Release Notes

Allied Telesis™

AlliedWare Plus Software Version 5.5.6-0.x and Device GUI 2.23.x

- AMF Plus Cloud
- SBx81CFC960
- SBx908 GEN3
- SBx908 GEN2
- x950 Series
- x930 Series
- x560-28YSQ
- x550 Series
- x540L Series
- x530 Series
- x530L Series
- x330 Series
- x320 Series
- x250 Series
- x240 Series
- x220 Series
- IE560 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
- 10GbE UTM Firewall app
- ARX200S Series
- AR4000S-Cloud
- AR4050S-5G
- AR4050S
- AR3050S
- AR1050V
- TQR Series

AlliedWare Plus 5.5.6-0.1, 5.5.6-0.2, 5.5.6-0.3
Device GUI 2.23.0

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/**

What's New in Version 5.5.6-0.3

Product families supported by these versions:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 3
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x560-28YSQ
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x220 Series
IE560-12GSX
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
10GbE UTM Firewall app
ARX200S Series
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQR Series

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.6-0.3. The Device GUI has not been updated with this version.

AlliedWare Plus file details are listed in Table 1 on the next page. You can obtain the AlliedWare Plus and Device GUI 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 76.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 78. 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		06/2026	■ VAA OS: vaa-5.5.6-0.3.iso ■ For AWS: vaa-5.5.6-0.3.vhd and upload_vhd.py ■ For Microsoft Azure: vaa_azure-5.5.6-0.3.vhd
SBx81CFC960	SBx8100	06/2026	SBx81CFC960-5.5.6-0.3.rel
SBx908 GEN3	SBx908 GEN3	06/2026	SBx90xGEN3-5.5.6-0.3.rel
SBx908 GEN2	SBx908 GEN2	06/2026	SBx908NG-5.5.6-0.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	06/2026	x950-5.5.6-0.3.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	06/2026	x930-5.5.6-0.3rel
x560-28YSQ	x560	06/2026	x560-5.5.6-0.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2026	x550-5.5.6-0.3.rel
x540L-28XTm x540L-28XS	x540L	06/2026	x540-5.5.6-0.3.rel

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

Models	Family	Date	Software File
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	06/2026	x530-5.5.6-0.3.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	06/2026	x530-5.5.6-0.3.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	06/2026	x330-5.5.6-0.3.rel
x320-10GH x320-11GPT	x320	06/2026	x320-5.5.6-0.3.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	06/2026	x250-5.5.6-0.3.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	06/2026	x240-5.5.6-0.3.rel
x220-28GS x220-52GT x220-52GP	x220	06/2026	x220-5.5.6-0.3.rel
IE560-12GSX	IE560	06/2026	IE560-5.5.6-0.3.rel
IE360-12GTX IE360-12GHX	IE360	06/2026	IE360-5.5.6-0.3.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	06/2026	IE340-5.5.6-0.3.rel
IE220-6GHX IE220-10GHX	IE220	06/2026	IE220-5.5.6-0.3.rel
IE210L-10GP IE210L-18GP	IE210L	06/2026	IE210-5.5.6-0.3.rel
SE540L-28XTm SE540L-28XS	SE540L	06/2026	SE540-5.5.6-0.3.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	06/2026	SE250-5.5.6-0.3.rel
SE240-10GTXm SE240-10GHXm	SE240	06/2026	SE240-5.5.6-0.3.rel
XS916MXT XS916MXS	XS900MX	06/2026	XS900-5.5.6-0.3.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	06/2026	GS980MX-5.5.6-0.3.rel

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

Models	Family	Date	Software File
GS980EM/10H GS980EM/11PT	GS980EM	06/2026	GS980EM-5.5.6-0.3.rel
GS980M/52 GS980M/52PS	GS980M	06/2026	GS980M-5.5.6-0.3.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	06/2026	GS970EMX-5.5.6-0.3.rel
AR4000S-Cloud		06/2026	Various files depending on deployment. See the Allied Telesis Support Portal.
ARX200S-GT ARX200S-GTX	ARX200S	06/2026	ARX200S-5.5.6-0.3.rel
10GbE UTM Firewall app		06/2026	ATVSTAPL-1.14.1.iso and vfw-x86_64-5.5.6-0.3.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	06/2026	AR4050S-5.5.6-0.3.rel AR3050S-5.5.6-0.3.rel
AR1050V	AR-Series VPN routers	06/2026	AR1050V-5.5.6-0.3.rel
TQ7613-R	TQR	06/2026	TQ7613R-5.5.6-0.3.rel
TQ7403-R	TQR	06/2026	TQ7403R-5.5.6-0.3.rel
TQ7413-R	TQR	06/2026	TQ7413R-5.5.6-0.3.rel
TQ6702 GEN2-R	TQR	06/2026	TQ6702GEN2R-5.5.6-0.3.rel
TQ6702e GEN2-R	TQR	06/2026	TQ6702eGEN2R-5.5.6-0.3.rel
TQ3403-R	TQR	06/2026	TQ3403R-5.5.6-0.3.rel

Caution: Software version 5.5.6-0.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 5.5.6 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.6 license installed, that license also covers all later 5.5.6 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 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

The SBx908 GEN3 switch does not require a release license.

Unsupported products

AlliedWare Plus version 5.5.6-0.1 and later do not support x230, x230L and GS970M series switches. The last version that supports these products is 5.5.5-2.x. The following models are not supported:

- x230-10GP
- x230-10GT
- x230-18GP
- x230-18GT
- x230-28GP
- x230-28GT
- x230L-17GT
- x230L-26GT
- GS970M/10PS
- GS970M/10
- GS970M/18PS
- GS970M/18
- GS970M/28PS
- GS970M/28

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

The 5.5.6-0.3 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.6-0.3.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 69.

Allied Telesis Wave Connect mobile app for TQR Series APs

From 5.5.6-0.1 onwards, you can use a new mobile app for initial provisioning of TQR Series access points. The app is called **Allied Telesis Wave Connect** and is available on the Apple App Store (iOS) and Google Play (Android).

Factory-fresh TQR Series APs can now be provisioned wirelessly via the mobile app, eliminating the need for wired access, controllers, or cloud connectivity during initial setup. In addition to initial provisioning, Allied Telesis Wave Connect also supports configuration and monitoring of existing access points.

The app logo is:

How it works

- A temporary provisioning SSID is automatically created when an AP is factory-fresh
- The provisioning SSID allows a mobile app to connect directly to the AP
- Initial configuration can be completed via the app and local GUI access
- The provisioning network is secure, per-device, and non-persistent.

This process is intended for initial setup only and is automatically disabled once the device enters normal operation.

Removal conditions

The provisioning network is automatically removed on first authentication, remote management, or wireless configuration and does not persist across reboots.

Once removed, the provisioning network:

- Does not appear in show running-config
- Is not saved to startup configuration
- Does not persist across reboots
- Can only be recreated by a factory reset.

For more information about wireless configuration of TQR Series APs, see Wireless Management for the TQR series using the Device GUI.

ARP Denial of Service Monitoring

CR-73938

From 5.5.6-0.3 onwards, AlliedWare Plus supports ARP Denial of Service (DoS) Monitoring.

When enabled, this feature monitors Ethernet and wireless interfaces for received ARP traffic. When the number of ARPs received per second exceeds a configured threshold, a log is generated indicating a potential ARP DoS attack.

This feature is disabled by default. You can enable it and set the threshold with the following commands.

To enable ARP DoS monitoring, use the command:

```
awplus# configure terminal
awplus(config)# arp dos-monitoring
```

To configure the monitoring threshold:

```
awplus(config)# arp dos-monitoring threshold <packets-per-second>
```

The default threshold is 100 ARP packets per second. To return the threshold to the default, use the command:

```
awplus(config)# no arp dos-monitoring threshold <packets-per-second>
```

To disable ARP DoS monitoring, use the command:

```
awplus(config)# no arp dos-monitoring
```

Issues Resolved in Version 5.5.6-0.3

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

CR	Module	Description	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560-12GSX	SE540L	SE250	SE240	x220	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2 / SBx908 GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200S	TQR Series
CR-90331	**AMF**	Previously, provisioning a new node using AMF Plus could result in a non-critical process failure. 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-90230	**MRP**	Previously, on MRP ring failure or formation, only forwarding database (FDB) entries for the MRP VLAN were flushed. This issue has been resolved. FDB entries for all VLANs on the MRP ring ports are now flushed.	-	-	-	-	-	Y	-	Y	Y	Y	Y	-	-	-	-	-	-	-	Y	Y	-	Y	Y	-	Y	-	-	-	-	-	-	Y
CR-90215	**HTTP, PKI**	Previously, during boot up, benign log messages could be produced, indicating that certificate files were missing. This issue has been resolved. These log messages are no longer incorrectly produced. 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
CR-90167	**Wi-Fi, Wireless Controller**	Previously, when an MLO (Multi Link Operation) capable station was connected to an MLO VAP, the Device GUI only displayed information for a single radio. This issue has been resolved, and the GUI now lists and displays information for every active radio used by the MLO client.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y

CR	Module	Description	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560-12GSX	SE540L	SE250	SE240	x220	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2 / SBx908 GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200S	TQR Series
CR-90143	**Wireless Controller**	Previously, AlliedWare Plus release files (with a .rel file extension) were not visible in the device GUI's Wireless Controller. This prevented users from selecting a release for firmware upgrade. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	Y	Y	Y	Y	Y	Y	-	-	Y	Y	-	-	Y	Y
CR-90009	**File system**	Previously, on some x220 series switches, the filesystem may have failed to be read at start-up, resulting in it being reformatted. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ER-7527	**SNMP**	Previously, if **snmp-server sysname** was not configured, the "sysname" object did not return the device hostname as configured in the running-configuration. Instead, it returned a null value. This issue has been resolved. Now, if **snmp-server sysname**: ■ is not configured, the "sysname" object will return the hostname configured in the running-configuration. ■ is configured, the "sysname" object will return this value, overriding the hostname configured in the running-configuration. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

What's New in Version 5.5.6-0.2 and Device GUI 2.23.0

Product families supported by these versions:

AMF Plus Cloud
SwitchBlade x8100: SBx81CFC960
SwitchBlade x908 Generation 3
SwitchBlade x908 Generation 2
x950 Series
x930 Series
x560-28YSQ
x550 Series
x540L Series
x530 Series
x530L Series
x330 Series
x320 Series
x250 Series
x240 Series
x220 Series
IE560-12GSX
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
10GbE UTM Firewall app
ARX200S Series
AR4000S-Cloud
AR4050S
AR4050S-5G
AR3050S
AR1050V
TQR Series

1. Not available in all regions

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.6-0.2 and Device GUI version 2.23.0.

AlliedWare Plus file details are listed in Table 1 on the next page. You can obtain the AlliedWare Plus and Device GUI 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 76.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 78. 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		05/2026	■ VAA OS: vaa-5.5.6-0.2.iso ■ For AWS: vaa-5.5.6-0.2.vhd and upload_vhd.py ■ For Microsoft Azure: vaa_azure-5.5.6-0.2.vhd
SBx81CFC960	SBx8100	05/2026	SBx81CFC960-5.5.6-0.2.rel
SBx908 GEN3	SBx908 GEN3	05/2026	SBx90xGEN3-5.5.6-0.2.rel
SBx908 GEN2	SBx908 GEN2	05/2026	SBx908NG-5.5.6-0.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	05/2026	x950-5.5.6-0.2.rel
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	05/2026	x930-5.5.6-0.2rel
x560-28YSQ	x560	05/2026	x560-5.5.6-0.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	05/2026	x550-5.5.6-0.2.rel
x540L-28XTm x540L-28XS	x540L	05/2026	x540-5.5.6-0.2.rel

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

Models	Family	Date	Software File
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	05/2026	x530-5.5.6-0.2.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	05/2026	x530-5.5.6-0.2.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	05/2026	x330-5.5.6-0.2.rel
x320-10GH x320-11GPT	x320	05/2026	x320-5.5.6-0.2.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	05/2026	x250-5.5.6-0.2.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	05/2026	x240-5.5.6-0.2.rel
x220-28GS x220-52GT x220-52GP	x220	05/2026	x220-5.5.6-0.2.rel
IE560-12GSX	IE560	05/2026	IE560-5.5.6-0.2.rel
IE360-12GTX IE360-12GHX	IE360	05/2026	IE360-5.5.6-0.2.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	05/2026	IE340-5.5.6-0.2.rel
IE220-6GHX IE220-10GHX	IE220	05/2026	IE220-5.5.6-0.2.rel
IE210L-10GP IE210L-18GP	IE210L	05/2026	IE210-5.5.6-0.2.rel
SE540L-28XTm SE540L-28XS	SE540L	05/2026	SE540-5.5.6-0.2.rel
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	05/2026	SE250-5.5.6-0.2.rel
SE240-10GTXm SE240-10GHXm	SE240	05/2026	SE240-5.5.6-0.2.rel
XS916MXT XS916MXS	XS900MX	05/2026	XS900-5.5.6-0.2.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	05/2026	GS980MX-5.5.6-0.2.rel

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

Models	Family	Date	Software File
GS980EM/10H GS980EM/11PT	GS980EM	05/2026	GS980EM-5.5.6-0.2.rel
GS980M/52 GS980M/52PS	GS980M	05/2026	GS980M-5.5.6-0.2.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	05/2026	GS970EMX-5.5.6-0.2.rel
AR4000S-Cloud		05/2026	Various files depending on deployment. See the Allied Telesis Support Portal.
ARX200S-GT ARX200S-GTX	ARX200S	05/2026	ARX200S-5.5.6-0.2.rel
10GbE UTM Firewall app		05/2026	ATVSTAPL-1.14.1.iso and vfw-x86_64-5.5.6-0.2.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	05/2026	AR4050S-5.5.6-0.2.rel AR3050S-5.5.6-0.2.rel
AR1050V	AR-Series VPN routers	05/2026	AR1050V-5.5.6-0.2.rel
TQ7613-R	TQR	05/2026	TQ7613R-5.5.6-0.2.rel
TQ7403-R	TQR	05/2026	TQ7403R-5.5.6-0.2.rel
TQ7413-R	TQR	05/2026	TQ7413R-5.5.6-0.2.rel
TQ6702 GEN2-R	TQR	05/2026	TQ6702GEN2R-5.5.6-0.2.rel
TQ6702e GEN2-R	TQR	05/2026	TQ6702eGEN2R-5.5.6-0.2.rel
TQ3403-R	TQR	05/2026	TQ3403R-5.5.6-0.2.rel

Caution: Software version 5.5.6-0.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 5.5.6 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.6 license installed, that license also covers all later 5.5.6 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 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

The SBx908 GEN3 switch does not require a release license.

Unsupported products

AlliedWare Plus version 5.5.6-0.1 and later do not support x230, x230L and GS970M series switches. The last version that supports these products is 5.5.5-2.x. The following models are not supported:

- x230-10GP
- x230-10GT
- x230-18GP
- x230-18GT
- x230-28GP
- x230-28GT
- x230L-17GT
- x230L-26GT
- GS970M/10PS
- GS970M/10
- GS970M/18PS
- GS970M/18
- GS970M/28PS
- GS970M/28

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

The 5.5.6-0.2 software version is ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.6-0.2 and Device GUI 2.23.0.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 69.

Enhancements in Device GUI 2.23.0 with 5.5.6-0.2

New country/region support for TQR Series APs

From 5.5.6-0.2 onwards, the following TQR series APs can be used in the following countries or regions.

In these countries, you can now configure the APs:

- directly with the Device GUI or CLI
- through the Wireless Controller that is embedded on various AlliedWare Plus devices
- through the AWC plug-in for Vista Manager (requires version 3.17.0 or later).

TQ7403-R

- Philippines (NTC)

TQ3403-R

- Hong Kong (OFCA)
- Malaysia (SIRIM)
- Thailand (NBTC)
- United States (FCC)
- Taiwan (NCC)
- European Union (CE)
- United Kingdom (UKCA)
- Australia (RCM)
- New Zealand (RCM)
- Singapore (SG)

TQ7613-R

- Malaysia (SIRIM)

New Local Wireless Profile Dashboard

Applies to local wireless configuration on TQR Series APs

From Device GUI version 2.23.0 onward (using version 5.5.6-0.2 or later), configuring your wireless network on TQR Series APs is quicker and easier than ever.

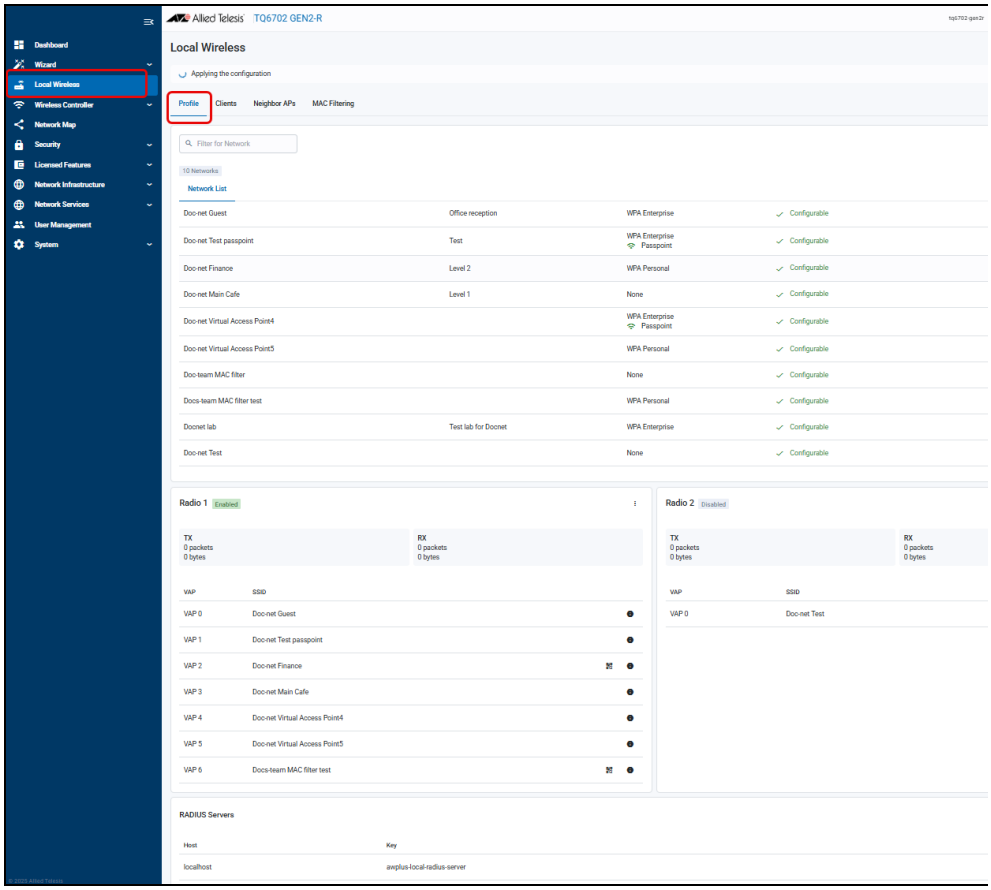
The new Local Wireless **Profile dashboard**, accessed via the **Profile** tab, provides a clear, at-a-glance view of your local wireless setup and how its components fit together:

Key capabilities

From the **Profile dashboard**, you can:

- View default wireless networks in the network widget
- See available radios and how default networks are assigned
- Rename default networks and update their settings and security
- Turn radios on or off and adjust radio settings
- Deploy your configuration
- Monitor the status of the applied configuration

This update simplifies understanding, configuring, and managing your local wireless network.



What's new

- **Reusable wireless networks** – Wireless networks are now created independently of VAPs and can be reused across multiple radios, eliminating the need to recreate the same configuration.
- **Unified dashboard view** – Networks and radios are displayed together on a single dashboard for improved visibility of wireless relationships.
- **Simplified work flow for single-device setups** – Common tasks are streamlined, speeding up configuration for single-AP deployments.

When to use the Local Wireless dashboard

Use the Local Wireless dashboard instead of selecting Wireless Controller in the left-hand menu when you are configuring a single TQR Series AP. It provides a faster and simpler setup experience while continuing to support existing wireless features.

Low RSSI Client Disconnection (per VAP)

Applies in 5.5.6-0.2 to local wireless configuration on TQR Series APs. Applied in 5.5.6-0.1 to all devices that support the Wireless Controller

Overview

From 5.5.6-0.2 and Device GUI 2.23.0 onwards, APs can disconnect wireless clients whose RSSI falls below a configurable threshold and prevent them from reconnecting until signal strength improves.

The feature is configurable per VAP and includes enable/disable control and an RSSI threshold range of –90 dBm to 0 dBm. This helps improve overall wireless performance by preventing low-signal clients from degrading network quality.

What this feature does

This feature automatically disconnects wireless clients (STAs) whose signal strength (RSSI) drops below a configured threshold. It also prevents those low-signal clients from reconnecting until their signal strength improves.

Why this matters

Clients with very low RSSI can:

- Cause poor performance
- Increase retransmissions
- Degrade overall wireless network quality

This feature helps maintain better network stability and performance by removing weak connections.

Key behavior to be aware of

Modern clients will normally try to reconnect automatically after being disconnected. With this feature enabled, reconnection attempts are rejected if the client's RSSI is still below the threshold.

Once the client's RSSI improves above the threshold, it can associate normally.

Commands

The new command available for this feature is: (**no**) **disconnect-low-signal**

Example To enable low-signal client disconnection on Network 1's VAP with a -60 dBm RSSI threshold, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# disconnect-low-signal
threshold -60
```

You can check a radio's Disconnect-low-signal setting status using **show wireless network**

```
awplus#show wireless network
Network ID 1:
 Description ...................
 Assigned VLAN ID .............. 1
 SSID ........................... allied24
...
 Airtime Percentage ............ 0
 Multicast Unicast conversion .. Disable
 Disconnect Low-Signal Clients . Disable <-----
 RSSI Threshold ................ -75 <-----
 Captive-Portal ................ Disable
  Authentication Mode .......... click-through
   ...
```

Device GUI

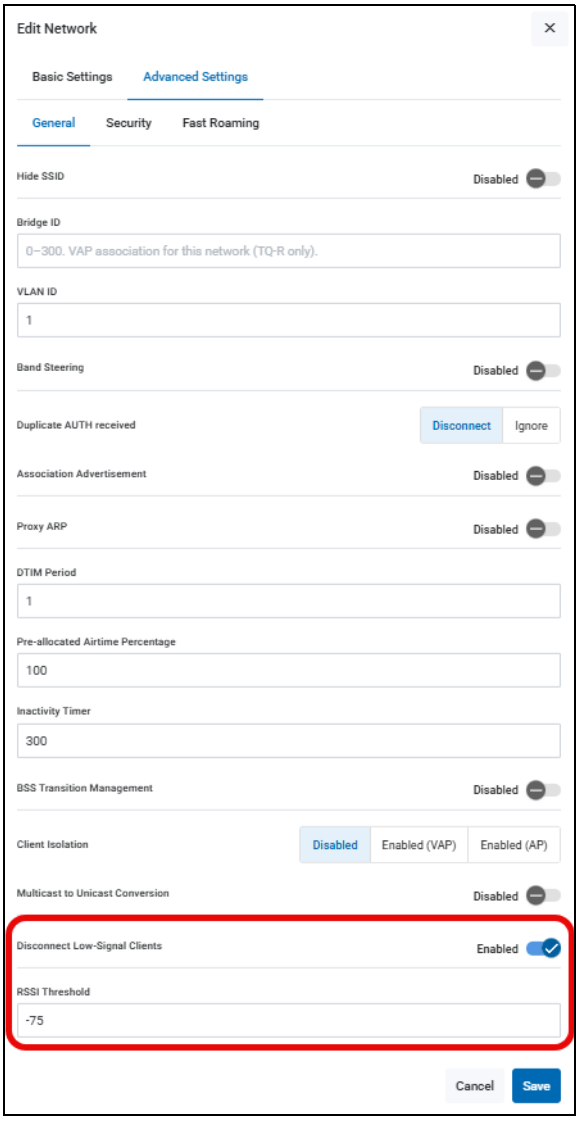
In the Device GUI, the settings to select are called **Disconnect Low-Signal Clients** and **RSSI Threshold**.

You can find these settings in the following places:

On a TQR Series AP

To change the Disconnect Low signal settings for a network:

1. Select **Local Wireless** in the left-hand menu
2. Select the **Profile** tab
3. Click on the + Add Network icon to add a new network, or click the Edit icon on the right-hand side of the network you want to edit.
4. Select **Advanced Settings**



For more information about wireless configuration of TQR Series APs, see Wireless Management for the TQR series using the Device GUI.

Radio Monitor Mode for Wireless APs

Applies to TQR Series

From version 5.5.6-0.2 onwards, the TQR Series devices support radio Monitor Mode.

Monitor Mode enables a wireless radio interface to operate as a dedicated air-sniffing scanner rather than functioning as a standard access point radio. It provides the scan data required for features such as client location tracking, RF analytics, and other monitoring-based functions. The AWC Plugin uses this information to support device discovery features.

Monitor Mode is enabled by the AWC Plug-in; therefore, it is normally not enabled on the TQR side.

How radio Monitor Mode works

When Monitor Mode is enabled, the radio interface:

- performs continuous channel scanning to collect wireless information, specifically data about nearby STAs (clients).
- scans the wireless channels every 30 seconds.
- does not support client connections or any normal Wi-Fi services. That is, if Monitor Mode is enabled, the radio operates in scan only mode, so the radio status is forced to disabled.

Commands

The new command available for this feature is: (**no) monitor mode**

The AWC Plug-in controls Monitor Mode on wireless AP radios. Even if Monitor Mode has been enabled once, this command allows Monitor Mode to be disabled on the TQR side and re-enables the radio.

Example Use the following commands to disable Monitor Mode on a wireless AP radio 1:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap local
awplus(config-wireless-ap)# radio 1
awplus(config-wireless-ap-radio)# no monitor-mode
awplus(config-wireless-ap-radio)# no force-disable
```

You can check a radio's Monitor Mode status using the **show wireless ap** command:

```
awplus>show wireless ap
 AP ID Local:
 Status ..................... Enable
 Description ................
 AP Profile ................. local
 IP Address ................. 127.0.0.1
 MAC Address ................ 889d.98f6.7f40
 Login Username .............
 Login Password ............. (encrypted)
 Radio 1:
  OverrideRadioStatus ....... Force-disable
  Channel .................... auto
  Power ...................... auto
  Monitor Mode ............... Enable
 Radio 2:
  OverrideRadioStatus .......
  Channel .................... auto
  Power ...................... auto
  Monitor Mode ............... Disable
 Radio 3:
  OverrideRadioStatus ....... Force-disable
  Channel .................... 1
  Power ...................... auto
  Monitor Mode ............... Enable
```

Faster wireless configuration with the AWC Plugin for Vista Manager

Applies to TQR Series APs

This release improves the performance and reliability of applying wireless configurations from the AWC Plugin for Vista Manager, enabling faster and more consistent configuration updates.

For more information about wireless configuration of TQR Series APs from the AWC Plugin for Vista Manager, see Autonomous Wave Control (AWC) Technical Documents.

Change format of Calling-Station-ID

Applies in 5.5.6-0.2 to local wireless configuration on TQR Series APs. Applied in 5.5.6-0.1 to all devices that support the Wireless Controller

From 5.5.6-0.2 and Device GUI 2.23.0 onwards, you can change the format of the MAC address used in the Calling-Station-ID. This is an attribute that the AP sends to a RADIUS server (attribute 43).

By default, the AP uses a format that complies with RFC3580. Therefore, it uses uppercase letters and separates octets with hyphens ("-"). However, some management systems require a different format. If you use one of these management systems, this enhancement lets you change the format.

On TQR Series APs, you can change the format for the AP itself, as well as for networks controlled by the Wireless Controller.

Commands

To change the format for WPA Enterprise (using security instance 1 on network 1 in this example) and apply it to APs, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 1 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# radius calling-station-id
{hyphen|unformatted} {lower-case|upper-case}
awplus(config-wireless-sec-wpa-ent)# exit
awplus(config-wireless)# network 1
awplus(config-wireless-network)# security 1
awplus(config-wireless-network)# exit
awplus(config-wireless)# exit
awplus(config)# exit
awplus# wireless ap-configuration apply ap {local|all|
<ap-id-range>}
```

To change the format for MAC authentication (on network 1 in this example), use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth radius calling-
station-id {hyphen|unformatted} {lower-case|upper-case}
awplus(config-wireless-network)# exit
awplus(config-wireless)# exit
```

```
awplus(config)# exit
awplus# wireless ap-configuration apply ap {local|all|
<ap-id-range>}
```

In both of the **calling-station-id** commands:

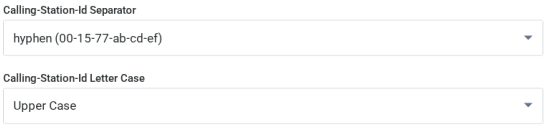
- **hyphen** sets the system to use dashes as separators (e.g. 99-00-AA-BB-CC-DD)
- **unformatted** sets the system to use no separators (e.g. 9900AABBCCDD)
- **lower-case** sets the system to use lower-case letters (e.g. 99-00-aa-bb-cc-dd)
- **upper-case** sets the system to use upper-case letters (e.g. 99-00-AA-BB-CC-DD).

To see the setting, use the commands:

```
awplus# show wireless network
awplus# show wireless security
```

Device GUI

In the Device GUI, the settings to select are called **Calling-Station-Id Separator** and **Calling-Station-Id Letter Case**.



You can find these settings in the following places.

To change the Calling-Station-ID format for a network:

1. Select Local Wireless in the left-hand menu.
2. On the Profile tab, click on the **+ Add Network** icon to add a new network, or click the Edit icon on the right-hand side of the network you want to edit.
3. In the Basic Settings tab, set the security to **WPA Enterprise** and then choose the desired **Calling-Station-Id Separator** and **Calling-Station-Id Letter Case**.

With MAC authentication on a TQR Series AP

To change the Calling-Station-ID format for use with MAC authentication in a network:

1. Select Local Wireless in the left-hand menu.
2. On the Profile tab, click on the **+ Add Network** icon to add a new network, or click the Edit icon on the right-hand side of the network you want to edit.
3. In the Advanced Settings tab, select the Security tab.
4. Set MAC Authentication to **radius** or **MAC Filter + External RADIUS** and then choose the desired **Calling-Station-Id Separator** and **Calling-Station-Id Letter Case**.

Wi-Fi Quality of Service (QoS)

Applies to the TQ7413-R.

From 5.5.6-0.2 and Device GUI 2.23.0 onwards, the Wireless Controller supports QoS.

Each radio in an access point has four QoS egress queues and four ingress queues. The QoS settings control the way the AP stores and handles packets in the queues.

Overview of the QoS settings

There are four types of QoS settings:

- **WiFi Multimedia (WMM)** - this enables QoS
- **No Acknowledgment** - this can help save bandwidth
- **APSD** (Automatic Power Save Delivery) - this can help save client battery life
- **EDCA** (Enhanced Distributed Channel Access) parameters - these control ingress and egress queue settings.

The EDCA parameters are in two sets:

- **AP** parameters - these control the four queues that store **egress** traffic that the AP transmits to the wireless clients.
- **Station** parameters - these control the four queues that store **ingress** traffic that the AP receives from the clients.

Table 2 defines the overall QoS parameters.

Table 2: Overall QoS settings

Parameter	Description
WiFi Multimedia (WMM)	Enable or disable QoS prioritizing and coordination. Here are the options: ■ Enabled: The access point uses the AP EDCA settings to control the flow of downstream traffic to the wireless clients and the station EDCA parameters to control the flow of upstream traffic from the clients. This is the default setting. ■ Disabled: QoS control of the upstream traffic from the clients is disabled. You can still configure some of the parameters that control the downstream traffic from the access point to the clients. WMM must be enabled on radios that use IEEE 802.11n or IEEE 802.11ac.

Table 2: Overall QoS settings (cont.)

Parameter	Description
No acknowledgements	Enable or disable No acknowledgements. Acknowledgements are verification signal data that wireless clients transmit to the access points. The Acknowledgment process takes bandwidth and airtime. Here are the options: ■ Enabled: The access point removes Acknowledgment to improve the amount of data transmission. ■ Disabled: No Acknowledgment is disabled. Acknowledgements are enabled by default.
APSD	Enable or disable Automatic Power Save Delivery (APSD). APSD allows wireless clients to enter standby or sleep mode to in order to save battery while connected to the access point. Here are the options: ■ Enabled: Enable APSD. ■ Disabled: Disable APSD. APSD is disabled by default.

Table 3 defines the AP EDCA parameters.

Table 3: AP EDCA Parameters

AP Parameter	Description
Data Type (Queue)	Lists the four egress queues: ■ Data 0 (Voice): High priority queue, with low latency and guaranteed bandwidth. The queue is used to store time-sensitive data, such as VOIP and streaming media. ■ Data 1 (Video): High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as video traffic. ■ Data 2 (Best Effort): Medium priority queue, with minimum throughput and delay. The queue is used to store most traditional IP data. ■ Data 3 (Background): Lowest priority queue, with high throughput. This queue is used for bulk data that requires maximum throughput and is not time-sensitive, such as FTP packets.

Table 3: AP EDCA Parameters (cont.)

AP Parameter	Description
AIFS (InterFrame Space)	Select the Arbitration Inter-Frame Spacing (AIFS) value to control the amount of time the access point waits after transmitting a frame and before transmitting the next frame. Queues with shorter wait times have higher priorities than queues with longer wait times. Here are the guidelines: ■ The wait time is measured in slots. ■ The range is 1 to 15 slots. ■ The defaults are: 1 for Data 0 and Data 1, 3 for Data 2, and 7 for Data 3.
cwMin (Minimum Contention Window)	Enter a value (in milliseconds) to be the lower limit of the range from which the access point determines the initial random back-off wait time for resending packets during transmission conflicts. Here are the guidelines: ■ The access point generates the first random number between 0 and this number. ■ If the first random back-off wait time expires before the data frame is sent, a retry counter is increased and the random back-off value (window) is doubled. Doubling continues until the size of the random back-off value reaches the number defined in the maximum contention window. ■ Valid values for this parameter are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. ■ This parameter must be lower than the cwMax value. ■ The defaults are: 3 for Data 0, 7 for Data 1, and 15 for Data 2 and Data 3.

Table 3: AP EDCA Parameters (cont.)

AP Parameter	Description
cwMax (Maximum Contention Window)	Select the maximum contention window, which is the upper limit (in milliseconds) for doubling the random back-off value. The doubling continues until either the data frame is sent or the maximum contention size is reached. Once the maximum contention window is reached, retries continue until a maximum number of retries is reached. Here are the guidelines: ■ This parameter must be greater than or equal to the cwMin value. ■ Valid values are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. ■ The default values are: 7 for Data 0, 15 for Data 1, 63 for Data 2, and 1023 for Data 3.
Max. Burst (unit: ms)	Specifies the maximum burst length for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Here are the guidelines: ■ This is an AP EDCA parameter only and as such applies only to egress traffic from the access point to the wireless clients. ■ The factory defaults are: 1500 for Data 0, 3000 for Data 1, and 0 for Data 2 and Data 3. ■ The range is 0 to 8100 milliseconds.

Table 4 defines the Station EDCA parameters.

Table 4: Station EDCA Parameters

Station Parameter	Description
Data Type (Queue)	Lists the four egress queues: ■ Data 0 (Voice) - High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as VoIP and streaming media. ■ Data 1 (Video): High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as video traffic. ■ Data 2 (Best Effort): Medium priority queue, with minimum throughput and delay. The queue is used to store most traditional IP data. ■ Data 3 (Background): Lowest priority queue, with high throughput. This queue is used for bulk data that requires maximum throughput and is not time-sensitive, such as FTP packets.
AIFS (InterFrame Space)	Select the Arbitration Inter-Frame Spacing (AIFS) value to control the wait time for data frames. The wait time is measured in slots and has the range 1 to 15 slots. Queues with shorter wait times have higher priorities than queues with longer wait times. Here are the guidelines: ■ The wait time is measured in slots. ■ The range is 1 to 15 slots. ■ The defaults are: 2 for Data 0 and Data 1, 3 for Data 2, and 7 for Data 3.

Table 4: Station EDCA Parameters (cont.)

Station Parameter	Description
cwMin (Minimum Contention Window)	Enter a value (in milliseconds) to be the lower limit of the range from which the station determines the initial random back-off wait time for resending packets during transmission conflicts. Here are the guidelines: ■ The first random number the station generates will be between 0 and this number. ■ If the first random back-off wait time expires before the data frame is sent, a retry counter is increased and the random back-off value (window) is doubled. Doubling continues until the size of the random back-off value reaches the number defined in the maximum contention window. ■ This parameter must be less than or equal to the cwMax value. ■ Valid values for this parameter are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023 milliseconds. ■ The defaults are: 3 for Data 0, 7 for Data 1, and 15 for Data 2 and Data 3.
cwMax (Maximum Contention Window)	Select the maximum contention window, which is the upper limit (in milliseconds) for doubling the random back-off value. The doubling continues until either the data frame is sent or the maximum contention size is reached. Once the maximum contention window is reached, retries continue until a maximum number of retries is reached. Here are the guidelines: ■ This parameter must be greater than or equal to the cwMin value. ■ Valid values are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. ■ The default values are: 7 for Data 0, 15 for Data 1, and 1023 for Data 2 and Data 3.
TXOP Limit	Select the Transmission Opportunity (TXOP) limit. It defines the time intervals that a WME client has the right to initiate transmission to the access point. Here are the guidelines: ■ The time intervals are in 32 microseconds. ■ The range is 0 to 256 intervals. ■ The default intervals are: 47 for Data 0, 94 for Data 1, and 0 for Data 2 and Data 3.

Commands

To enable QoS by enabling WiFi Multimedia, use the commands:

Enable WMM

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile 1
awplus(config-wireless-ap-prof)# radio 1
awplus(config-wireless-ap-prof-radio)# wmm enable
```

In the same mode, you can also enable APSD, disable acknowledgements, and change the ECDA settings. Use the commands:

Enable APSD

```
awplus(config-wireless-ap-prof-radio)# apsd enable
```

Disable acknowledgement

```
awplus(config-wireless-ap-prof-radio)# no
acknowledgements enable
```

Set EDCA for APs

```
awplus(config-wireless-ap-prof-radio)#edca-parameters ap
{background|best-effort|video|voice}
[aifs <1-15>|ecw-min <0-15>|ecw-max <0-15>|max-burst <0-
8100>]
```

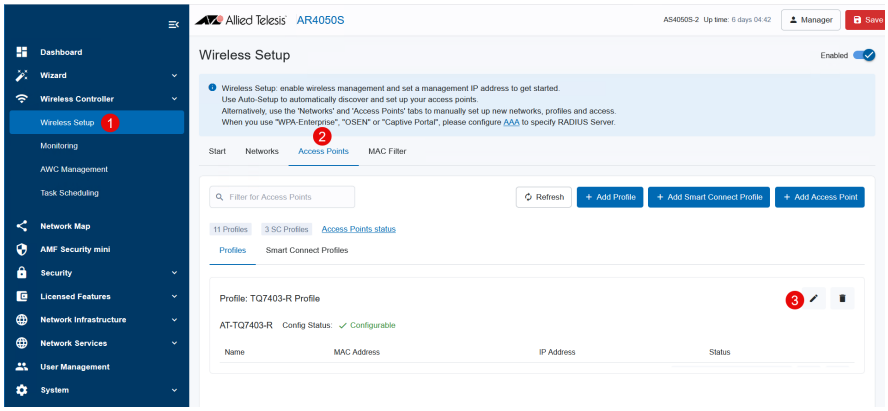
Set EDCA for stations

```
awplus(config-wireless-ap-prof-radio)#edca-parameters sta
{background|best-effort|video|voice}
[aifs <1-15>|ecw-min <0-15>|ecw-max <0-15>|txop <0-255>]
```

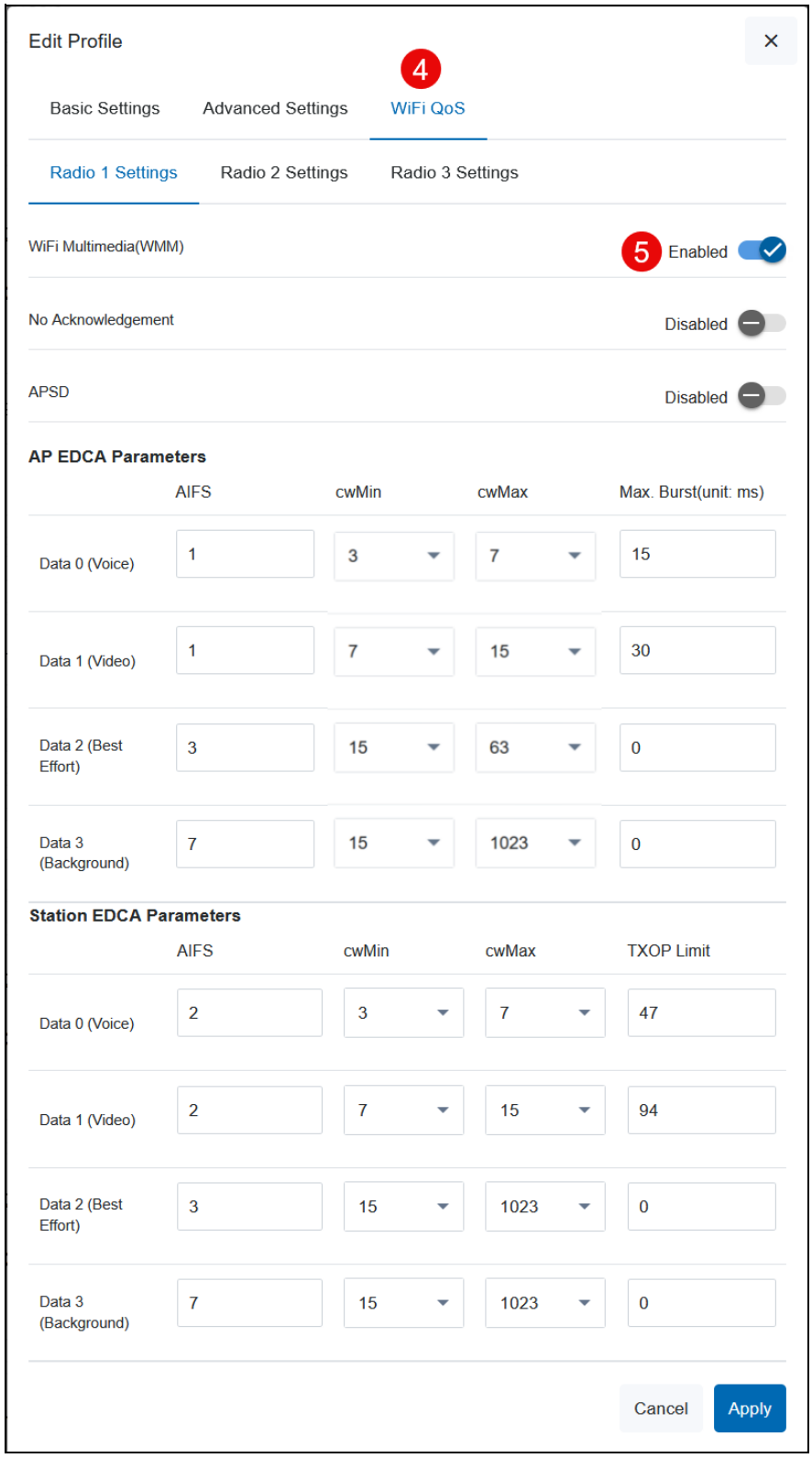
Device GUI

To enable and configure QoS, do the following steps:

1. Select **Wireless Controller > Wireless Setup** in the left-hand menu.
2. Select the **Access Points** tab.
3. Click on the **+ Add Profile** icon to add a new profile, or click the **Edit** icon on the right-hand side of the profile you want to edit.



4. Select the **WiFi QoS** tab.
5. Depending on the radio, you may need to enable **WiFi Multimedia (WMM)**. As well as enabling QoS processing, this makes the EDCA parameters display.
6. Configure the other settings if required and click **Apply**.



Issues Resolved in Version 5.5.6-0.2

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

CR	Module	Description	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2 / SBx908 GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200S	TQR Series
CR-89856	**AWC**	Previously, reapplying wireless configuration while using the multicast-to-unicast conversion feature could cause a system reboot. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y
CR-89884	**AWC**	Previously, using the **power-channel calculate** feature could cause a system reboot if multicast-to-unicast conversion was used. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y
CR-88919	**AWC Captive Portal**	Previously, 2-step authentication was only being pulled from AWC if MAC authentication was set to RADIUS. If other authentication methods were used, the pull command was not retrieving the 2-step configuration from AWC. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y
CR-90104	**MACsec**	Previously, on x240-52 platforms MACsec was not able to be configured on uplink ports. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

CR	Module	Description	GS970EMX	XS900MX	GS980M	GS980MX	GS980EM	IE220	IE210L	IE340\IE340L	IE360	IE560/12GSX	SE540/SE540L	SE250	SE240	x220	x240	x250	x320	x330	x540L	x530, x530L	x550	x930	x950	SBx8100 CFC960	SBx908 GEN2 / SBx908 GEN3	AR1050V	AR3050S	AR4050S / AR4050S-5G	10GbE UTM Firewall/AR4000S-Cloud	AMF Cloud	ARX200S	TQR Series
CR-90007	**PKI, SSL**	Previously, the default self-signed certs would unnecessarily re-generate at bootup. 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	Y

What's New in Version 5.5.6-0.1 and Device GUI 2.23.0

Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.6-0.1 and Device GUI version 2.23.0.

AlliedWare Plus file details are listed in Table 1 on the next page. You can obtain the AlliedWare Plus and Device GUI 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 76.

For instructions on how to update the web-based GUI, see "Accessing and Updating the Web-based GUI" on page 78. 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. Note that 5.5.6-0.1 does not support TQR Series access points.

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Plus Cloud		03/2026	■ VAA OS: vaa-5.5.6-0.1.iso ■ For AWS: vaa-5.5.6-0.1.vhd and upload_vhd.py ■ For Microsoft Azure: vaa_azure-5.5.6-0.1.vhd
SBx81CFC960	SBx8100	03/2026	SBx81CFC960-5.5.6-0.1.rel
SBx908 GEN3	SBx908 GEN3	03/2026	SBx90xGEN3-5.5.6-0.1.rel
SBx908 GEN2	SBx908 GEN2	03/2026	SBx908NG-5.5.6-0.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ x950-52XTQm	x950	03/2026	x950-5.5.6-0.1.rel

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

Models	Family	Date	Software File
x930-28GTX x930-28GPX x930-28GSTX x930-52GTX x930-52GPX	x930	03/2026	x930-5.5.6-0.1rel
x560-28YSQ	x560	03/2026	x560-5.5.6-0.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	03/2026	x550-5.5.6-0.1.rel
x540L-28XTm x540L-28XS	x540L	03/2026	x540-5.5.6-0.1.rel
x530-10GHXm x530-18GHXm x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530DP-28GHXm x530DP-52GHXm	x530	03/2026	x530-5.5.6-0.1.rel
x530L-10GHXm x530L-18GHXm x530L-28GTX x530L-28GPX x530L-52GTX x530L-52GPX	x530L	03/2026	x530-5.5.6-0.1.rel
x330-10GTX x330-20GTX x330-28GTX x330-52GTX	x330	03/2026	x330-5.5.6-0.1.rel
x320-10GH x320-11GPT	x320	03/2026	x320-5.5.6-0.1.rel
x250-18XS x250-18XTm x250-28XS x250-28XTm	x250	03/2026	x250-5.5.6-0.1.rel
x240-10GTXm x240-10GHXm x240-26GHXm	x240	03/2026	x240-5.5.6-0.1.rel
x220-28GS x220-52GT x220-52GP	x220	03/2026	x220-5.5.6-0.1.rel
IE560-12GSX	IE560	03/2026	IE560-5.5.6-0.1.rel
IE360-12GTX IE360-12GHX	IE360	03/2026	IE360-5.5.6-0.1.rel
IE340-12GT IE340-12GP IE340-20GP IE340L-18GP	IE340	03/2026	IE340-5.5.6-0.1.rel
IE220-6GHX IE220-10GHX	IE220	03/2026	IE220-5.5.6-0.1.rel
IE210L-10GP IE210L-18GP	IE210L	03/2026	IE210-5.5.6-0.1.rel
SE540L-28XTm SE540L-28XS	SE540L	03/2026	SE540-5.5.6-0.1.rel

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

Models	Family	Date	Software File
SE250-18XS SE250-18XTm SE250-28XS SE250-28XTm	SE250	03/2026	SE250-5.5.6-0.1.rel
SE240-10GTXm SE240-10GHXm	SE240	03/2026	SE240-5.5.6-0.1.rel
XS916MXT XS916MXS	XS900MX	03/2026	XS900-5.5.6-0.1.rel
GS980MX/10HSm GS980MX/18HSm GS980MX/28 GS980MX/28PSm GS980MX/52 GS980MX/52PSm	GS980MX	03/2026	GS980MX-5.5.6-0.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	03/2026	GS980EM-5.5.6-0.1.rel
GS980M/52 GS980M/52PS	GS980M	03/2026	GS980M-5.5.6-0.1.rel
GS970EMX/10 GS970EMX/20 GS970EMX/28	GS970EMX	03/2026	GS970EMX-5.5.6-0.1.rel
AR4000S-Cloud		03/2026	Various files depending on deployment. See the Allied Telesis Support Portal.
ARX200S-GT ARX200S-GTX	ARX200S	03/2026	ARX200S-5.5.6-0.1.rel
10GbE UTM Firewall app		03/2026	ATVSTAPL-1.14.1.iso and vfw-x86_64-5.5.6-0.1.app
AR4050S AR4050S-5G AR3050S	AR-Series UTM firewalls	03/2026	AR4050S-5.5.6-0.1.rel AR3050S-5.5.6-0.1.rel
AR1050V	AR-Series VPN routers	03/2026	AR1050V-5.5.6-0.1.rel

Caution: Software version 5.5.6-0.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 5.5.6 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.6 license installed, that license also covers all later 5.5.6 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 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

The SBx908 GEN3 switch does not require a release license.

Unsupported products

AlliedWare Plus version 5.5.6-0.1 and later do not support x230, x230L and GS970M series switches. The last version that supports these products is 5.5.5-2.x. The following models are not supported:

- x230-10GP
- x230-10GT
- x230-18GP
- x230-18GT
- x230-28GP
- x230-28GT
- x230L-17GT
- x230L-26GT
- GS970M/10PS
- GS970M/10
- GS970M/18PS
- GS970M/18
- GS970M/28PS
- GS970M/28

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

The 5.5.6-0.1 software version is **not** ISSU compatible with previous software versions.

New Features and Enhancements

This section summarizes the new features and enhancements in 5.5.6-0.1 and Device GUI 2.23.0.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 69.

Enhancements in AlliedWare Plus 5.5.6-0.1

Enhancements in Device GUI 2.23.0

Low RSSI Client Disconnection (per VAP)

Applies to all devices that support the Wireless Controller

Overview

From 5.5.6-0.1 and Device GUI 2.23.0 onwards, APs can disconnect wireless clients whose RSSI falls below a configurable threshold and prevent them from reconnecting until signal strength improves.

The feature is configurable per VAP and includes enable/disable control and an RSSI threshold range of –90 dBm to 0 dBm. This helps improve overall wireless performance by preventing low-signal clients from degrading network quality.

What this feature does

This feature automatically disconnects wireless clients (STAs) whose signal strength (RSSI) drops below a configured threshold. It also prevents those low-signal clients from reconnecting until their signal strength improves.

Why this matters

Clients with very low RSSI can:

- Cause poor performance
- Increase retransmissions
- Degrade overall wireless network quality

This feature helps maintain better network stability and performance by removing weak connections.

Key behavior to be aware of

Modern clients will normally try to reconnect automatically after being disconnected. With this feature enabled, reconnection attempts are rejected if the client's RSSI is still below the threshold.

Once the client's RSSI improves above the threshold, it can associate normally.

Commands

The new command available for this feature is: (**no**) **disconnect-low-signal**

Example

To enable low-signal client disconnection on Network 1's VAP with a -60 dBm RSSI threshold, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# disconnect-low-signal
threshold -60
```

You can check a radio's Disconnect-low-signal setting status using **show wireless network**

```
awplus#show wireless network
Network ID 1:
 Description ...................
 Assigned VLAN ID ............. 1
 SSID ......................... allied24
...
 Airtime Percentage ............ 0
 Multicast Unicast conversion .. Disable
 Disconnect Low-Signal Clients . Disable <-----
 RSSI Threshold ................ -75 <-----
 Captive-Portal ................ Disable
  Authentication Mode .......... click-through
   ...
```

Device GUI

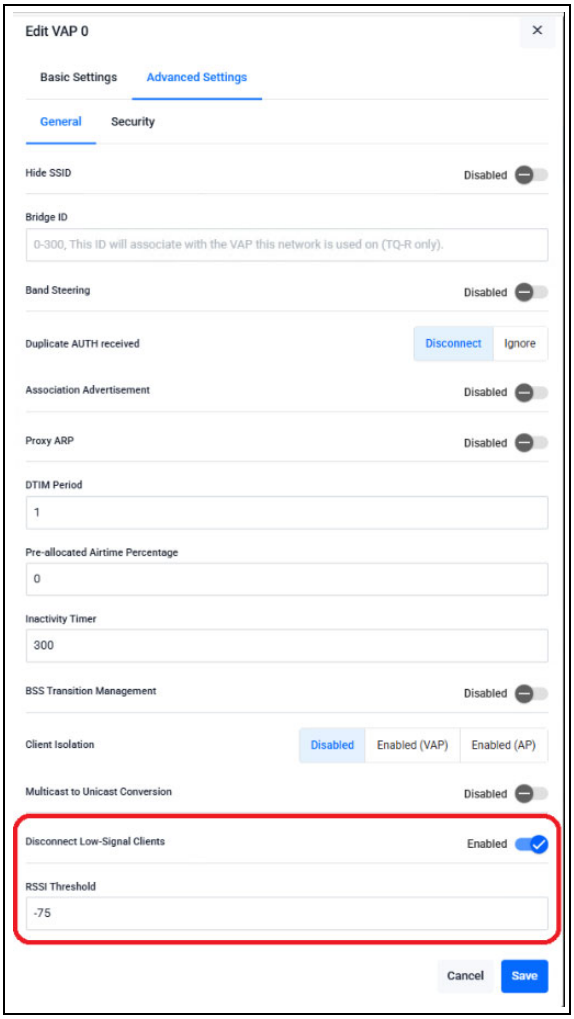
In the Device GUI, the settings to select are called **Disconnect Low-Signal Clients** and **RSSI Threshold**.

You can find these settings in the following places:

On the Wireless Controller

To change the Disconnect Low signal settings for a network:

1. Select **Wireless Controller > Wireless Setup** in the left-hand menu.
2. Select the **Networks** tab.
3. Click on the + Add Network icon to add a new network, or click the Edit icon on the right-hand side of the network you want to edit.
4. Select **Advanced Settings**



Enhanced Control Over Wireless Configuration Application

Applies to all platforms that support the Wireless Controller

Overview

From 5.5.6-0.1 and Device GUI 2.23.0 onwards, you can control when wireless Access Points (APs) apply configuration changes, helping to prevent unexpected wireless service interruptions.

Background

Previously, when restoring a backup, updating firmware, or performing similar operations using the Wireless Controller, wireless configurations were automatically applied to managed APs. During this process, wireless communication could be interrupted for several minutes.

For environments that require strict control over wireless availability, these automatic interruptions could be disruptive if they occurred outside planned maintenance windows.

What's New

Administrators can now choose whether AP configurations are applied automatically or manually after an AP joins AWC management.

When manual application is enabled:

- Automatic configuration application is skipped
- Wireless interruptions are avoided
- Configuration changes can be applied manually or during scheduled maintenance tasks

Important Notes

- This feature is controlled by a global setting and applies to all managed APs.

Commands

This feature supports the command: **`config-apply manual`**

When enabled, administrators must manually apply AP configurations using the command: **wireless ap-configuration apply**

Example To enable manual application of AP configuration after an AP has joined AWC management, use the commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# config-apply manual
```

Updated show command output

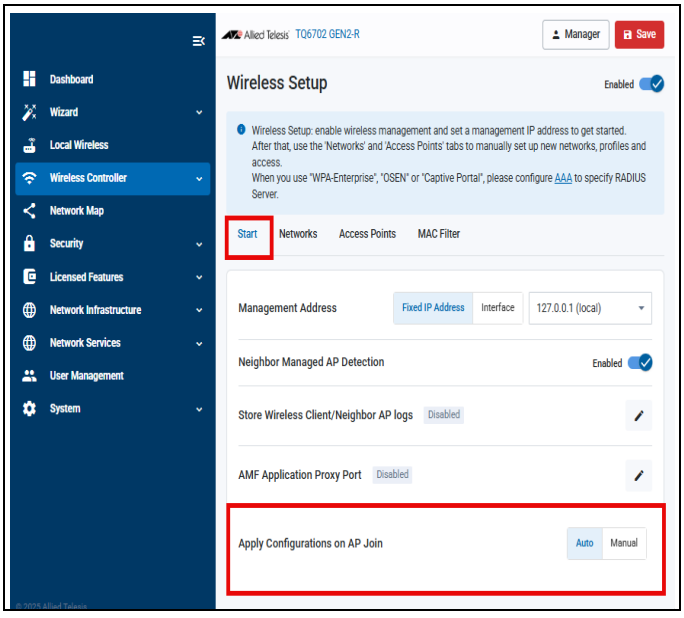
You can check the status of this feature using **show wireless**

```
- For Switch/Router products
awplus# show wireless
Wireless Controller Mode ........ Enable
Management IP Address ........... 192.168.8.30
Rogue AP Detection ..............  Enable
Neighbor Managed AP Detection ... Enable
Emergency Mode ..................  Active
 Activated User .................  admin
 Activated Time .................  2020-02-19 12:11:33
Emergency USB Trigger ...........  Enable
 Trigger Key 1 ..................  TestKey1
  Description ...................  ABC School
 Trigger Key 2 ..................  Test Key2
  Description ...................  DEF School
Log .............................  Enable
Log Destination .................  USB
Log Size Wireless Client ........  5000
Log Rotate Wireless Client ......  100
Log Rotate neighbor AP ..........  100
Log Interval neighbor AP ........  60
Wireless AMF Application Proxy
 Port Status ....................  Enable
 Port Number ....................  5443
Configuration Apply Mode ........ Manual
```

Device GUI

To locate the **Apply Configurations on AP Join** feature, go to:

- Wireless Controller > Wireless Setup > Start



Change format of Calling-Station-ID

Applies to all devices that support the Wireless Controller

From 5.5.6-0.1 and Device GUI 2.23.0 onwards, you can change the format of the MAC address used in the Calling-Station-ID. This is an attribute that the AP sends to a RADIUS server (attribute 43).

By default, the AP uses a format that complies with RFC3580. Therefore, it uses uppercase letters and separates octets with hyphens ("-"). However, some management systems require a different format. If you use one of these management systems, this enhancement lets you change the format.

Commands

To change the format for WPA Enterprise (using security instance 1 on network 1 in this example) and apply it to APs, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# security 1 mode wpa-enterprise
awplus(config-wireless-sec-wpa-ent)# radius calling-station-id
{hyphen|unformatted} {lower-case|upper-case}
awplus(config-wireless-sec-wpa-ent)# exit
awplus(config-wireless)# network 1
awplus(config-wireless-network)# security 1
awplus(config-wireless-network)# exit
awplus(config-wireless)# exit
awplus(config)# exit
awplus# wireless ap-configuration apply ap {local|all|
<ap-id-range>}
```

To change the format for MAC authentication (on network 1 in this example), use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# network 1
awplus(config-wireless-network)# mac-auth radius calling-
station-id {hyphen|unformatted} {lower-case|upper-case}
awplus(config-wireless-network)# exit
awplus(config-wireless)# exit
awplus(config)# exit
awplus# wireless ap-configuration apply ap {local|all|
<ap-id-range>}
```

In both of the **calling-station-id** commands:

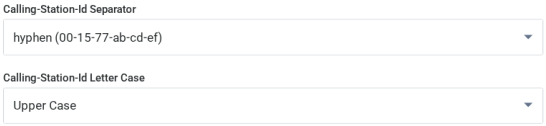
- **hyphen** sets the system to use dashes as separators (e.g. 99-00-AA-BB-CC-DD)
- **unformatted** sets the system to use no separators (e.g. 9900AABBCCDD)
- **lower-case** sets the system to use lower-case letters (e.g. 99-00-aa-bb-cc-dd)
- **upper-case** sets the system to use upper-case letters (e.g. 99-00-AA-BB-CC-DD).

To see the setting, use the commands:

```
awplus# show wireless network
awplus# show wireless security
```

Device GUI

In the Device GUI, the settings to select are called **Calling-Station-Id Separator** and **Calling-Station-Id Letter Case**.



You can find these settings in the following places.

With WPA Enterprise on the Wireless Controller

To change the Calling-Station-ID format for a network:

1. Select **Wireless Controller > Wireless Setup** in the left-hand menu.
2. Select the Networks tab.
3. Click on the **+ Add Network** icon to add a new network, or click the Edit icon on the right-hand side of the network you want to edit.
4. In the Basic Settings tab, set the security to **WPA Enterprise** and then choose the desired **Calling-Station-Id Separator** and **Calling-Station-Id Letter Case**.

With MAC authentication on the Wireless Controller

To change the Calling-Station-ID format for use with MAC authentication in a network:

1. Select Wireless Setup in the Wireless Controller menu.
2. Select the Networks tab.
3. Click on the **+ Add Network** icon to add a new network, or click the Edit icon on the right-hand side of the network you want to edit.
4. In the Advanced Settings tab, select the Security tab.
5. Set MAC Authentication to **radius** or **MAC Filter + External RADIUS** and then choose the desired **Calling-Station-Id Separator** and **Calling-Station-Id Letter Case**.

Specify an interface for AP management

Applies to all devices that support the Wireless Controller

From 5.5.6-0.1 and Device GUI 2.23.0 onwards, you can select an interface for AP management, instead of an address.

You need to do this if the device acting as the Wireless Controller learns its IP address by DHCP. Otherwise, with DHCP the configuration will fail to apply on boot. This is because the device hasn't yet learned its IP address so cannot use that address as the management address. Also, the DHCP lease could also run out and the address change.

Commands

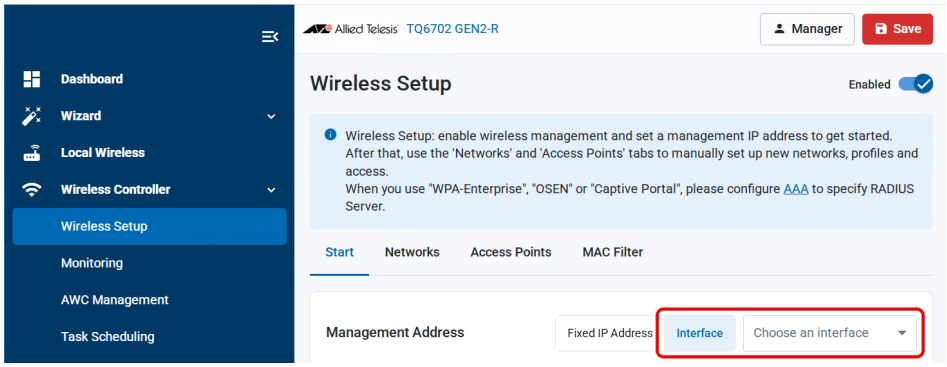
To set an interface for management, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# management interface <interface-name>
```

Device GUI

To set an interface for management:

1. Select **Wireless Controller > Wireless Setup** in the left-hand menu.
2. In the Management Address field on the Start tab, select Interface and choose the interface from the drop-down list.



New Task Scheduling page

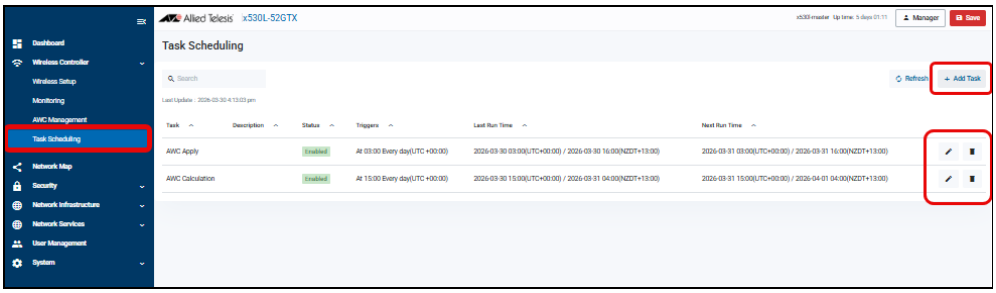
Applies to all devices supporting the Wireless Controller

From Device GUI version 2.23.0 onwards (using version 5.5.6-0.1 and later), the **Tasks** tab has been removed from the **Monitoring** page on the Wireless Controller. This tab previously supported view and delete actions only.

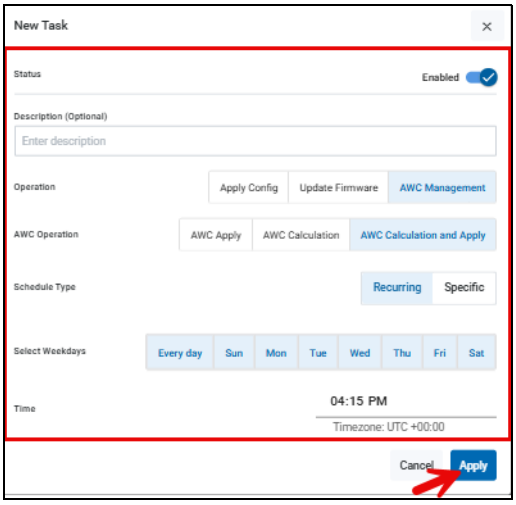
A new **Task Scheduling** page has been introduced in its place. This page provides full task management capabilities, including:

- Creating and deleting tasks
- Editing task configuration
- Enabling and disabling tasks
- Scheduling task execution
- Viewing task details

In the **Task Scheduling** page, you can add, edit, and delete tasks.



When adding or editing a task, click **Apply** to save your configuration.



SNMP Recent Events List update

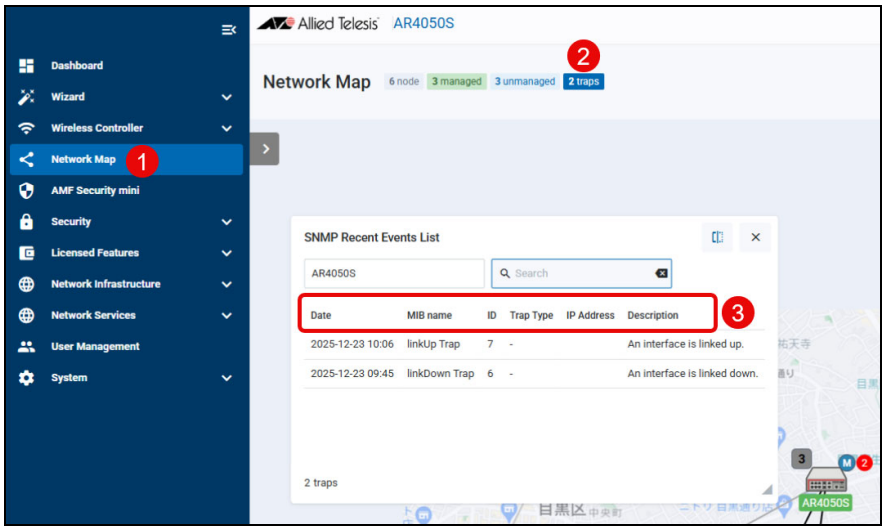
Applies to all devices running AlliedWare Plus

From Device GUI version 2.23.0 (using AlliedWare Plus software version 5.5.6-0.1 onwards), the **Interface** column and related processing have been removed from the **SNMP Recent Events List**.

To access the SNMP Recent Events List:

1. Select **Network Map** from the left-hand menu.
2. Click the **Traps** button or the red circle badge.

3. The **SNMP Recent Events List** opens. The **Interface** column is no longer available.



AMF Plus Cloud supported on Windows Server 2025

From AlliedWare Plus version 5.5.6-0.1 onwards, AMF Plus Cloud is supported on a Host OS of Windows Server 2025.

For installation of AMF Plus Cloud, see the AMF Plus Cloud on Microsoft Hyper-V Installation Guide.

Priority-based Flow Control (PFC) support for SBx908 GEN3

From AlliedWare Plus version 5.5.6-0.1 onwards, Priority-based Flow Control (PFC) is supported on the SBx908 GEN3.

Priority-based Flow Control (PFC) is an enhancement to traditional Ethernet flow control. It allows per-priority pause of traffic rather than pausing all traffic on a link. This lets you provide lossless Ethernet for specific traffic classes (e.g., storage or real-time traffic) by enabling flow control on a per-priority basis.

For more information about PFC, see the Priority-based Flow Control (PFC) Feature Overview and Configuration Guide.

QoS Egress Pool shared memory lossless mode for Priority-based Flow Control (PFC)

Applies to SBx908 GEN3, x560, x540L, and SE540 Series switches

From AlliedWare Plus version 5.5.6-0 onwards, when using Priority-based Flow Control (PFC), you can configure an egress pool to provide lossless traffic priority.

PFC is an enhancement to traditional Ethernet flow control. It allows per-priority pause of traffic rather than pausing all traffic on a link. This lets you provide lossless Ethernet for specific traffic classes (e.g., storage or real-time traffic) by enabling flow control on a per-priority basis.

For PFC to operate in a lossless manner a lossless egress pool must be configured, and all PFC enabled priorities assigned to the lossless pool.

When you have configured the lossless pool, a percentage of the total pool is dedicated to the lossless traffic classes. The remainder of the egress pool is available to the remaining lossy traffic classes. This means that if the lossy traffic consumes its portion of the egress pool, it will not affect the designated lossless traffic classes.

Example: configuring the lossless egress pool

In the following example, you have enabled PFC on port1.0.1. Now, you want to configure the lossless egress pool. You want to add the two PFC enabled priorities, 2 and 3, and allocate a buffer percentage of 10%. This will allow the device to buffer egress data for those priorities.

You can configure this example with the following process.

Step 1: Enter configuration mode

Enter configuration mode for the device. Use the command:

```
awplus# configure terminal
```

Step 2: Enable the lossless egress pool

Enable the lossless egress pool on the device. This will also put the device in **config-qos-egress** mode. Use the command:

```
awplus(config)# mls qos egress-pool lossless
```

Step 3: Assign the priorities

Assign the PFC-enabled priorities to the lossless pool. Use the commands:

```
awplus(config-qos-egress)# priority 2
awplus(config-qos-egress)# priority 3
```

Step 4: Set the buffer percentage

Set the buffer percentage for the lossless pool. Use the command:

```
awplus(config-qos-egress)# buffer-percentage 10
```

Step 5: Return to privileged exec mode

Return to privileged exec mode for the device. Use the command:

```
awplus(config-qos-egress)# end
```

Step 6: Update the config file

Update the config file by writing your changes to the startup config file. Use the command:

```
awplus# write
```

Step 7: Reboot the device

Reboot the device to apply the changes. Use the command:

```
awplus# reboot
```

So now, in our example, the lossless egress pool has been enabled and configured, and the PFC-enabled priorities, 2 and 3, have been added.

Further documentation

For more information about PFC, see the Priority-based Flow Control (PFC) Feature Overview and Configuration Guide.

DCBX Phase 1: ETS and PFC

Applies to: SBx908 GEN3, x560, x540L, and SE540 Series switches

From AlliedWare Plus version 5.5.6-0 onwards, DCBX (Data Center Bridging eXchange protocol) is available for devices configured for Enhanced Transmission Selection (ETS) or Priority-based Flow Control (PFC). For the first phase of implementation, these features transmit their configuration to their neighbors.

DCBX is used by Data Center Bridging (DCB) devices to exchange configuration information with directly connected peers. The protocol may also be used for misconfiguration detection and for configuration of the peer.

DCBX uses LLDP to exchange attributes between two links peers. When DCBX and LLDP are enabled on an interface, the following Type-Length-Value (TLV) elements will be advertised:

Table 1-1: ETS Configuration TLV — D.2.9 of IEEE Std 802.1Q-2018

Field	Description	AlliedWare Plus Support
Willing	Indicates if the device is willing to accept configuration from neighbors	Always 0 to indicate unwilling
Credit Based Shaper	Indicates if the device supports the Credit-based Shaper transmission selection algorithm	Always 0 to indicate unsupported
Max Traffic Classes	Indicates the maximum number of traffic classes the device supports.	Always 0 to indicate support for 8 traffic classes
Priority Assignment Table	Mapping of priority to traffic classes	Mappings as configured by mls qos map cos-queue <0-7> to <0-7>
Traffic Class Bandwidth Table	Indicates the current bandwidth percentage configured for each traffic class	Percentages as configured by mls qos scheduler-set <1-12> wrr-queue group 1 percent <1-100> queue <0-7>
TSA Assignment Table	Indicates the Transmission selection algorithm to be used for each traffic class	ETS (2) for traffic classes configured with wrr-queue and percent. Otherwise Strict Priority (0)

Additionally, if PFC is enabled on an interface, the following TLV elements will be advertised:

Table 1-2: PFC TLV — D.2.11 of IEEE Std 802.1Q-2018

Item	Default profile	Profile1
Willing	Indicates if the device is willing to accept configuration from neighbors	Always 0 to indicate unwilling
MACsec Bypass Capability	Indicates if the device is capable of bypassing MACsec processing when MACsec is disabled	Always 0 to indicate capable
PFC Capability	Indicates the maximum number of traffic classes that simultaneously support PFC on the device	Always 8
PFC Enable	Indicates if PFC is enabled for each the priority	As configured by pfc priority <0-7>

Example: configuring DCBX on a PFC-enabled interface

In the following example, you have enabled PFC on port1.0.1, and configured the lossless egress pool. Now, you want to enable DCBX on port1.0.1. This will allow the interface to advertise its PFC settings.

You can configure this example with the following process.

Step 1: Enter configuration mode

Enter configuration mode for the device. Use the command:

```
awplus# configure terminal
```

Step 2: Enable the DCBX service

Enable the DCBX service on the device. Use the command:

```
awplus(config)# service dcbx
```

Step 3: Enter interface configuration mode

Enter interface configuration mode for port1.0.1. Use the command:

```
awplus(config)# interface port1.0.1
```

Step 4: Enable DCBX for PFC

Enable DCBX for PFC on the interface. Use the command:

```
awplus(config-if)# dcbx pfc
```

Step 5: Return to global configuration mode

Return to global configuration mode for the device. Use the command:

```
awplus(config-if)# exit
```

Step 6: Enable LLDP

Enable LLDP for the interface. Use the command:

```
awplus(config)# lldp run
```

So now, in our example, port1.0.1 is using DCBX to advertise its PFC settings.

Further documentation

For more information about ETS, see the Enhanced Transmission Selection (ETS) Overview and Configuration Guide.

For more information about PFC, see the Priority-based Flow Control (PFC) Feature Overview and Configuration Guide.

SCEP certificate management

Applies to all devices running AlliedWare Plus

From version 5.5.6-0.1 onwards, AlliedWare Plus supports Enrollment over Simple Certificate Enrollment Protocol (SCEP) certificate management. SCEP allows certificates to be signed over a secure HTTP channel. These certificates will be renewed automatically, greatly reducing the maintenance burden of keeping certificates valid on network devices.

How to create a trustpoint based on a certificate signed over SCEP

Use the following steps to create a trustpoint based on an SCEP service. This example creates a trustpoint named 'rolleston'.

1. Enter configuration mode.

```
awplus> enable
awplus# configure terminal
```

Note that PKI commands require maximum user privileges to execute.

2. Declare a trustpoint named 'rolleston' and enter trustpoint configuration mode.

```
awplus(config)# crypto pki trustpoint rolleston
```

You can use any name for the trustpoint, so long as the first character is alphanumeric, and all characters are alphanumeric, underscores, dashes, or periods.

Do not use the names 'local', 'default-selfsigned' or 'default-system' for the trustpoint. These names have special meanings. For all other trustpoint names, this command just instantiates the trustpoint by initializing its storage container.

3. Declare that the trustpoint will use an SCEP server for signing.

```
awplus(ca-trustpoint)# enrollment scep
```

This command affects the process, but doesn't immediately cause any action to be taken. In other words, this command does not result in certificate generation; it only affects how certificate generation will be done later.

4. Specify the SCEP server to communicate with.

```
awplus(ca-trustpoint)# scep-url https://scep.example.com:8443
```

5. Enter the username and password for communicating with the SCEP server.

These commands are required if the SCEP server requires authentication.

```
awplus(ca-trustpoint)# scep-username rolleston-user
awplus(ca-trustpoint)# scep-password rolleston-password
```

6. Declare the keypair that the trustpoint will use.

```
awplus(ca-trustpoint)# rsakeypair rolleston-server-key
```

This step specifies that the trustpoint uses the key pair 'rolleston-server-key' when enrolling the server (creating its certificate). This command does not create the key pair. If the key pair does not exist, it is created later when you run the **crypto pki enroll** command. You can specify the key length here, but if the key already exists with a different length, the parameter is ignored.

7. Leave trustpoint configuration mode.

```
awplus(ca-trustpoint)# end
```

8. If necessary, install the certificate authority (CA) used to sign the root certificate.

```
awplus# crypto pki import default-system
```

If the certificate the server uses for TLS was not signed by one of the default set of root CA certificates, then the CA used to sign that certificate must be installed as a trusted root CA certificate.

9. Retrieve the CA certificate that the SCEP server will use to sign the server certificate.

```
awplus# crypto pki authenticate rolleston
```

10. Create the server certificate.

```
awplus# crypto pki enroll rolleston
```

This command creates the server certificate. This is a single-step process for a trustpoint with an SCEP certificate authority. This process:

- Creates the server certificate for the local device using the RSA key pair specified in the trustpoint parameters.
- Generates the key pair if the key pair specified in the **rsakeypair** command does not exist.
- Creates a new key pair named after the trustpoint if the **rsakeypair** command was not executed for this trustpoint.

By default, the subject name of the server certificate has the CN (common name) field set to the fully qualified domain name of the system, since that is commonly required when other systems validate the subject name. However, you can substitute a subject name of your choice by using the **subject** command in trustpoint-configuration mode. The device will then communicate with the SCEP server to have its own server certificate signed.

At this point, the trustpoint is set up. It contains the:

- trustpoint's SCEP root CA certificate
- server RSA public/private keys
- trustpoint's own server certificate, signed by the SCEP root CA certificate.

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

Maximum Receive Unit (MRU) support for switchports added to some switches

Added to SBx908 GEN3, x560, x540L and SE540 Series switches

From version 5.5.6-0.1 onwards, you can set an MRU on switchports on the above switch families. Note that some other switches already support setting an MRU.

The MRU of an interface indicates the largest size of a packet that the interface can accept. When a device receives packets whose size is greater than the interface MRU, it drops those packets.

The MRU can be from 68 to 10240 bytes (the jumbo frame size).

Note that the MRU sizes specify the payload only. For an Ethernet frame, provision is made (internally) for header components, which increase the frame size internally by 22 bytes. For example, once the header is added, the default frame size is 1522 bytes.

To set the MRU, use the commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface <port>
awplus(config-if)# mru <68-10240>
```

Note that you can also set a Maximum Transmit Unit (MTU) on switchports. The MRU and MTU can be different.

MACsec support added to XEMs on SBx908 GEN3

From version 5.5.6-0.1 onwards, MACsec (Media Access Control Security) is supported on XEM3-12YS, XEM3-8CQ and XEM3-2DQ modules on the SBx908 GEN3.

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

Number of multicast routes increased on SBx908 GEN3

From version 5.5.6-0.1 onwards, the SBx908 GEN3 supports up to 32K multicast routes with IPv4 PIM-SM and IGMP.

To make this increase available, you need to enable the silicon-profile named “profile1”. Use the commands:

```
awplus# configure terminal
awplus(config)# platform silicon-profile profile1
```

New SNMP trap for testing connectivity

Applies to all AlliedWare Plus devices

From version 5.5.6-0.1 onwards, a new private SMNP trap is available for testing connectivity between the AlliedWare Plus device and an SNMP manager. The new trap is called atSample.

The objects for the new trap are:

- atSnmpTest OBJECT IDENTIFIER ::= { sysinfo 30 }
- atSnmpTestTrap OBJECT IDENTIFIER ::= { atSnmpTest 0 }
- atSample TRAP-TYPE ::= { atSnmpTestTrap 1 }

You can now also direct the test to a specific host.

To send this test trap, use the command:

```
awplus# test snmp trap snmp atsample [<host-address>]
```

The host address is a valid IPv4 or IPv6 address, and must exist as an SNMP host. If you don't specify a host address, the test trap is sent to all trap hosts.

Previously, you could use this command to test the connectivity by sending either a coldStart or warmStart trap. However, using these traps could be confusing, so the new trap has been created to avoid that confusion. You can still use these traps instead of the new trap if you prefer.

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

AMF Plus master support added to IE560-12GSX

From version 5.5.6-0.1 onwards, IE560-12GSX switches can act as an AMF Plus master switch, controlling up to 20 nodes.

AMF Plus is the Allied Telesis Autonomous Management Framework™ Plus - a suite of features that simplify network management from the core to the edge.

For more information about AMF Plus, see the AMF Plus Feature Overview and Configuration Guide. For license details, see the IE560-12GSX datasheet.

OpenFlow service now disabled by default

Applies to all AlliedWare Plus products that support OpenFlow

From version 5.5.6-0.1 onwards, the OpenFlow service is no longer enabled by default. To enable the service, use the commands:

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

If you have already configured OpenFlow on your switch and you upgrade to 5.5.6-0.1 or later, the switch will automatically enable the OpenFlow service. You do not have to change your configuration.

If you use 5.5.6-0.1 or later to configure OpenFlow for the first time, you need to enter this command before configuring OpenFlow.

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

SSL and SSH upgrades

Applies to all AlliedWare Plus products

From 5.5.6-0.1 onwards, SSL and SSH have been upgraded to enhance security.

AlliedWare Plus no longer supports DSA or Finite-field Diffie-Hellman. This could impact SSH connections with very old devices.

RADIUS over TLS (RadSec) support for TLSv1.3

Applies to all AlliedWare Plus products that support local RADIUS server

From 5.5.6-0.1 onwards, RADIUS over TLS (RadSec) supports TLSv1.3 when connecting to a peer device.

Customers and administrators do not need to take any action because of this enhancement:

- If the peer device also supports TLSv1.3, then v1.3 will be used automatically.
- If the peer device does not support TLSv1.3, then v1.2 will be used automatically, as before.

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

ECDSA certificate support in PKI trustpoints

Applies to all AlliedWare Plus products

From version 5.5.6-0.1 onwards, trustpoints can use ECDSA as the certificate algorithm, as well as or instead of RSA. Devices now maintain both RSA and ECDSA certificate chains simultaneously within a single trustpoint, allowing modern clients to use ECDSA while supporting older clients that require RSA.

By default, trustpoints generate both ECDSA (curve size of 384 bits) and RSA (2048 bits) certificates and keys. This means:

- The default self-signed trustpoint automatically generates both RSA and ECDSA keys on first boot-up (unless keys already exist)
- The device generates both RSA and ECDSA certificates automatically when processing the **crypto pki authenticate** and **crypto pki enroll** commands.

Additionally, the AlliedWare Plus HTTP server now supports multiple server certificates from multiple trustpoints. It now has:

- **Multiple trustpoints**: you can configure HTTP to use multiple trustpoints
- **All certificates loaded**: the HTTP server loads and presents all RSA and ECDSA certificates from all configured trustpoints
- **Client-driven selection**: TLS client negotiation determines which certificate is used
- **Algorithm restriction**: You can restrict which algorithm types it can use.

Command changes - Key generation and use in trustpoints

To generate an ECDSA public/private key pair, use the command:

```
awplus# crypto key generate ecdsa [label <label>] [256|384|
521]
```

You can use the generated key for multiple server certificates.

The **label** identifies the key in other commands. If you do not specify a label, the key will be labeled "server-default". The label must start with an alphanumeric character, and can only contain alphanumeric characters, underscores, dashes, and dots (periods). The maximum length of the label is 63 characters.

The key curve size can be **256**, **384** or **521** bits. The default is 384.

To use that key pair when enrolling the local server with a trustpoint (named 'tp1' in this example), use the commands:

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint tp1
awplus(ca-trustpoint)# eckeypair <label>
```

You can also generate a key directly when enrolling the local server. Use the commands:

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint tp1
awplus(ca-trustpoint)# eckeypair <label> [256|384|521]
```

The key curve size will only be used when enrolling the server, and can be **256**, **384** or **521** bits. The default is 384.

When authenticating a trustpoint, AlliedWare Plus now generates both RSA and ECDSA CA certificates:

```
awplus# crypto pki authenticate tp1
Generating 2048-bit key for RSA local CA...
Generating P-384 ECDSA key for ECDSA local CA...
Successfully authenticated trustpoint "tp1".
```

When enrolling the server to the trustpoint, AlliedWare Plus now generates both RSA and ECDSA certificates. In this example, it uses the default key pairs:

```
awplus# crypto pki enroll tp1
Using private key "server-default"...
Using ECDSA private key "server-default-ecdsa"...
Successfully enrolled the local server.
Successfully created ECDSA server certificate.
```

The following show commands now show ECDSA certificate information:

```
awplus# show crypto pki trustpoint
awplus# show crypto pki certificates
awplus# show crypto key mypubkey [ecdsa|rsa] [<label>]
```

Command changes - HTTP server

To decide which certificate type the HTTP server can use for TLS handshakes, use the commands:

```
awplus# configure terminal
awplus(config)# http certificate-algorithm [ecdsa|rsa|all]
```

The default is **all**, which allows both ECDSA and RSA certificates.

To use multiple trustpoints with the HTTP server, use the commands:

```
awplus# configure terminal
awplus(config)# http trustpoint <namelist>
```

The names are space-separated, for example **http trustpoint tp1 tp2 tp3**.

For more information about trustpoints, see the PKI 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:

- Changes that may affect device or network configuration
- Limits to upgrade compatibility on SwitchBlade x908 GEN2, x950 and x930 Series switches

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

- Software release licensing
- Upgrading a VCStack with rolling reboot
- Forming or extending a VCStack with auto-synchronization
- AMF 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 5.5.5-1.x version, please check the 5.5.5-2.x release note as well. Release notes are available from our website, including:

- 5.5.5-x.x release notes
- 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

Changes that may affect device or network configuration

Summary	Affected devices	Detail
Telnet is deprecated	All AlliedWare Plus devices	For security reasons, Telnet is deprecated in 5.5.6-0.1 and will no longer be maintained. Do not use Telnet; use SSH instead. While Telnet commands are still available in 5.5.6-0.x, Telnet is disabled by default. Telnet commands should be limited to use only in testing environments.

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 63 and "Details for x930 Series" on page 63 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.

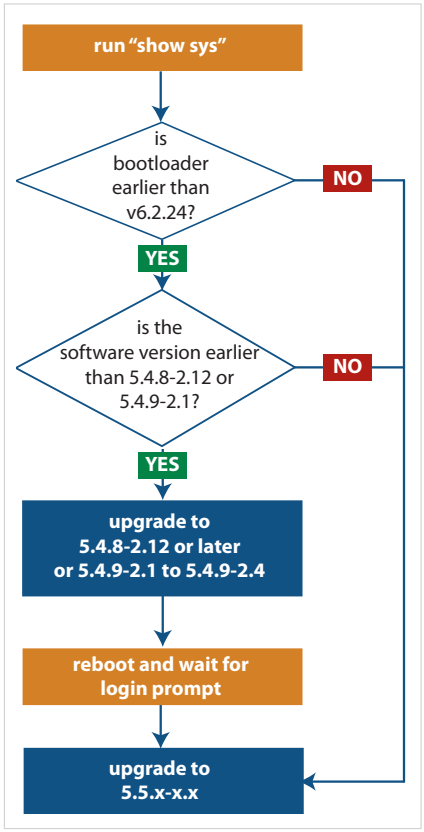
Instead, before upgrading from one of those versions to the current version, make sure your switch is running one of these specified versions:

- 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
```



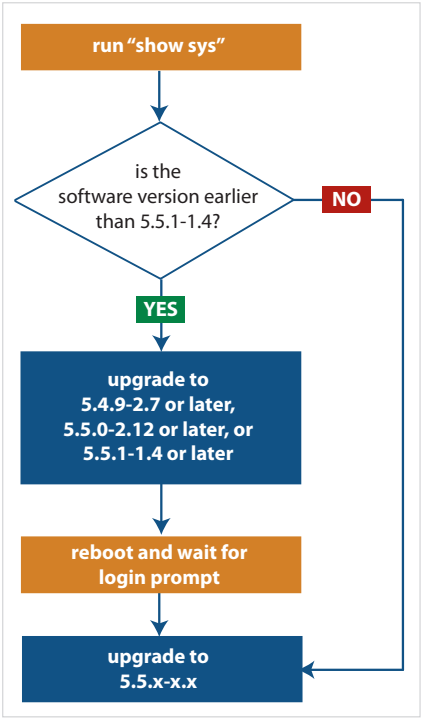
Details for x930 Series

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
```

Software release licensing

Applies to SBx908 GEN2 and SBx8100 Series switches

Please ensure you have a 5.5.6 license on your switch if you are upgrading to 5.5.6-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 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

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 version.

AMF Plus security has been increased in 5.5.5-2.1. This change means that once **any** node in an AMF network is upgraded to 5.5.5-2.1 or later, **all** nodes should run one of the following AlliedWare Plus maintenance versions (or later):

- 5.5.1-2.17 (available from the Allied Telesis Support Portal)
- 5.5.3-0.7 (available on request)
- 5.5.3-2.8 (available on request)
- 5.5.4-0.6 (available on request)
- 5.5.4-1.9 (available on request)
- 5.5.4-2.5 (available from the Allied Telesis Support Portal)
- 5.5.5-0.2 (available from the Allied Telesis Support Portal)
- 5.5.5-1.2 (available from the Allied Telesis Support Portal)
- 5.5.5-2.1 (available from the Allied Telesis Support Portal)
- 5.5.6-0.1 (available from the Allied Telesis Support Portal)

Effect if products are not upgraded

Devices running older versions can still join the AMF Plus network. However, the following functionality will not be supported:

- Remote login: Using the command **atmf remote-login <node>** to or from a node with the older security.
- Using the following commands in a single-node working-set (the command **atmf working-set <node>**) to or from a node with the older security:
  - atmf recover
  - atmf cleanup
  - banner login
  - boot system
  - boot config
  - copy
  - delete
  - edit
  - erase factory-default
  - issu boot
  - mail
  - move
  - mtrace
  - ping

- remote-login (VCS)
- terminal monitor
- test cable-diagnostics tdr interface
- traceroute

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 - both called "bulk upgrades" in this section:

- 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 your AMF master to upgrade to 5.5.6-0.x if **your AMF master** is running any of the following versions:

- 5.5.1-2.17 and later
- 5.5.4-2.5 and later
- 5.5.5-0.2 and later
- 5.5.5-1.2 and later
- 5.5.5-2.1 and later
- 5.5.6-0.1 and later

Security key incompatibilities mean that you can't upgrade to 5.5.6-0.x if your AMF master is running **any** release earlier than these. For example, you can't upgrade directly if the master is running any 5.5.2 or 5.5.3 release, or if it is running 5.5.4-0.x, 5.5.4-1.x or 5.5.4-2.4.

If your master is running an earlier release, see the 5.5.5-2.x release notes for detailed instructions on how to upgrade.

Procedure for using reboot-rolling or distribute-firmware

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

In summary, the procedure 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 selecting Configuration Guides in the left-hand menu and searching for the feature name.
- **Datasheets** - find these by selecting Datasheets in the lefthand menu and searching for the product series name.
- **Installation Guides** - find these by selecting Installation Guides in the lefthand menu and searching for the product series name.
- **Command References** - find these by selecting Reference Guides in the lefthand menu and searching for the product series name.

Verifying the Release File

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 5.5.6-0.3 below or in the release file'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. For more information, see Getting Started with the AlliedWare Plus Command Line Interface.

Table 1: Hash values for 5.5.6-0.3

Product Family	Software File	Hash
AR1050V	AR1050V-5.5.6-0.3.rel	b8444e94b8533a4aadbb5f0ab936da08d8c60674232a34bcf01747acf9050812
AR3050S	AR3050S-5.5.6-0.3.rel	8df3ecde6ec31f110a0df3a1e0ff96740691dde9e873e1b095cd2cc860919510
AR4000S-Cloud	AR4000S-Cloud-5.5.6-0.3.rel	ae866885f2bf8f8dc463540244bf467bea8b49bf8677f7bb22fdc3160dc46e24
AR4050S and AR4050S-5G	AR4050S-5.5.6-0.3.rel	8df3ecde6ec31f110a0df3a1e0ff96740691dde9e873e1b095cd2cc860919510

Product Family	Software File	Hash
ARX200S	ARX200S-5.5.6-0.3.rel	65994df239e443236ba9711e2ad85f8aeab4c6e293d5f46f7407f809666b3ce3
GS970EMX	GS970EMX-5.5.6-0.3.rel	10723e8af1e8397747cb835e13bdc04810af4c1ecfe1d71e21d985d48531f363
GS980EM	GS980EM-5.5.6-0.3.rel	a9f5a3ce333c53828781743b3d70d70fa1ac002d38976bcac933dc13417431f2
GS980M	GS980M-5.5.6-0.3.rel	a62d2033ef4eeac8f7e7048a19ff8c680bcbc78aed74f7879c3f3d870411f6a7
GS980MX	GS980MX-5.5.6-0.3.rel	a9f5a3ce333c53828781743b3d70d70fa1ac002d38976bcac933dc13417431f2
IE210	IE210-5.5.6-0.3.rel	84105724a0b148064b570f16ec65eba362f9c526307681ba4b3b826a489fca71
IE220	IE220-5.5.6-0.3.rel	c68ee71152a8b26ee77376f97a9fc7a3ec5efe7ea7ca3dec385daacb4bc7f19b
IE340	IE340-5.5.6-0.3.rel	c2c8bad03bf43e0b0e5695b88fbb7bbec356e7f860f3a36d7c609c2ee6e38c3f
IE360	IE360-5.5.6-0.3.rel	0f788f3e4902f93a30042568792d9b24019699c6dfb31d12dd9792909e707312
IE560	IE560-5.5.6-0.3.rel	fdd7d9cfd35fc13db35508641f52d63083c3bff09548f2b42c2266fa4fb48dd9
SBx81CFC960	SBx81CFC960-5.5.6-0.3.rel	f875d26bdeba18d3070b27d5f4d78bd2e7c7181ecc3aa7e86dc2c697fc4584a4
SBx908 GEN2	SBx908NG-5.5.6-0.3.rel	54cfe97cb889e2ae0ed093beca72540a70507662017fbc764eb05e25c2c2df4c
SBx908 GEN3	SBx90xGEN3-5.5.6-0.3.rel	69d01e3bbf0b7303d456623cd50b63621a11340d371a55244427d1ce238aa85e
SE240	SE240-5.5.6-0.3.rel	1b858a33ae442340492e807bf601bea614d0359954994d7931c118b7b1f3a9ce
SE250	SE250-5.5.6-0.3.rel	a54653babc34aafb067814a7b3b1527e1164436694ec80aa285327b4afbf2fcd
SE540L	SE540-5.5.6-0.3.rel	6a11f506c9b1e80c5f3e1529d74d7dd0735e118167f91c8beee3fad58ac264ea
TQ3403-R	TQ3403R-5.5.6-0.3.rel	e78e07abf7850b716feb65bbc1404b2d9c0a4cfccdb52a9880879a5c8c2ba710
TQ6702e GEN2-R	TQ6702eGEN2R-5.5.6-0.3.rel	b19632d74c3204b13b7df52dc54d87db74c4aa4dcd34abeda87105bcb710ddeb
TQ6702 GEN2-R	TQ6702GEN2R-5.5.6-0.3.rel	b4dfd2249dfaccbcdb0f02faefed74689093fc695cf4bdf76e4debacb61bb383
TQ7403-R	TQ7403R-5.5.6-0.3.rel	afd45dd1fb49ac4b0a7b4b39030cd476b7427637415f831fe031e5e5876ebbca
TQ7613-R	TQ7613R-5.5.6-0.3.rel	a5fd05859d9d9047581d217e8f320b69330acf1897e3a2e28fdd955b2e909d74
AMF Plus Cloud	vaa-5.5.6-0.3.rel	16267e995da8a1e0b89243d9f8483d18a8971a29764b5209cc5d1065cc6e03b4

Product Family	Software File	Hash
x220	x220-5.5.6-0.3.rel	a62d2033ef4eeac8f7e7048a19ff8c680bcbc78aed74f7879c3f3d870411f6a7
x240	x240-5.5.6-0.3.rel	1b858a33ae442340492e807bf601bea614d0359954994d7931c118b7b1f3a9ce
x250	x250-5.5.6-0.3.rel	a54653babc34aafb067814a7b3b1527e1164436694ec80aa285327b4afbf2fcd
x320	x320-5.5.6-0.3.rel	a9f5a3ce333c53828781743b3d70d70fa1ac002d38976bcac933dc13417431f2
x330	x330-5.5.6-0.3.rel	10723e8af1e8397747cb835e13bdc04810af4c1ecfe1d71e21d985d48531f363
x530 and x530L	x530-5.5.6-0.3.rel	a9f5a3ce333c53828781743b3d70d70fa1ac002d38976bcac933dc13417431f2
x540L	x540-5.5.6-0.3.rel	6a11f506c9b1e80c5f3e1529d74d7dd0735e118167f91c8beee3fad58ac264ea
x550	x550-5.5.6-0.3.rel	144ac3a970f0fc6e7a3395e8128f86899639b90d75ef5da8e42c282e8e1ed21e
x560	x560-5.5.6-0.3.rel	6a11f506c9b1e80c5f3e1529d74d7dd0735e118167f91c8beee3fad58ac264ea
x930	x930-5.5.6-0.3.rel	f3e3d628e85120108b9bc0b1ebc57cb87a7e07e7066506e743ccf2090e50f20b
x950	x950-5.5.6-0.3.rel	54cfe97cb889e2ae0ed093beca72540a70507662017fbc764eb05e25c2c2df4c
XS900MX	XS900-5.5.6-0.3.rel	7cd2005cd47f5daa3db609e9652d75e6fdde9ec85f20350b6b18288e70fdea83

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-2026
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                   : 5.5.6
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 05-May-2028
License expiry date            : N/A
Release                        : 5.5.6
```

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-2026
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.5.6
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 05-May-2028
License expiry date            : N/A
Release                        : 5.5.6
```

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 72 and
- "Licensing this Version on an SBx8100 Series CFC960 Control Card" on page 74.

To update the firmware:

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

2. If necessary, delete or move files to create space in 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 or your USB drive onto the device.

   To copy the release file from a TFTP server to flash memory, enter Privileged Exec mode and enter the command:

   ```
   awplus# copy tftp flash
   ```

   To copy the release file from a USB device, when your current directory is the top-level flash directory, enter the command:

   ```
   awplus# copy usb:<source-filename> flash
   ```

   On SBx8100 Series switches, you only need to copy the new release to the Active SBx81CFC960 Control Fabric Card (CFC). If your SBx8100 system has a standby CFC installed, the new release file, the configuration file, and all licenses are automatically synchronized from the Active CFC.

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 SBx8100-5.5.6-0.3.rel
SBx908 GEN3	awplus(config)# boot system SBx90xGEN3-5.5.6-0.3.rel
SBx908 GEN2	awplus(config)# boot system SBx908NG-5.5.6-0.3.rel
x950 series	awplus(config)# boot system x950-5.5.6-0.3.rel
x930 series	awplus(config)# boot system x930-5.5.6-0.3.rel
x560-28YSQ	awplus(config)# boot system x560-5.5.6-0.3.rel
x550 series	awplus(config)# boot system x550-5.5.6-0.3.rel

Product	Command
x540L series	awplus(config)# boot system x540-5.5.6-0.3.rel
x530 series	awplus(config)# boot system x530-5.5.6-0.3.rel
x330 series	awplus(config)# boot system x330-5.5.6-0.3.rel
x320 series	awplus(config)# boot system x320-5.5.6-0.3.rel
x250 series	awplus(config)# boot system x250-5.5.6-0.3.rel
x240 series	awplus(config)# boot system x240-5.5.6-0.3.rel
x220 series	awplus(config)# boot system x220-5.5.6-0.3.rel
IE560 series	awplus(config)# boot system IE560-5.5.6-0.3.rel
IE360 series	awplus(config)# boot system IE360-5.5.6-0.3.rel
IE340 series	awplus(config)# boot system IE340-5.5.6-0.3.rel
IE220 series	awplus(config)# boot system IE220-5.5.6-0.3.rel
IE210L series	awplus(config)# boot system IE210-5.5.6-0.3.rel
SE540L series	awplus(config)# boot system SE540-5.5.6-0.3.rel
SE250 series	awplus(config)# boot system SE250-5.5.6-0.3.rel
SE240 series	awplus(config)# boot system SE240-5.5.6-0.3.rel
XS900MX series	awplus(config)# boot system XS900-5.5.6-0.3.rel
GS980M series	awplus(config)# boot system GS980M-5.5.6-0.3.rel
GS980EM series	awplus(config)# boot system GS980EM-5.5.6-0.3.rel
GS980MX series	awplus(config)# boot system GS980MX-5.5.6-0.3.rel
GS970EMX series	awplus(config)# boot system GS970EMX-5.5.6-0.3.rel
AR4050S-5G	awplus(config)# boot system AR4050S-5.5.6-0.3.rel
AR4050S	awplus(config)# boot system AR4050S-5.5.6-0.3.rel
AR3050S	awplus(config)# boot system AR3050S-5.5.6-0.3.rel
AR1050V	awplus(config)# boot system AR1050V-5.5.6-0.3.rel
ARX200S series	awplus(config)# boot system ARX200S-5.5.6-0.3.rel

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

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

6. Reboot using the new software version.

```
awplus# reload
```

Accessing and Updating the Web-based GUI

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

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

On 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 the Wireless Controller (was 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 firewalls, routers and access points: 192.168.1.1

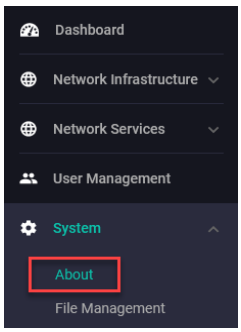
2. Open a web browser and browse to the IP address from step 1.

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 5.5.6-0.x is **2.23.0**.

If you have an earlier version, update it as described in "Update the GUI on switches" on page 79 or "Update the GUI on routers and firewalls" on page 80.



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 v5.5.6-0.x is awplus-gui_555_42.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. 556) matches the version of AlliedWare Plus running on the switch.

2. Log into the GUI:

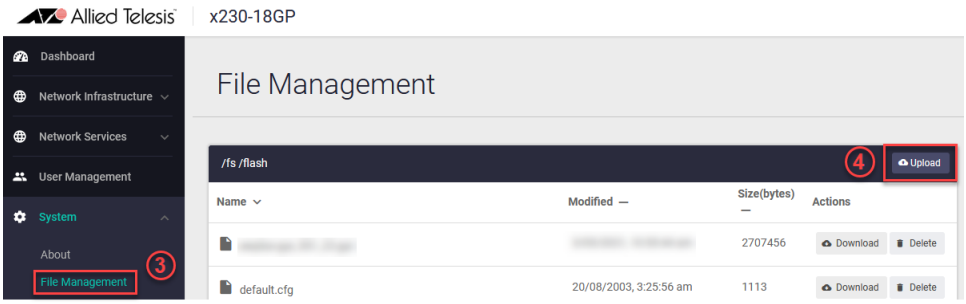
   Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

   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 routers and firewalls

Prerequisite: On AR and ARX 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 v2.23.0 or later.