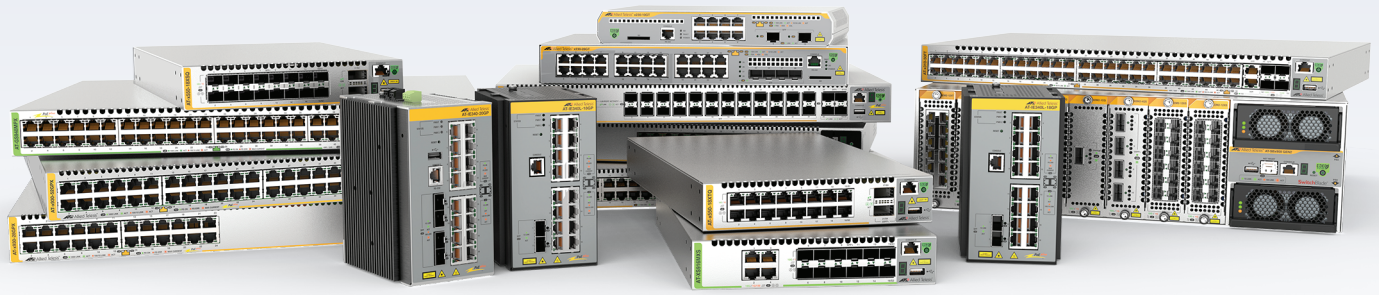
Release Note for AlliedWare Plus Software Version 5.5.5-0.x



AlliedWare Plus OPERATING SYSTEM

AMF Plus Cloud
SBx81CFC960
SBx908 GEN2
x950 Series
x930 Series
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x230 Series
x220 Series
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series
SE250 Series
SE240 Series
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
ARX200S-GTX
AR4000S-Cloud
AR4050S-5G
AR4050S
AR3050S
AR1050V
TQ7403-R
TQ6702 GEN2-R

» 5.5.5-0.2 » 5.5.5-0.5

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 5.5.5-0.5 1

Introduction 1

Issues Resolved in Version 5.5.5-0.5 5

What's New in Version 5.5.5-0.2 1

Introduction 1

New Features and Enhancements 5

Important Considerations Before Upgrading 18

Obtaining User Documentation 24

Verifying the Release File 24

Licensing this Version on an SBx908 GEN2 Switch 26

Licensing this Version on an SBx8100 Series CFC960 Control Card 28

Installing this Software Version 30

Accessing and Updating the Web-based GUI 32

What's New in Version 5.5.5-0.5

Product families supported by this version:

AMF Plus 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
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series[1]
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
ARX200S-GTX
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ7403-R
TQ6702 GEN2-R

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-0.5.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the Allied Telesis Support Portal. 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 30.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 32. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		06/2025	vaa-5.5.5-0.5.iso (VAA OS) vaa-5.5.5-0.5.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-0.5.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	06/2025	SBx81CFC960-5.5.5-0.5.rel
SBx908 GEN2	SBx908 GEN2	06/2025	SBx908NG-5.5.5-0.5.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	06/2025	x950-5.5.5-0.5.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	06/2025	x930-5.5.5-0.5.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2025	x550-5.5.5-0.5.rel
x540L-28XTm x540L-28XS	x540L	06/2025	x540-5.5.5-0.5.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	06/2025	x530-5.5.5-0.5.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	06/2025	x530-5.5.5-0.5.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	06/2025	x330-5.5.5-0.5.rel
x320-10GH x320-11GPT	x320	06/2025	x320-5.5.5-0.5.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	06/2025	x250-5.5.5-0.5.rel

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

Models	Family	Date	Software File
x240-10GTXm x240-10GHXm x240-26GHXm	x240	06/2025	x240-5.5.5-0.5.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	06/2025	x230-5.5.5-0.5.rel
x220-28GS x220-52GT x220-52GP	x220	06/2025	x220-5.5.5-0.5.rel
IE360-12GTX IE360-12GHX	IE360	06/2025	IE360-5.5.5-0.5.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	06/2025	IE340-5.5.5-0.5.rel
IE220-6GHX IE220-10GHX	IE220	06/2025	IE220-5.5.5-0.5.rel
IE210L-10GP IE210L-18GP	IE210L	06/2025	IE210-5.5.5-0.5.rel
SE540L-28XTm SE540L-28XS	SE540L	06/2025	SE540-5.5.5-0.5.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	06/2025	SE250-5.5.5-0.5.rel
SE240-10GTXm SE240-10GHXm	SE240	06/2025	SE240-5.5.5-0.5.rel
XS916MXT XS916MXS	XS900MX	06/2025	XS900-5.5.5-0.5.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	06/2025	GS980MX-5.5.5-0.5.rel
GS980EM/10H GS980EM/11PT	GS980EM	06/2025	GS980EM-5.5.5-0.5.rel
GS980M/52 GS980M/52PS	GS980M	06/2025	GS980M-5.5.5-0.5.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	06/2025	GS970EMX-5.5.5-0.5.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2025	GS970-5.5.5-0.5.rel
AR4000S-Cloud		06/2025	AR-4000S-Cloud-5.5.5-0.5.iso
ARX200S-GTX	ARX200S	06/2025	ARX200S-5.5.5-0.5.rel

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

Models	Family	Date	Software File
10GbE UTM Firewall		06/2025	ATVSTAPL-1.10.1.iso and vfw-x86_64-5.5.5-0.5.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	06/2025	AR4050S-5.5.5-0.5.rel AR3050S-5.5.5-0.5.rel
AR1050V	AR-Series VPN routers	06/2025	AR1050V-5.5.5-0.5.rel
TQ7403-R	Wireless AP Router	06/2025	TQ7403R-5.5.5-0.5.rel
TQ6702 GEN2-R	Wireless AP Router	06/2025	TQ6702GEN2R-5.5.5-0.5.rel

Caution: Software version 5.5.5-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.5 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.5 license installed, that license also covers all later 5.5.5 versions. Such switches will not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 26 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 28.

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

The 5.5.5-0.5 software version is ISSU compatible with previous software versions.

Issues Resolved in Version 5.5.5-0.5

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	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	ARX200	TQ6702 GEN2-R/TQ7403
CR-86716	**API**	Previously, when the system was very busy, API requests could fail to receive responses, resulting in health check failures. 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	Y
CR-86605	**CLI**	Previously, in rare circumstances it was possible for a IMI Shell (CLI) child process to continue running indefinitely if the parent process had been terminated. 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	-	Y	Y
CR-86640	**RADIUS Port Authentication**	Previously, AlliedWare Plus devices had a logic error where, after receiving more than 255 CoA-Disconnect messages from a RADIUS server, they would mistakenly treat any further CoA-Disconnect messages as duplicates and discard them. 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-86728	**Software Licensing**	Previously, FSL subscription licenses (with a .lic extension) could incorrectly expire on the morning of their expiration date instead of 1 second before midnight on the day of expiration. This issue has been resolved; all installed FSL licenses will now correctly expire at 1 second before midnight. New licenses do not need to be installed for this corrected behavior to take effect. 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	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	ARX200	TQ6702 GEN2-R/TQ7403
CR-86961	**System**	With this software update, users no long have access to non-user related internal configuration files. 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

What's New in Version 5.5.5-0.2

Product families supported by this version:

AMF Plus 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
IE360 Series
IE340 Series
IE220 Series
IE210L Series
SE540L Series[1]
SE250 Series[1]
SE240 Series[1]
XS900MX Series
GS980MX Series
GS980EM Series
GS980M Series
GS970EMX Series
GS970M Series
10GbE UTM Firewall
ARX200S-GTX
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQ7403-R
TQ6702 GEN2-R

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.5-0.2.

Software file details for this version are listed in Table 1 on the next page. You can obtain the software files from the Allied Telesis Support Portal. 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 30.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 32. The GUI offers easy visual monitoring and configuration of your device.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		05/2025	vaa-5.5.5-0.2.iso (VAA OS) vaa-5.5.5-0.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.5-0.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	05/2025	SBx81CFC960-5.5.5-0.2.rel
SBx908 GEN2	SBx908 GEN2	05/2025	SBx908NG-5.5.5-0.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	05/2025	x950-5.5.5-0.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	05/2025	x930-5.5.5-0.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2025	x550-5.5.5-0.2.rel
x540L-28XTm x540L-28XS	x540L	05/2025	x540-5.5.5-0.2.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	05/2025	x530-5.5.5-0.2.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	05/2025	x530-5.5.5-0.2.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	05/2025	x330-5.5.5-0.2.rel
x320-10GH x320-11GPT	x320	05/2025	x320-5.5.5-0.2.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	05/2025	x250-5.5.5-0.2.rel

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

Models	Family	Date	Software File
x240-10GTXm x240-10GHXm x240-26GHXm	x240	05/2025	x240-5.5.5-0.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	05/2025	x230-5.5.5-0.2.rel
x220-28GS x220-52GT x220-52GP	x220	05/2025	x220-5.5.5-0.2.rel
IE360-12GTX IE360-12GHX	IE360	05/2025	IE360-5.5.5-0.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	05/2025	IE340-5.5.5-0.2.rel
IE220-6GHX IE220-10GHX	IE220	05/2025	IE220-5.5.5-0.2.rel
IE210L-10GP IE210L-18GP	IE210L	05/2025	IE210-5.5.5-0.2.rel
SE540L-28XTm SE540L-28XS	SE540L	05/2025	SE540-5.5.5-0.2.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	05/2025	SE250-5.5.5-0.2.rel
SE240-10GTXm SE240-10GHXm	SE240	05/2025	SE240-5.5.5-0.2.rel
XS916MXT XS916MXS	XS900MX	05/2025	XS900-5.5.5-0.2.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	05/2025	GS980MX-5.5.5-0.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	05/2025	GS980EM-5.5.5-0.2.rel
GS980M/52 GS980M/52PS	GS980M	05/2025	GS980M-5.5.5-0.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	05/2025	GS970EMX-5.5.5-0.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	05/2025	GS970-5.5.5-0.2.rel
AR4000S-Cloud		05/2025	AR-4000S-Cloud-5.5.5-0.2.iso
ARX200S-GTX	ARX200S	05/2025	ARX200S-5.5.5-0.2.rel

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

Models	Family	Date	Software File
10GbE UTM Firewall		05/2025	ATVSTAPL-1.10.1.iso and vfw-x86_64-5.5.5-0.2.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	05/2025	AR4050S-5.5.5-0.2.rel AR3050S-5.5.5-0.2.rel
AR1050V	AR-Series VPN routers	05/2025	AR1050V-5.5.5-0.2.rel
TQ7403-R	Wireless AP Router	05/2025	TQ7403R-5.5.5-0.2.rel
TQ6702 GEN2-R	Wireless AP Router	05/2025	TQ6702GEN2R-5.5.5-0.2.rel

Caution: Software version 5.5.5-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.5 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.5 license installed, that license also covers all later 5.5.5 versions. Such switches will not need a new license before upgrading to later versions.

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

- "Licensing this Version on an SBx908 GEN2 Switch" on page 26 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 28.

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

The 5.5.5-0.2 software version is **not** ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.5-0.2:

- "AlliedWare Plus enhancements" on page 5
- "Wireless enhancements" on page 11

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 24.

AlliedWare Plus enhancements

Media Redundancy Protocol (MRP) improvements

Available on: IE360, IE340, IE220, SBx908 GEN 2

From software version 5.5.5-0.2 onwards, MRP includes the following improvements and fixes:

- support for **SBx908 GEN2** Series devices.
- reliable operation during stack failover on products with stacking support.
- correct functionality when a XEM is hot-swapped.
- support for SNMP Traps and Multiple Rings with common MRP manager on the **IE360, IE340, IE220,** and **SBx908 GEN2** Series devices.

What is MRP used for?

MRP is a standardized redundancy protocol used in Industrial Ethernet ring networks. Ethernet technology does not allow physical loops, as they cause packets to circulate endlessly and overload the network. This means providing media redundancy within an Ethernet network requires the use of a protocol that is able to monitor and resolve the physical loops introduced by redundant pathways.

Media redundancy is primarily used to avoid single points of failure in industrial communication networks. If a failure occurs on a redundant structure, the network falls back to a secondary state in which communication is still viable, and repairs can be made to restore the system to the previous fault-free state.

MRP is specified for ring networks with up to 50 devices. It guarantees fully predictable switch-over behavior. Allied Telesis switches support worst-case switch-over times of 200 or 500ms.

For more information, see the Media Redundancy Protocol (MRP) Feature Overview and Configuration Guide.

ECMP for BGP routes under named VRF

Available on: All devices that support BGP and VRF-lite: ARX200S, AR4050S, AR3050S, SBx8100CFC960, SBx908 GEN2, x950, x930, x540L, and x530 Series.

AlliedWare Plus version 5.5.5-0.2 onwards supports Equal-Cost Multi-Path (ECMP) for BGP routes learned via BGP peers under named VRFs.

Previously, ECMP for BGP was applied only within the default VRF.

Now, ECMP for BGP can be configured within a specific named VRF, allowing per-VRF ECMP settings instead of being limited to the global default VRF.

This means the router can now perform ECMP not only for the default VRF but also for routes learned within different VRFs. As a result, traffic across multiple VRFs can be load-balanced using ECMP, improving efficiency in multi-VRF environments.

The following example configurations demonstrate ECMP usage in both the global VRF and a named VRF.

ECMP under Global VRF - max paths = 64

```
router bgp 1
  max-paths ebgp 3
  max-paths ibgp 4
  neighbor 10.10.10.2 remote-as 2
  neighbor 10.10.10.2 activate
```

ECMP under Named VRF - max paths = 8

```
router bgp 1
 address-family ipv4 vrf RED
  max-paths ebgp 3
  max-paths ibgp 4
  neighbor 10.10.10.2 remote-as 2
  neighbor 10.10.10.2 activate
 exit-address-family
```

For more information on route selection, see the Route Selection Feature Overview and Configuration Guide.

Support for IP unnumbered on tunnel interfaces

Available on: AR-Cloud, ARX200 series, AR4050S series, AR3050S, AR1050V, TQ6702 GEN2-R and TQ7403-R

From AlliedWare Plus version 5.5.5-0.2 onwards, point-to-point **tunnel** interfaces support IP unnumbered functionality. To help save scarce IPv4 addresses, a tunnel can use the IP unnumbered functionality to borrow the IP address of another specified interface.

Use the following command when configuring a tunnel interface:

```
ip unnumbered <interface>
```

For example, to borrow an IP address from vlan10 on tunnel0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip address 6.6.6.6/24
awplus(config-if)# exit
awplus(config)# interface tunnel0
awplus(config-if)# ip unnumbered vlan10
```

For more information, see the **PPP IP Borrow** section, in the PPP Feature Overview and Configuration Guide.

Support for 1000 IPsec tunnels on ARX200S-GTX

From AlliedWare Plus version 5.5.5-0.2 onwards, ARX200-GTX firewalls support 1000 IPsec tunnels. Previously, 500 tunnels were supported.

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

Preparing factory-new devices for Secure Zero Touch Provisioning (SZTP)

Available on: SBx908 GEN2, x950, x930, x550, x540L, x530, x530L, x330, x320, x250, x240, x220, IE360, IE340, IE220, XS900MX, GS980MX, GS970EMX, GS980EM, GS980M, SE540L, SE250, SE240, ARX200S, AR4050S, AR3050S, AR1050S, TQ6702 GEN2-R and TQ7403-R

From AlliedWare Plus version 5.5.5-0.2 onwards, factory-new devices may initially operate as a DHCP client before being assigned static IP addressing. And if a network DHCP server allocates IP and DNS information, the device may perform network time synchronization, DNS resolution, and automatically attempt to connect to a remote Allied Telesis bootstrapping service using the Secure Zero Touch Provisioning (SZTP) protocol.

This change in functionality is in preparation for a secure zero touch provisioning service that Allied Telesis will offer from later in 2025.

Radius Proxy NAS limits increased for x530 Series

Available on: x530 Series

Software version 5.5.5-0.2 extends RADIUS Proxy NAS support limits from 100 to 1000 on the x530 Series. RADIUS Proxy acts as a RADIUS server to clients (Network Access Servers) and redirects requests from clients to another RADIUS server as a client. So the client registers a RADIUS Proxy as a RADIUS server and does not recognize any difference for the RADIUS communication.

This software version increases the number of Network Access Servers that the RADIUS Proxy can support—from a limit of 100 NAS devices to 1000.

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

Optimized startup and resource management

Available on: All AlliedWare Plus devices

From software version 5.5.5-0.2 onwards, routing daemons (PIM, RIP, OSPFv6, etc.) now start only when explicitly enabled in the configuration, improving system startup time and reducing resource usage.

Existing configurations will continue to function as before. Users attempting to configure disabled services will receive clear prompts to enable them.

This software version actively disables the following services by default:

- rip
- ripng
- ospf
- ospf6
- vrrp
- pim
- pim6
- pdm
- onm
- epsr

To enable a service, use the command **service xxxx**. For example, to enable the PIM service, use the commands:

```
awplus# configure terminal
awplus(config)# service pim
```

DoS attack prevention support

Available on: x540L, x250, x240, SE540L, SE250 and SE240 Series

From software version 5.5.5-0.2 onwards, Denial of Service (DoS) attack prevention is supported on the following platforms:

- x240
- SE240
- x250
- SE250
- x540L
- SE540L

Six different DoS attacks can be detected: IP Options, Land, Ping-of-Death, Smurf, Synflood, and Teardrop.

When the attack is detected, three different actions are available:

1. Shut down the port for one minute
2. Cause an SNMP trap
3. Send traffic to the mirror port

Syntax `dos {ipoptions|land|ping-of-death|smurf broadcast <ip-address>|synflood|teardrop} action {shutdown|trap|mirror}`

To configure ping-of-death DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos ping-of-death action shutdown
```

DoS attack detection is not configured by default on any switch port interface.

For more information on network protection, see the Intrusion Prevention System (IPS) Feature Overview and Configuration Guide.

Command removed - license update online

Applies to all AlliedWare Plus devices

The **license update online** command has been removed as this functionality is no longer available.

AR4050S-5G band restrictions for regulatory compliance

Available on: AR4050S-5G

Due to regulatory requirements, some bands may not be supported depending on the carrier you are using and the country or region that you are in. From AlliedWare Plus version 5.5.5-0.2 onwards new band restrictions apply to AR4050S-5G routers located in Taiwan.

To display band restrictions for your router in your country, use the command **show 5g band**.

The example below shows the current band restrictions for Taiwan:

```
awplus#show 5g band

APN profile transmit mode Not Set

Bands available with active carrier GENERIC
------------------------------------------------------------------------
RATs : WCDMA,LTE,NR5G
GWC  : B1,B2,B4,B5,B6,B8,B9,B19
LTE  : B1,B2,B3,B4,B5,B7,B8,B12,B13,B14,B17,B18,B19,B20,B25,B26,B28,B29,B30,B32,
B34,B38,B39,B40,B41,B42,B46,B48,B66,B71
TDS  :
NRSA : n1,n2,n3,n5,n28,n41,n66,n71,n77,n78,n79
NRNSA: n1,n2,n3,n5,n28,n41,n66,n71,n77,n78,n79

Bands excluded due to regulatory compliance
LTE  : B30 and B48
Country Band Restrictions Applied: Taiwan

Bands available to use:
------------------------------------------------------------------------
GWC:    B1 B8
LTE:    B1 B3 B7 B8 B28 B38 B41
NRNSA:  n1 n3 n28 n41 n78
NRSA:   n1 n3 n28 n41 n78
```

For more information about band restrictions for regulatory compliance, see the 5G Mobile UTM Firewall Feature Overview and Configuration Guide.

Wireless enhancements

From version 5.5.5-0.2 onwards, and using Device GUI version 2.20.0, the following wireless features have been added to the TQ6702 GEN2-R and TQ7403-R (TQ-R Series).

Additional ARP Proxy option

Available on: TQ6702 GEN2-R and TQ7403-R

From software version 5.5.5-0.2 onwards, TQ-R Series wireless AP routers have a new option to allow ARP packets from unknown addresses for Proxy ARP, rather than dropping the packets.

How it works

Some stations, such as IP phones, do not send packets for Proxy ARP learning. This means that the Proxy ARP drops any ARP packets that the TQ-R cannot respond to by proxy, which causes delayed IP resolution. This feature implements an option to allow ARP packets from unknown addresses for Proxy ARP, rather than dropping them. This speeds up IP resolution for stations such as IP phones.

New commands

- **proxy-arp-through enable**

  Use this command to set the Proxy ARP feature to allow ARP packets through from unlearned IP addresses:

  Use the **no** variant to set the Proxy ARP back to disabled (the default).

- **cb-proxy-arp-through enable**

  Use this command to set the Channel Blanket Proxy ARP feature to allow ARP packets through from unlearned IP addresses:

  Use the **no** variant to set the Proxy ARP back to disabled (the default).

Examples

To set the Proxy ARP feature to allow ARP packets through from unlearned IP addresses for network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# proxy-arp-through enable
```

To configure Proxy ARP to forward ARP packets from unlearned IP addresses on Channel Blanket for network 20, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile 20
awplus(config-wireless-ap-prof)# channel-blanket
awplus(config-wireless-ap-prof-cb)# cb-proxy-arp-through
enable
```

Show commands Use these commands to display information about the Proxy ARP settings:

```
show wireless network <1-65535>
show wireless ap-profile
```

For more information on TQ-R management, see Wireless Management for the TQ6702 GEN2-R using the Device GUI

Automatically enable wireless during AMF Plus recovery

Available on: TQ6702 GEN2-R and TQ7403-R

From software version 5.5.5-0.2 onwards, TQ-R Series wireless AP routers can automatically recover over a wireless link to the AMF Plus Master. This allows zero touch replacement.

How it works

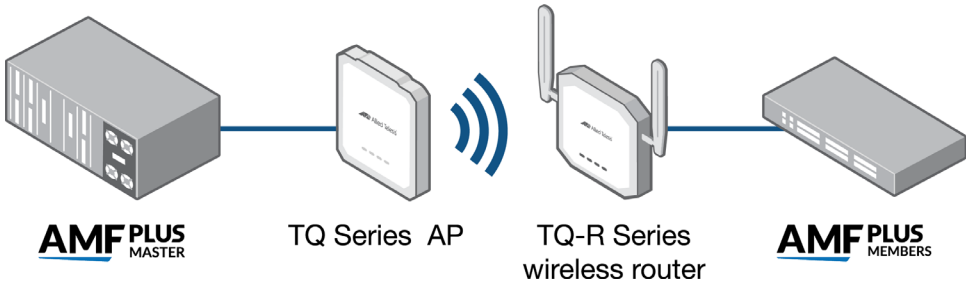
For example, when a TQ-R Series wireless router belongs to a remote sub-network connected to a switch that has the AMF Plus Master network, this means that the sub-network is connected to the AMF Plus Master wirelessly.

When attempting recovery, the **wireless ap-configuration apply ap local** command is automatically applied to the recovering wireless device that has wireless configuration. This allows the recovering device to access the AMF Plus Master even when it is only accessible via a wireless connection.

This makes it possible for the TQ-R Series wireless router to automatically recover from the AMF Plus Master via the switch, with zero touch replacement.

Overview of the configuration steps

This example shows how to set up the following network for automatic recovery of a TQ-R series device over a wireless network:



1. Set the WDS child on the TQ-R Series device:

```
wireless
ap-profile local
radio 1
enable
vap 0 network 1 wds child
```

2. Then on the TQ Series AP, use the GUI to set the WDS parent mode, with the same SSID and password. The AP and TQ-R form a Wireless Distribution System (WDS) wireless link once they both have an active VAP with the same SSID and password.

3. Set the AMF Plus network name on the three AMF Plus devices (master, member, and TQ-R series):

```
atmf-device(config)# atmf network-name NETWORK1
```

4. Set the master:

```
atmf-master(config)# atmf master
```

5. Set the AMF Plus link between the TQ-R and the AMF Plus member:

```
TQR(config-if)# atmf-link
atmf-member(config-if)# atmf-link
```

6. Set the AMF Plus virtual link between the TQ-R and AMF Plus master:

```
TQR(config)# atmf virtual-link id 66 ip 192.168.69.10 remote-id 53 remote-ip 192.168.1.23
atmf-master(config)# atmf virtual-link id 53 ip 192.168.1.23 remote-id 66 remote-ip 192.168.69.10
```

Now the TQ-R can perform a full AMF Plus recovery over the wireless link to the AMF Plus master. To trigger this recovery manually, run the command **atmf cleanup** on the TQ-R.

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

TQ-R Series RFScan Improvements

Available on: TQ6702 GEN2-R and TQ7403-R

AlliedWare Plus version 5.5.5-0.2 onwards provides improved TQ Router RFScan functionality.

The RFScan feature for detecting neighboring APs has been significantly improved. The previous method of scanning all channels on a radio simultaneously, which could lead to prolonged communication loss, has been replaced.

You can now select between two scan methods:

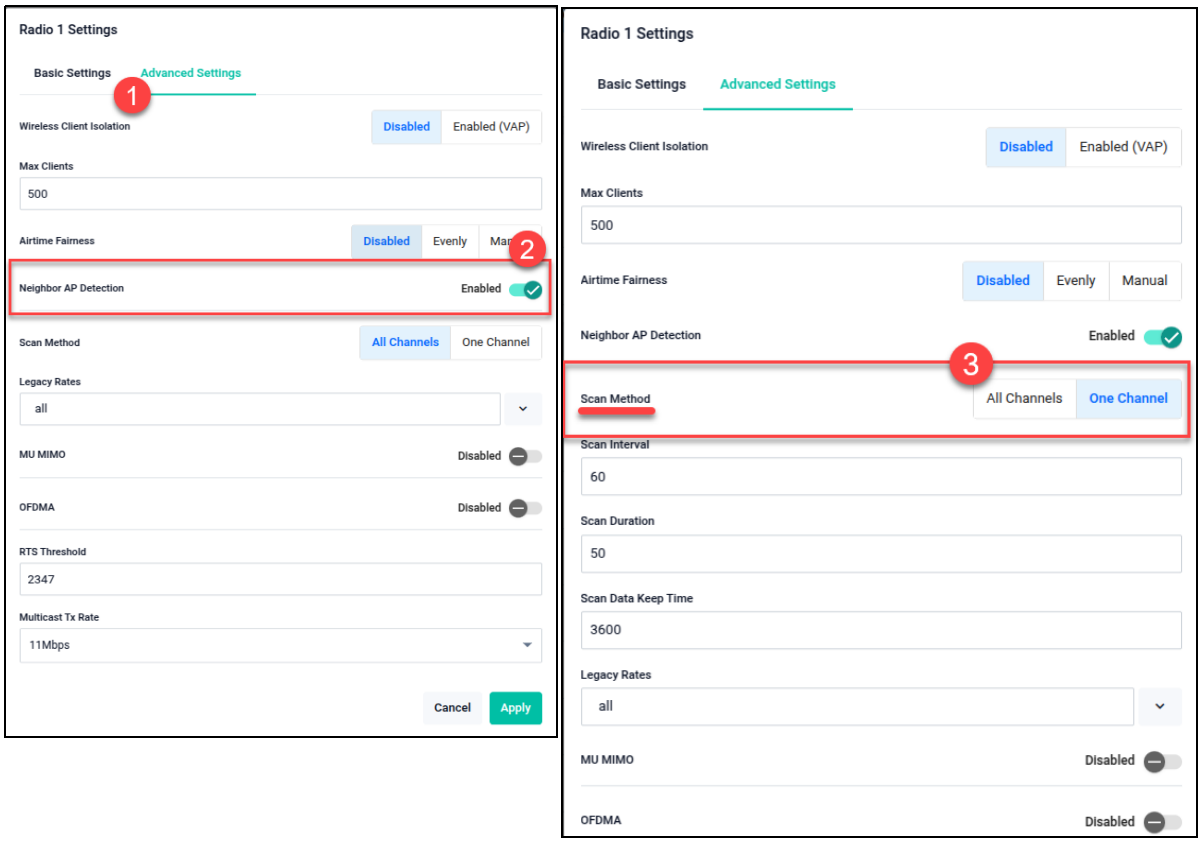
- **All-Channel Scan**: Scans all channels at once (behavior similar to the initially improved 5 GHz, 4 channels at a time approach).
- **Single-Channel Scan**: Scans one channel at a time, allowing configuration of scan interval, duration, and data retention.

To configure these settings through the GUI:

1. Go to: Wireless > Radio Settings > Advanced Settings tab

2. Enable **Neighbor AP Detection**

3. Select Scan Method, **All Channels** or **One Channel**



Two-step authentication enhancements on TQ-R Series

Available on: TQ6702 GEN2-R and TQ7403-R

AlliedWare Plus version 5.5.5-0.2 onwards introduces an enhancement to two-step authentication that allows STAs (stations) to connect using either MAC authentication **or** Captive Portal (CP) authentication.

Previously, authentication required both MAC and CP methods. Now, STAs can connect if they succeed in either method.

This means:

- if MAC authentication fails, the STA can still connect via CP.
- if MAC authentication succeeds, the STA can connect without needing CP authentication.

This allows web-authenticated devices to stay authenticated, even if they move between different switches.

Captive Portal behavior and centralized authentication remain unchanged.

New command There is a new command available: **mac-auth two-step-auth-with-cp enable**

To disable two-step authentication on Network 1, and allow an STA to connect using either MAC authentication or CP authentication, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# no mac-auth two-step-auth-with-cp enable
```

To enable two-step authentication (the default) on network 1, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth two-step-auth-with-cp enable
```

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

Additional Proxy ARP option

Available on: TQ6702 GEN2-R and TQ7403-R

From software version 5.5.5-0.2 onwards, TQ-R Series wireless AP routers have a new option to allow ARP packets from unknown addresses for Proxy ARP, rather than dropping the packets.

How it works

Some stations, such as IP phones, do not send packets for Proxy ARP learning. This means that the Proxy ARP drops any ARP packets that the TQ-R cannot respond to by proxy, which causes delayed IP resolution.

This feature implements an option to allow ARP packets from unknown addresses for Proxy ARP, rather than dropping them. This speeds up IP resolution for stations such as IP phones.

New commands

- **proxy-arp-through enable**

  Use this command to set the Proxy ARP feature to allow ARP packets through from unlearned IP addresses:

  The default is disabled. Use the **no** variant to set the Proxy ARP back to disabled.

- **cb-proxy-arp-through enable**

  Use this command to set the Channel Blanket Proxy ARP feature to allow ARP packets through from unlearned IP addresses:

  The default is disabled. Use the **no** variant to set the Proxy ARP back to disabled.

Examples To set the Proxy ARP feature to allow ARP packets through from unlearned IP addresses for network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 20
awplus(config-wireless-network)# proxy-arp-through enable
```

To set the Proxy ARP feature to allow ARP packets for Channel Blanket through from unlearned IP addresses for network 20, use the commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile 20
awplus(config-wireless-ap-prof)# channel-blanket
awplus(config-wireless-ap-prof-cb)# cb-proxy-arp-through enable
```

Show commands Use these commands to display information about the Proxy ARP settings:

```
awplus# show wireless network <1-65535>
awplus# show wireless ap-profile
```

For more information on wireless management, see: Wireless Management for the TQ6702 GEN2-R using the Device GUI

Wired MAC authentication

Available on: TQ6702 GEN2-R andQ7403-R

From AlliedWare Plus version 5.5.5-0.2 onwards, MAC Authentication is supported on the Ethernet interfaces of wireless TQ Routers. However, functionality is more limited compared to other AlliedWare Plus products.

MAC Authentication is a simple method of controlling ingress to an interface on a networking device. Multiple supplicants on a port can be individually authenticated, similar to having **auth host-mode multi-supplicant** configured.

The process of configuring MAC authentication on TQ-R Series is similar to that on other products. First, define the authentication method list to be used, then enable MAC authentication on the relevant port.

Additionally, you must configure a bridge and add the authenticated Ethernet port to the bridge group. The following is a basic example of bridge configuration:

```
aaa authentication auth-mac default group radius
!
bridge 1
!
interface eth1
 bridge-group 1
 auth-mac enable
```

New commands

There are two new commands for TQ-R Ethernet ports:

- **auth-mac nas-id** <*name*>

  This command adds a NAS-Identifier attribute to RADIUS authentication requests.

  For example, to add NAS-Identifier attribute to RADIUS Access Request, use the commands:

  ```
  awplus# configure terminal
  awplus(config)# interface eth1
  awplus(config-if)# auth-mac nas-id NASID100
  ```

- **auth-mac username** {hyphen|colon|dot|none} {lower-case|upper-case}

  This is similar to the existing 'auth-mac username' command, but uses slightly different parameters. It defines the MAC address format used in the username and password sent to the RADIUS server during MAC-based authentication.

  For example, to format the MAC address with colons and uppercase letters in the username and password, use the following commands:

  ```
  awplus# configure terminal
  awplus(config)# interface eth1
  awplus(config-if)# auth-mac username colon upper-case
  ```

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

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that 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 Plus software version compatibility
- Upgrading all devices in an AMF Plus network

Please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.3-2.x version, please check the 5.5.4-0.x, 5.5.4-1.x and 5.5.4-2.x release notes. Release notes are available from our website, including:

- 5.5.4-x.x release notes
- 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 19 and "Details for x930 Series" on page 20 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.

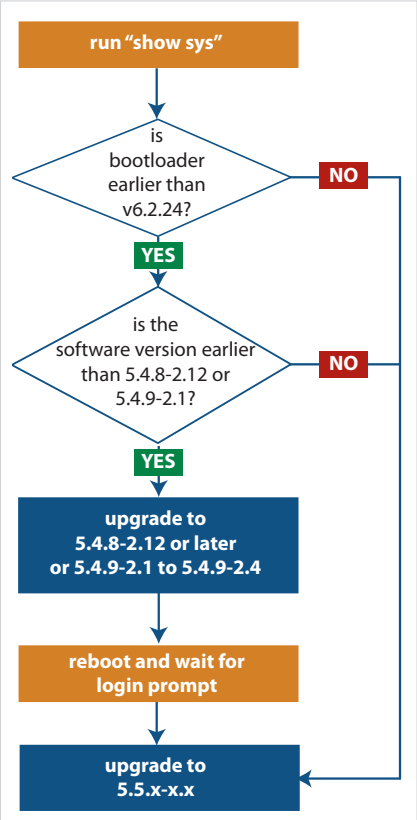
Instead, before upgrading from one of those versions to the current version, make sure your switch is running one of these specified versions:

- 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:

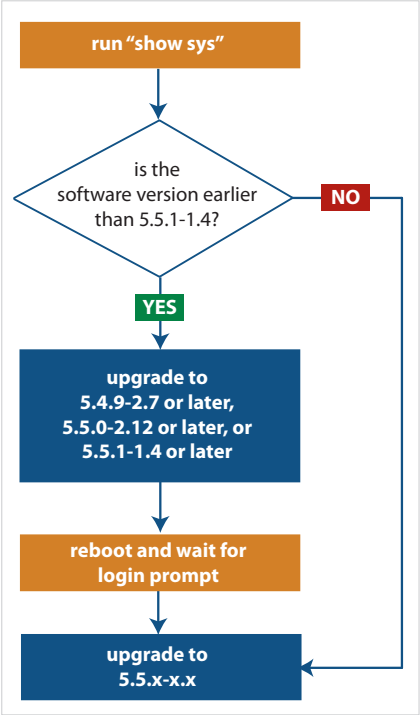
```
awplus# show system
```



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 **license update online** command is no longer available for downloading licenses due to changes in Allied Telesis' license management portal. This change is applicable to all firmware versions, not just the latest.

Summary	Affected devices	Detail
license update online command no longer available.	All AlliedWare Plus devices with subscription licenses across all firmware versions, including previous versions.	Since January 2025, the **license update online** command is no longer available for downloading licenses. To obtain licenses, please contact your authorized Allied Telesis support center. After obtaining the license, use the **license update file** command to install it.

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.5 license on your switch if you are upgrading to 5.5.5-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 26 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 28.

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 Plus software version compatibility

Applies to all AlliedWare Plus devices

We strongly recommend that all nodes in an AMF Plus 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 Plus network

Applies to all AlliedWare Plus devices

This version supports upgrades across AMF Plus networks. There are two methods for upgrading firmware on an AMF Plus 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 Plus 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 Plus 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 Plus upgrade method is most suitable.

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

Obtaining User Documentation

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

- **Feature Overview and Configuration Guides** - find these by searching for the featuC613-10613-00 REV Dre 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 lefthand menu.

Verifying the Release File

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

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

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

This command compares the SHA256 hash of the release file with the correct hash for the file. The correct hash is listed in the table Hash values for 5.5.5-0.5 below or in the release's sha256sum file, which is available from the Allied Telesis Support Portal.

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 5.5.5-0.5

Product family	Software File	Hash
AMF Plus Cloud	vaa-5.5.5-0.5.rel	f9bbb64a0f09d459d4ede55b421934414c5fe3c43233d2b4d96451872e145f20
SBx8100	SBx81CFC960-5.5.5-0.5.rel	5e845e0fde55b24be4a821b7a3a23f7ba0513c1de756d79b7312e50486feb4a3
SBx908 GEN2	SBx908NG-5.5.5-0.5.rel	aefb91b8733d43096a5369a7f1246f3752dce058a2fe472169df01fe5893b684
x950	x950-5.5.5-0.5.rel	aefb91b8733d43096a5369a7f1246f3752dce058a2fe472169df01fe5893b684
x930	x930-5.5.5-0.5.rel	9476ba0a8d4c9b5c260b74ed41fa29360adcc7f568592f5b3482e1b672b9cff1
x550	x550-5.5.5-0.5.rel	88835f1c92c60130e5043a448d56e1547d5ae6963165050349146acba7a3885f
x540L	x540-5.5.5-0.5.rel	1f66530920d9389390248e736195fad63aac045fc729e1ad087ba17c5b39b4bf
x530 & x530L	x530-5.5.5-0.5.rel	33a46b89006837963a72ef0685f7ec486a075119d66d507dfc2f6d3b4dcadf4f

Table: Hash values for 5.5.5-0.5

Product family	Software File	Hash
x330	x330-5.5.5-0.5.rel	2f7f383872a8f69185b10e30c3a6ab583c83364aae0577a49b1cb915e041f70c
x320	x320-5.5.5-0.5.rel	33a46b89006837963a72ef0685f7ec486a075119d66d507dfc2f6d3b4dcadf4f
x250	x250-5.5.5-0.5.rel	2766391fceab5a547ffe3f4673a811c134acee20186205cc32b87426760925a7
x240	x240-5.5.5-0.5.rel	db5c7b85dcedab021979e44ff5f929b1702a1629c5e5a3785ed3796d51eeb2c4
x230 & x230L	x230-5.5.5-0.5.rel	26ddd5aa0857b083c28a41ad0698d4925c03f6c165a13395ef8e751574fb9046
x220	x220-5.5.5-0.5.rel	83c274d6d9b7832c5988b26819bc293485fdc67f5c4f7caf254eba605fc31b58
IE360	IE360-5.5.5-0.5.rel	ae6f218e852bc458b55a12cfb1c24850db835264a540ddf338a7479dd8c2d36a
IE340 & IE340L	IE340-5.5.5-0.5.rel	da802a3885e03996a95a6770618382321671e38cf1eaea2d58e659d086c3c705
IE220	IE220-5.5.5-0.5.rel	70c27c23a45f8f61e63f9f6d89edb860e1091a2126fbce9b38bc8a9cbd5a98d0
IE210L	IE210-5.5.5-0.5.rel	26ddd5aa0857b083c28a41ad0698d4925c03f6c165a13395ef8e751574fb9046
SE540L	SE540-5.5.5-0.5.rel	1f66530920d9389390248e736195fad63aac045fc729e1ad087ba17c5b39b4bf
SE250	SE250-5.5.5-0.5.rel	2766391fceab5a547ffe3f4673a811c134acee20186205cc32b87426760925a7
SE240	SE240-5.5.5-0.5.rel	db5c7b85dcedab021979e44ff5f929b1702a1629c5e5a3785ed3796d51eeb2c4
XS900MX	XS900-5.5.5-0.5.rel	d67d30314a3e68b7a9d0e78bf78bf43af9f120c388c79e1d1094185b1b80be4d
GS980MX	GS980MX-5.5.5-0.5.rel	33a46b89006837963a72ef0685f7ec486a075119d66d507dfc2f6d3b4dcadf4f
GS980EM	GS980EM-5.5.5-0.5.rel	33a46b89006837963a72ef0685f7ec486a075119d66d507dfc2f6d3b4dcadf4f
GS980M	GS980M-5.5.5-0.5.rel	83c274d6d9b7832c5988b26819bc293485fdc67f5c4f7caf254eba605fc31b58
GS970EMX	GS970EMX-5.5.5-0.5.rel	2f7f383872a8f69185b10e30c3a6ab583c83364aae0577a49b1cb915e041f70c
GS970M	GS970-5.5.5-0.5.rel	26ddd5aa0857b083c28a41ad0698d4925c03f6c165a13395ef8e751574fb9046
ARX200S	ARX200S-5.5.5-0.5.rel	b3eeae93c6573f0f6ca9bad35430344f698e94aa4cca4bc664afb5eeb6f83452
AR4050S-5G	AR4050S-5.5.5-0.5.rel	86c8a6dff7c5031e6b2979c8e62dd78ef4119cb1a179353d5c86dd7f53b813c8
AR4050S	AR4050S-5.5.5-0.5.rel	86c8a6dff7c5031e6b2979c8e62dd78ef4119cb1a179353d5c86dd7f53b813c8
AR3050S	AR3050S-5.5.5-0.5.rel	86c8a6dff7c5031e6b2979c8e62dd78ef4119cb1a179353d5c86dd7f53b813c8
AR1050V	AR1050V-5.5.5-0.5.rel	5106196eef09ab4f05172afcfda21caaee07b5c2096cd799d831ad8c518b9b11
TQ6702 GEN2-R	TQ6702GEN2R-5.5.5-0.5.rel	537003910e6bca5ee148cbf108cfd9d2245333c7ede64cadfb0cd45a46a23a6f
TQ7403-R	TQ7403R-5.5.5-0.5.rel	6f39023a9d1175698ea612d78a0702def997e51177c5881ae318cb14be715c0d

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                   : 5.5.5
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 05-May-2025
License expiry date            : N/A
Release                        : 5.5.5
```

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                   : 5.5.5
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 05-May-2025
License expiry date            : N/A
Release                        : 5.5.5
```

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 26 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 28.

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 SBx8100-5.5.5-0.5.rel`
SBx908 GEN2	`awplus(config)# boot system ARX200S-5.5.5-0.5.rel`
x950 series	`awplus(config)# boot system x950-5.5.5-0.5.rel`
x930 series	`awplus(config)# boot system x930-5.5.5-0.5.rel`
x550 series	`awplus(config)# boot system x550-5.5.5-0.5.rel`
x540L series	`awplus(config)# boot system x540-5.5.5-0.5.rel`
x530 series	`awplus(config)# boot system x530-5.5.5-0.5.rel`
x330 series	`awplus(config)# boot system x330-5.5.5-0.5.rel`
x320 series	`awplus(config)# boot system x320-5.5.5-0.5.rel`
x250 series	`awplus(config)# boot system x250-5.5.5-0.5.rel`
x240 series	`awplus(config)# boot system x240-5.5.5-0.5.rel`
x230 series	`awplus(config)# boot system x230-5.5.5-0.5.rel`
x220 series	`awplus(config)# boot system x220-5.5.5-0.5.rel`

Product	Command
IE360 series	`awplus(config)# boot system IE360-5.5.5-0.5.rel`
IE340 series	`awplus(config)# boot system IE340-5.5.5-0.5.rel`
IE220 series	`awplus(config)# boot system IE220-5.5.5-0.5.rel`
IE210L series	`awplus(config)# boot system IE210-5.5.5-0.5.rel`
SE540L series	`awplus(config)# boot system SE540-5.5.5-0.5.rel`
SE250 series	`awplus(config)# boot system SE250-5.5.5-0.5.rel`
SE240 series	`awplus(config)# boot system SE240-5.5.5-0.5.rel`
XS900MX series	`awplus(config)# boot system XS900-5.5.5-0.5.rel`
GS980M series	`awplus(config)# boot system GS980M-5.5.5-0.5.rel`
GS980EM series	`awplus(config)# boot system GS980EM-5.5.5-0.5.rel`
GS980MX series	`awplus(config)# boot system GS980MX-5.5.5-0.5.rel`
GS970EMX series	`awplus(config)# boot system GS970EMX-5.5.5-0.5.rel`
GS970M series	`awplus(config)# boot system GS970-5.5.5-0.5.rel`
AR4050S-5G	`awplus(config)# boot system AR4050S-5.5.5-0.5.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.5.5-0.5.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.5.5-0.5.rel`
AR1050V	`awplus(config)# boot system AR1050V-5.5.5-0.5.rel`
ARX200S-GTX	`awplus(config)# boot system ARX200S-5.5.5-0.5.rel`
TQ6702 GEN2-R	`awplus(config)# boot system TQ6702GEN2R-5.5.5-0.5.rel`
TQ7403-R	`awplus(config)# boot system TQ7403R-5.5.5-0.5.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

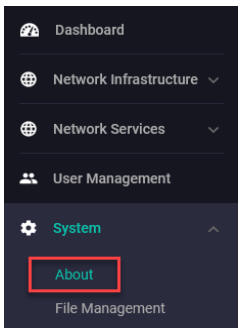
2. Open a web browser and browse to the IP address from step 1.

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 5.5.5-0.x is **2.20.0**.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 33 or "Update the GUI on AR-Series devices" on page 34.



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 the Allied Telesis Support Portal. The GUI filename to use with AlliedWare Plus v5.5.5-0.x is awplus-gui_555_38.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. 555) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

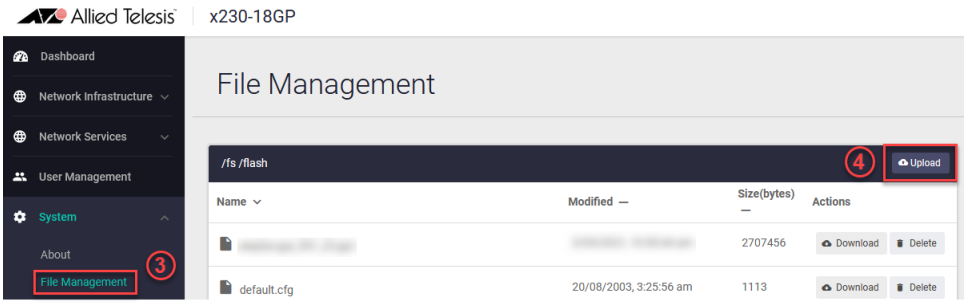
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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 Support 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 v2.20.0 or later.