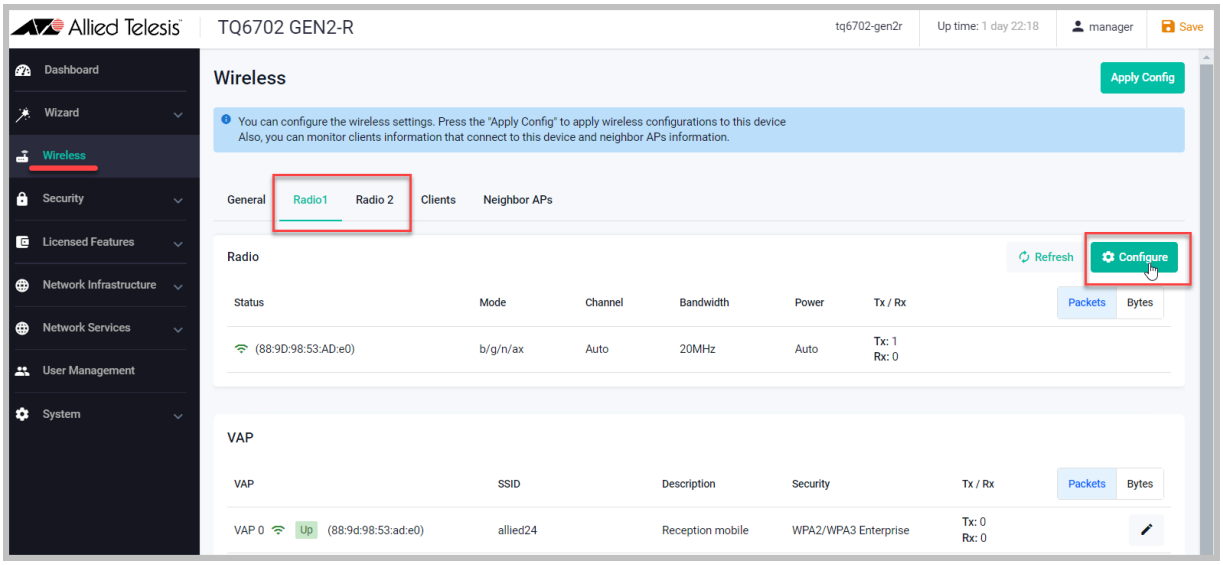
Bandwidth options

Radio1:

- b/g/n: 20 MHz, 40 MHz

Radio2:

- a/n: 20 MHz, 40 MHz
- a/n/ac: 20 MHz, 40 MHz, 80 MHz, 80+80 MHz



The additional radio options and their behavior with MU-MIMO and OFDMA

Both MU-MIMO and OFDMA are used to enhance network performance. They complement each other in this way:

- MU-MIMO handles multiple devices simultaneously.
- OFDMA efficiently divides the channel for those devices.

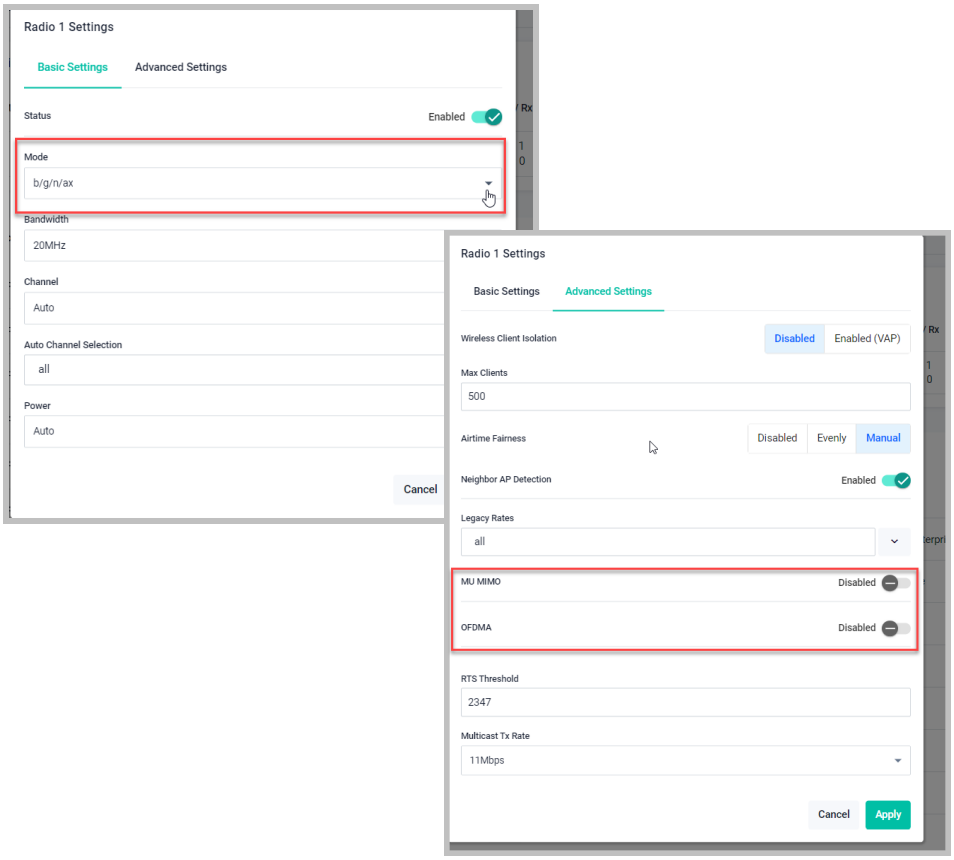
The additional radio mode options (highlighted in red in the table) interact with MU-MIMO and OFDMA as follow:

✓ Can be configured and are displayed in the settings tab

× Can not be configured and are not displayed in the settings tab

Mode	Radio mode						
	Radio 1 (2.4GHz)			Radio2 (5GHz)			
	b/g	b/g/n	b/g/n/ax	a	a/n	a/n/ac	a/n/ac/ax
MU-MIMO	x	x	✓	x	x	✓	✓
OFDMA	x	x	✓	x	x	x	✓

For each radio, the **Mode** settings are located in the Basic Settings tab, while the **MU-MIMO** and **OFDMA** settings are in the Advanced Settings tab.



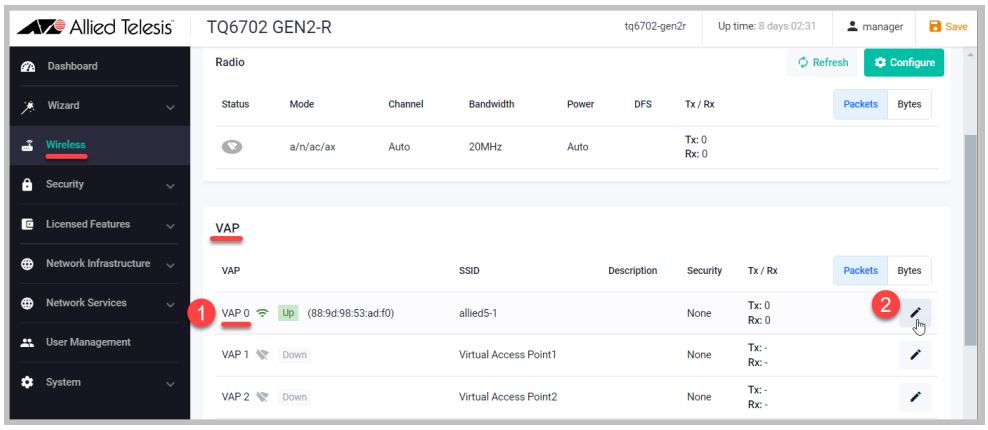
Multicast to Unicast conversion

From version 5.5.4-1.1 onwards, you can configure an Access Point to convert multicast packets into unicast packets destined for the client connected to the VAP. This conversion allows each client to receive data at the highest possible rate it support.

To configure this feature:

1. Select **Wireless** from the left menu, and then select the Radio you want to configure.

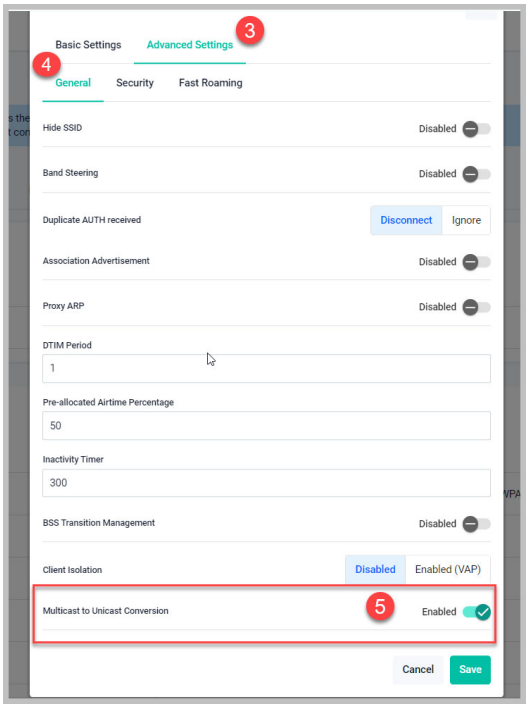
2. Click **Edit** VAP0.



3. Click **Advanced Settings**.

4. Select the **General** tab.

5. Enable **Multicast to Unicast Conversion**.



Airtime Fairness for each VAP

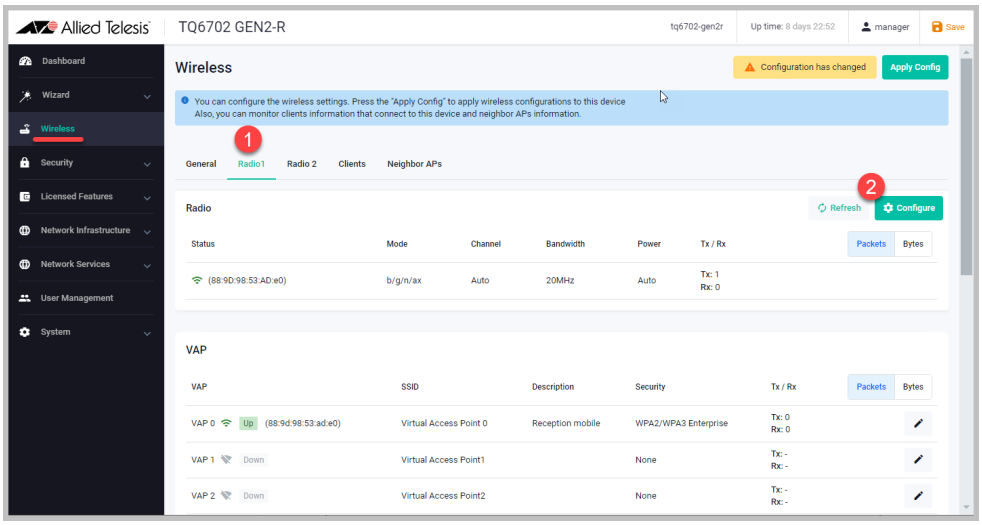
Version 5.4.4-1.1 adds the ability to set each VAP's Airtime Fairness percentage **manually**.

Airtime fairness is a concept and feature designed to ensure that all devices on a wireless network receive a fair share of the available airtime. This is particularly important in environments where devices with varying capabilities and data rates are connected to the same wireless access point.

To set Airtime Fairness to Manually:

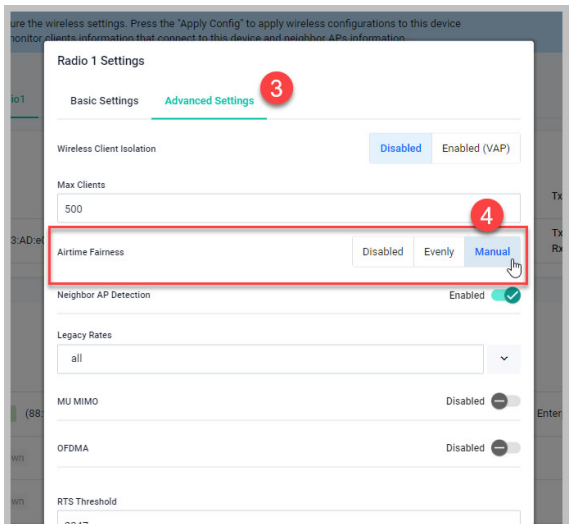
1. Select **Wireless** from the menu on the left, and then select the **Radio** you want to configure.

2. Click **Configure**.



3. Click **Advanced Settings**.

4. Select the desired **Airtime Fairness** setting to **Manual**.

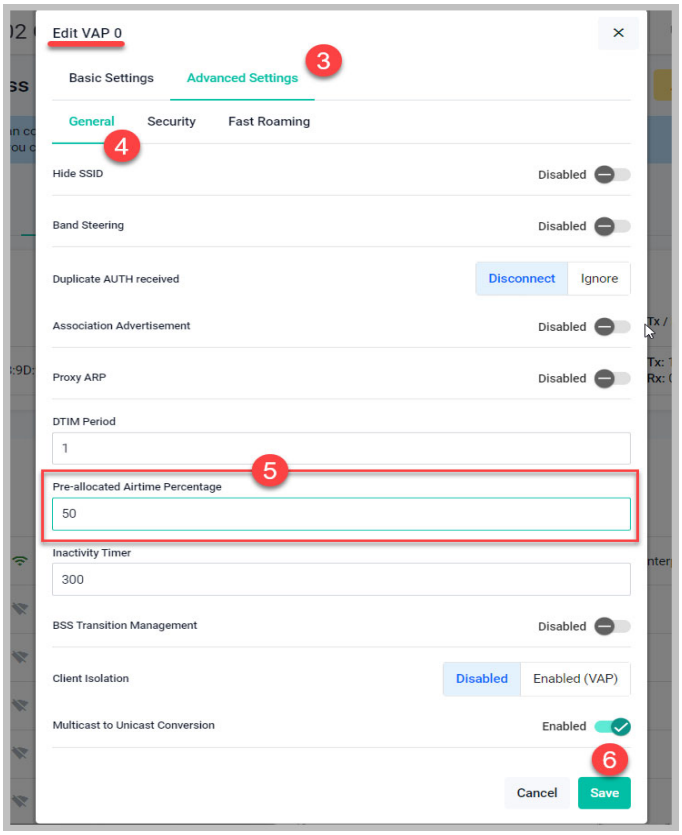


5. Click **Apply**.

You can now configure the VAP's **Pre-allocated Airtime Percentage**.

From the **Wireless** window:

1. Select the **VAP** you want to configure.
2. Click **Edit**.
3. Select **Advanced Settings**.
4. Select **General**.
5. Type in the **Pre-allocated Airtime Percentage** value, for example 50 (percent).
6. Click **Save**.



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
- Changes that may affect device or network configuration

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

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

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

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

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

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

The solution Before upgrading to the latest firmware version, upgrade to one of the specified older versions. See "Details for SBx908 GEN2 and x950 Series" on page 35 and "Details for x930 Series" on page 36 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, switches where the bootloader is older than 6.2.24 are affected. If your bootloader is older than 6.2.24, you **cannot** upgrade to the most recent firmware version directly from:

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

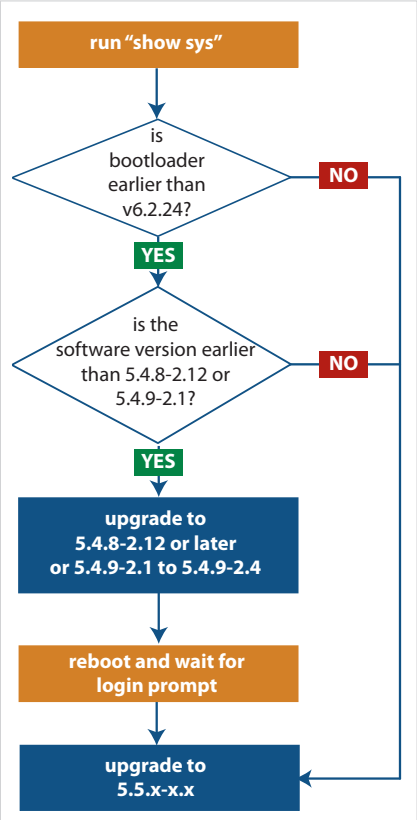
Instead, before upgrading from one of those versions to the current version, make sure your switch is running one of these specified versions:

- 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 most recent firmware version.

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

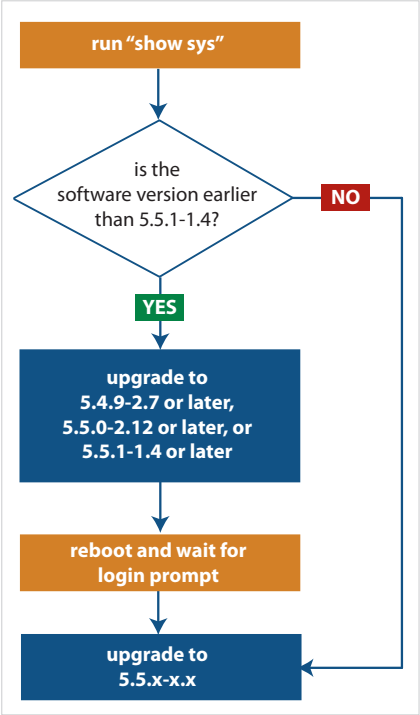
```
awplus# show system
```



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 most recent firmware version 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 most recent firmware version, 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 most recent firmware version.

To see your current firmware 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
VRF configuration reordered in running config	All devices that support VRF	From 5.5.4-0.1 onwards, VRF configuration is printed near the start of running configuration files. This makes sure that AlliedWare Plus creates the VRF instances before running commands that use those VRFs.

Summary	Affected devices	Detail

DES deprecated for TACACS+ server key encryption	All devices that support TACACS+	From 5.5.4-0.1 onwards, newly-created TACACS+ shared keys are stored as AES-encrypted keys. It is no longer possible to create a DES-encrypted key. If the device's running-config contains a DES key, the device will automatically convert it to an AES key.
		
		This means that if the running-config contains this command:
		
		`tacacs-server key 8 <DES-obfuscated-string>`
		
		the device will convert it to this command:
		
		`tacacs-server key 9 <AES-obfuscated-string>`

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.4 license on your switch if you are upgrading to 5.5.4-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 42

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.

Advanced Notification of Password Change in version 5.5.4-2.1

From the upcoming AlliedWare Plus version 5.5.4-2.1, users will be prompted to change the login password when first logging in to a device in factory new state (or that has been reset to that state).

Devices that already have a user configuration will not be affected.

This change will not affect devices running 5.5.4-1.x or earlier.

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 left-hand 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 left-hand 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 Hash values for 5.5.4-1.7 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 for 5.5.4-1.7

Product family	Software File	Hash
AMF Cloud	vaa-5.5.4-1.7.rel	a65216d23f4d048744edab2941cc371949d6a08a01a2219269d7dd5cffa4efdd
SBx8100	SBx81CFC960-5.5.4-1.7.rel	5c8e092a9faf5ddb3c5e72d6162a701ea8efc34bd7254a5da177954cb9573d5c
SBx908 GEN2	SBx908NG-5.5.4-1.7.rel	f06080c3f5577ddcfc0ca292cef8b44e3c1e75ad90d0827039f64b97fe2edea3
x950	x950-5.5.4-1.7.rel	f06080c3f5577ddcfc0ca292cef8b44e3c1e75ad90d0827039f64b97fe2edea3
x930	x930-5.5.4-1.7.rel	6d415c2894eaf74cf492246cb144bc86cd57cebeabcb0f4dbfbdb53560c38951
x550	x550-5.5.4-1.7.rel	5492b739e28657ed1be9b407595b867c14e8b197407ae58fadb6ba669252be73
x530 & x530L	x530-5.5.4-1.7.rel	16c4024d1dd0c55c2388ef8e7a89669e6eaf205835b00bf24def5fc8bc88494a
x330	x330-5.5.4-1.7.rel	6843e842877a40ac6b9591942cd779eed4c2c79b7ecc7f1c72689e2d85a36c8a
x320	x320-5.5.4-1.7.rel	16c4024d1dd0c55c2388ef8e7a89669e6eaf205835b00bf24def5fc8bc88494a
x230 & x230L	x230-5.5.4-1.7.rel	6b10ac9fd39e222c8f5eba7a316c713aaba493249709c1e30830104f62afb87c
x220	x220-5.5.4-1.7.rel	b84225fa5dbdf6663dfc10d5671abf5322c89d5af7e85c8130207e29354117c1
IE340 & IE340L	IE340-5.5.4-1.7.rel	238ef17b7a481092dbb36c971eda60f1d9f61162bcea4cc64c242ec6fbdca056
IE220	IE220-5.5.4-1.7.rel	c124b8e3096ef50734d4a7bff4a44f5150477b9db94ae06df652cf6e919f5255
IE210L	IE210-5.5.4-1.7.rel	6b10ac9fd39e222c8f5eba7a316c713aaba493249709c1e30830104f62afb87c
XS900MX	XS900-5.5.4-1.7.rel	8b906285b233a687492129748c06c843706c5515ded80fd88a882764903b58cd
GS980MX	GS980MX-5.5.4-1.7.rel	16c4024d1dd0c55c2388ef8e7a89669e6eaf205835b00bf24def5fc8bc88494a
GS980EM	GS980EM-5.5.4-1.7.rel	16c4024d1dd0c55c2388ef8e7a89669e6eaf205835b00bf24def5fc8bc88494a
GS980M	GS980M-5.5.4-1.7.rel	b84225fa5dbdf6663dfc10d5671abf5322c89d5af7e85c8130207e29354117c1
GS970EMX	GS970EMX-5.5.4-1.7.rel	6843e842877a40ac6b9591942cd779eed4c2c79b7ecc7f1c72689e2d85a36c8a
GS970M	GS970-5.5.4-1.7.rel	6b10ac9fd39e222c8f5eba7a316c713aaba493249709c1e30830104f62afb87c
AR4050S-5G	AR4050S-5.5.4-1.7.rel	791767d49648c46eb97ebcb7e36331ba2d26e5bc3fa930ff052e68ed9452b095
AR4050S	AR4050S-5.5.4-1.7.rel	791767d49648c46eb97ebcb7e36331ba2d26e5bc3fa930ff052e68ed9452b095
AR3050S	AR3050S-5.5.4-1.7.rel	791767d49648c46eb97ebcb7e36331ba2d26e5bc3fa930ff052e68ed9452b095
AR1050V	AR1050V-5.5.4-1.7.rel	f3ca6a6ce066d45b1f7d46b9cb5999eef909d6ba8115787b4a644cf72275c444
TQ6702 GEN2-R	TQ6702GEN2R-5.5.4-1.7.rel	bb411aee065f515aa0ccaa10b7528fe034817bc74fff51514fe13406b29581eb

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-2024
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                    : 5.5.4
Customer name                   : ABC Consulting
Quantity of licenses            : 1
Type of license                 : Full
License issue date              : 20-Mar-2024
License expiry date             : N/A
Release                         : 5.5.4
```

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-2024
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.5.4
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2024
License expiry date            : N/A
Release                        : 5.5.4
```

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 42 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 45.

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 SBx8100-5.5.4-1.7.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.5.4-1.7.rel`
x950 series	`awplus(config)# boot system x950-5.5.4-1.7.rel`
x930 series	`awplus(config)# boot system x930-5.5.4-1.7.rel`
x550 series	`awplus(config)# boot system x550-5.5.4-1.7.rel`
x530 series	`awplus(config)# boot system x530-5.5.4-1.7.rel`
x330 series	`awplus(config)# boot system x330-5.5.4-1.7.rel`
x320 series	`awplus(config)# boot system x320-5.5.4-1.7.rel`
x240 series	`awplus(config)# boot system x240-5.5.4-1.7.rel`
x230 series	`awplus(config)# boot system x230-5.5.4-1.7.rel`
x220 series	`awplus(config)# boot system x220-5.5.4-1.7.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.4-1.7.rel`
IE220 series	`awplus(config)# boot system IE220-5.5.4-1.7.rel`

Product	Command
IE210L series	`awplus(config)# boot system IE210-5.5.4-1.7.rel`
SE240 series	`awplus(config)# boot system SE240-5.5.4-1.7.rel`
SE250 series	`awplus(config)# boot system SE250-5.5.4-1.7.rel`
SE540L series	`awplus(config)# boot system SE540L-5.5.4-1.7.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.4-1.7.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.4-1.7.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.4-1.7.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.4-1.7.rel`
GS970EMX series	`awplus(config)# boot system GS970EMX-5.5.4-1.7.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.4-1.7.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.4-1.7.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.4-1.7.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.4-1.7.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.4-1.7.rel`
TQ6702 GEN2-R	`awplus(config)# boot system TQ6702GEN2R-5.5.4-1.7.rel`

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

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

5. 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

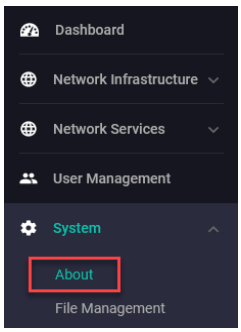
2. Open a web browser and browse to the IP address from step 1.

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 5.5.4-1.x is 2.18.0.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 50 or "Update the GUI on AR-Series devices" on page 51.



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 v5.5.4-1.x is awplus-gui_554_34.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. 554) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

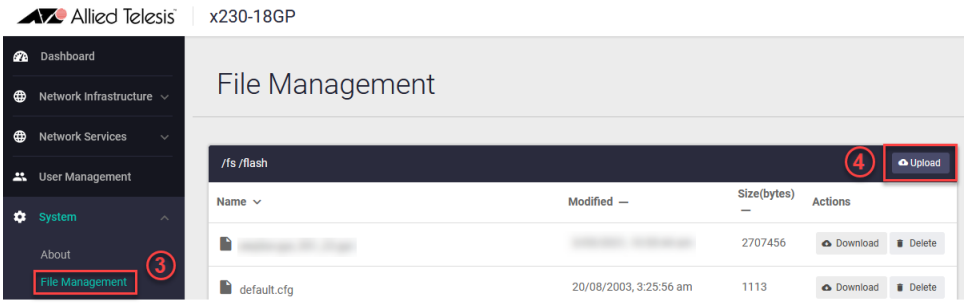
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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 v2.18.0 or later.