Allied Telesis™

Release Note for AlliedWare Plus Software Version 5.4.7-2.x

AlliedWare Plus
OPERATING SYSTEM

» SBx8100 Series » SBx908 GEN2 » SBx908 » DC2552XS/L3
» x930 Series » x550 Series » x510 Series » IX5 Series
» x310 Series » x230 Series
» IE500 Series » IE300 Series » IE200 Series
» XS900MX Series » GS970MX Series » GS900MX/MPX Series
» FS980M Series » AMF Cloud
» AR4050S » AR3050S » AR2050V » AR2010V

» 5.4.7-2.1 » 5.4.7-2.2 » 5.4.7-2.3 » 5.4.7-2.4

Acknowledgments

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

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

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by registered mail including a check for US$15 to cover production and shipping costs and a CD with the GPL code will be mailed to you.

GPL Code Request
Allied Telesis Labs (Ltd)
PO Box 8011
Christchurch
New Zealand

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

Getting the most from this Release Note

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

Content

What’s New in Version 5.4.7-2.4

For:
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x550 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the issues resolved in AlliedWare Plus software version 5.4.7-2.4. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.Contact your authorized Allied Telesis support center to obtain a license.

Caution: Software version 5.4.7-x.x requires a release license for the SBx908 and SBx8100 switches (but not for the SBx908 GEN2). If you are using either of these switches, make sure that each switch has a 5.4.7 license certificate before you upgrade.

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

- “Licensing this Software Version on an SBx908 or SBx908 GEN2 Switch” on page 44 and
- “Licensing this Software Version on an SBx8100 Series Switch Control Card” on page 46.

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	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	12/2017	GS900-5.4.7-2.4.rel	GS900-gui_547_02.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	12/2017	FS980-5.4.7-2.4.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M	12/2017	GS970-5.4.7-2.4.rel	GS970-gui_547_03.jar
XS916MXT XS916MXS	XS900MX	12/2017	XS900-5.4.7-2.4.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	12/2017	IE200-5.4.7-2.4.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	12/2017	IE300-5.4.7-2.4.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	12/2017	IE510-5.4.7-2.4.rel	IE510-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	12/2017	x230-5.4.7-2.4.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	12/2017	x310-5.4.7-2.4.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	12/2017	IX5-5.4.7-2.4.rel	IX5-gui_547_01.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	12/2017	x510-5.4.7-2.4.rel	x510-gui_547_01.jar

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ	x550	12/2017	x550-5.4.7-2.4.rel	x550-gui_547_02.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	12/2017	x930-5.4.7-2.4.rel	x930-gui_547_01.jar
DC2552XS/L3		12/2017	dc2500-5.4.7-2.4.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	12/2017	SBx908NG-5.4.7-2.4.rel	SBx908NG-gui_547_01.jar
SBx908 (see Table)	SBx908	12/2017	SBx908-5.4.7-2.4.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	12/2017	SBx81CFC400-5.4.7-2.4.rel SBx81CFC960-5.4.7-2.4.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_03.jar
AR4050S AR3050S	AR-series UTM firewalls	12/2017	AR4050S-5.4.7-2.4.rel AR3050S-5.4.7-2.4.rel	See "Accessing the AR-Series Firewall GUI" on page 50
AR2050V AR2010V	AR-series VPN firewalls	12/2017	AR2050V-5.4.7-2.4.rel AR2010V-5.4.7-2.4.rel	See "Accessing the AR-Series Firewall GUI" on page 50
AMF Cloud			vaa-5.4.7-2.4.iso (VAA OS) vaa-5.4.7-2.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-2.4.vhd (for Microsoft Azure)	

Unsupported models

x610 and x210 Series switches are not supported by version 5.4.7-1.1 and later.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.7-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules)

Product	Supported in version 5.4.7-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

New Features and Enhancements

This section summarizes the new features in 5.4.7-2.4 since 5.4.7-1.3:

AWC on Routers

On AR-Series devices, this software update adds support for Allied Telesis Autonomous Wave Control (AWC) to control your wireless network. AWC is an advanced network technology that utilizes game theory to deliver significant improvements in wireless network connectivity and performance.

AWC can automatically minimize coverage gaps and reduce Access Point (AP) interference and respond to network configuration changes and bandwidth demands from user devices. You can configure AWC through the command line with 5.4.7-2.4, or through the Firewall GUI from January 2018. See the following page for a list of the AWC commands.

MAC auth

By default MAC authentication supplicants are added to the FDB dynamically.

AlliedWare Plus 5.4.7-2.4 adds a new command, **auth-mac static**, which configures MAC authentication to use static entries in the FDB. Static entries persist in the FDB, even if there is no traffic flow from the supplicant. To revert to default behavior using dynamic entries, use the **no auth-mac static** variant of the command.

The **auth roaming disconnected** command, which allows a supplicant to move to another authenticating interface without re-authentication, is supported for MAC authentication when static FDB entries are configured.

BGP added to IE300

From AlliedWare Plus version 5.4.7-2.4 onwards, AlliedWare Plus supports 256 BGP routes on IE300 Series switches, as part of the Premium feature license.

If you already have a Premium license, you can get it upgraded to include BGP by contacting your Allied Telesis representative. This is already available on SBx8100 Series, SBx908, SBx908 GEN2, DC2552XS/L3, x930, x510, x510L, x550 Series, AR4050S, AR3050S, AR2050V and AR2010V.

For more information about BGP configuration, see our comprehensive Routing Protocols Guide and Configuring IPv6 Routing solutions using BGP4+.

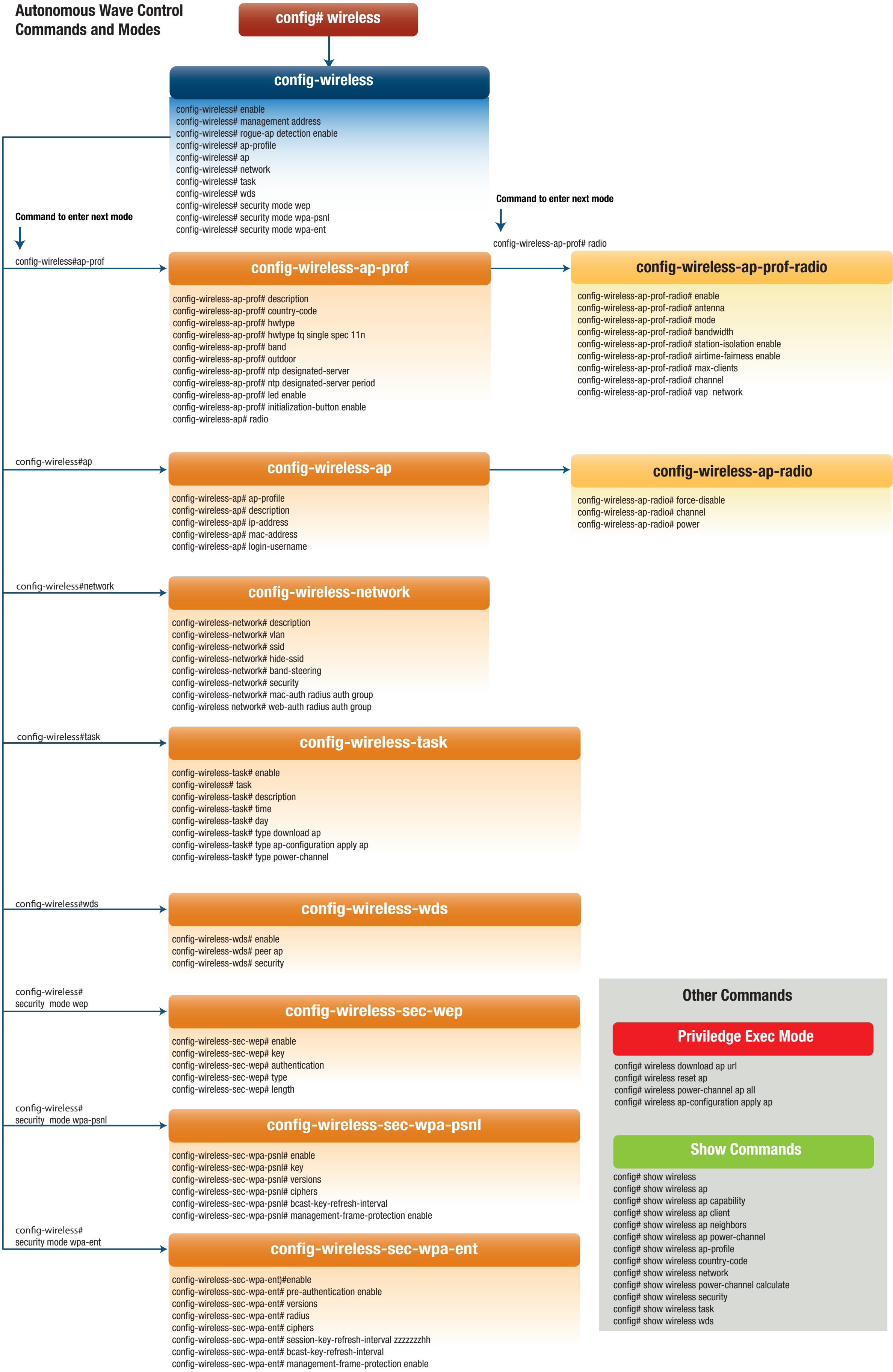
ACL Scaling

Internal handling of ACLs has been improved when they are applied with an interface range. This reduces the amount of time to apply a large number of ACLs to multiple ports at the same time, and reduces the number of used HW table filter entries.

On FS980M, SBx908, SBx81CFC400, and SBx81CFC960 systems, each VLAN ACL filter now only uses one entry per VLAN - unless any ports within a VLAN also have port ACLs or QoS policy-maps attached. On such ports, each VLAN ACL filter uses an extra entry.

Previously, each VLAN ACL filter always used one entry per port in the VLAN.

Autonomous Wave Control Commands and Modes



config# wireless

config-wireless

```
config-wireless# enable
config-wireless# management address
config-wireless# rogue-ap detection enable
config-wireless# ap-profile
config-wireless# ap
config-wireless# network
config-wireless# task
config-wireless# wds
config-wireless# security mode wep
config-wireless# security mode wpa-psnl
config-wireless# security mode wpa-ent
```

Command to enter next mode

config-wireless#ap-prof

config-wireless-ap-prof

```
config-wireless-ap-prof# description
config-wireless-ap-prof# country-code
config-wireless-ap-prof# hwtype
config-wireless-ap-prof# hwtype tq single spec 11n
config-wireless-ap-prof# band
config-wireless-ap-prof# outdoor
config-wireless-ap-prof# ntp designated-server
config-wireless-ap-prof# ntp designated-server period
config-wireless-ap-prof# led enable
config-wireless-ap-prof# initialization-button enable
config-wireless-ap# radio
```

Command to enter next mode

config-wireless-ap-prof# radio

config-wireless-ap-prof-radio

```
config-wireless-ap-prof-radio# enable
config-wireless-ap-prof-radio# antenna
config-wireless-ap-prof-radio# mode
config-wireless-ap-prof-radio# bandwidth
config-wireless-ap-prof-radio# station-isolation enable
config-wireless-ap-prof-radio# airtime-fairness enable
config-wireless-ap-prof-radio# max-clients
config-wireless-ap-prof-radio# channel
config-wireless-ap-prof-radio# vap  network
```

config-wireless#ap

config-wireless-ap

```
config-wireless-ap# ap-profile
config-wireless-ap# description
config-wireless-ap# ip-address
config-wireless-ap# mac-address
config-wireless-ap# login-username
```

config-wireless-ap-radio

```
config-wireless-ap-radio# force-disable
config-wireless-ap-radio# channel
config-wireless-ap-radio# power
```

config-wireless#network

config-wireless-network

```
config-wireless-network# description
config-wireless-network# vlan
config-wireless-network# ssid
config-wireless-network# hide-ssid
config-wireless-network# band-steering
config-wireless-network# security
config-wireless-network# mac-auth radius auth group
config-wireless network# web-auth radius auth group
```

config-wireless#task

config-wireless-task

```
config-wireless-task# enable
config-wireless# task
config-wireless-task# description
config-wireless-task# time
config-wireless-task# day
config-wireless-task# type download ap
config-wireless-task# type ap-configuration apply ap
config-wireless-task# type power-channel
```

config-wireless#wds

config-wireless-wds

```
config-wireless-wds# enable
config-wireless-wds# peer ap
config-wireless-wds# security
```

config-wireless#
security mode wep

config-wireless-sec-wep

```
config-wireless-sec-wep# enable
config-wireless-sec-wep# key
config-wireless-sec-wep# authentication
config-wireless-sec-wep# type
config-wireless-sec-wep# length
```

config-wireless#
security mode wpa-psnl

config-wireless-sec-wpa-psnl

```
config-wireless-sec-wpa-psnl# enable
config-wireless-sec-wpa-psnl# key
config-wireless-sec-wpa-psnl# versions
config-wireless-sec-wpa-psnl# ciphers
config-wireless-sec-wpa-psnl# bcast-key-refresh-interval
config-wireless-sec-wpa-psnl# management-frame-protection enable
```

config-wireless#
security mode wpa-ent

config-wireless-sec-wpa-ent

```
config-wireless-sec-wpa-ent)#enable
config-wireless-sec-wpa-ent# pre-authentication enable
config-wireless-sec-wpa-ent# versions
config-wireless-sec-wpa-ent# radius
config-wireless-sec-wpa-ent# ciphers
config-wireless-sec-wpa-ent# session-key-refresh-interval zzzzzzzhh
config-wireless-sec-wpa-ent# bcast-key-refresh-interval
config-wireless-sec-wpa-ent# management-frame-protection enable
```

Other Commands

Priviledge Exec Mode

```
config# wireless download ap url
config# wireless reset ap
config# wireless power-channel ap all
config# wireless ap-configuration apply ap
```

Show Commands

```
config# show wireless
config# show wireless ap
config# show wireless ap capability
config# show wireless ap client
config# show wireless ap neighbors
config# show wireless ap power-channel
config# show wireless ap-profile
config# show wireless country-code
config# show wireless network
config# show wireless power-channel calculate
config# show wireless security
config# show wireless task
config# show wireless wds
```

Issues Resolved in Version 5.4.7-2.4

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58190	**AMF**	Previously, a recovering AMF node with several AMF links could sometimes fail to recover over an aggregated link. This issue has been resolved. ISSU: Effective when CFCs upgraded ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-58781	**AMF**	Previously, an IE200 variant switch could fail to join an AMF network operating in secure mode. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-58784	**AMF** **API**	Previously, under very rare circumstances, the AMF process could cause a fatal error that resulted in the device restarting unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-58717	**AMF** **VCStack**	Previously, it was possible for the AMF process to restart unexpectedly during a stack member device reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	–	–	–	Y	–	–	Y	Y	–	–	–	Y	Y	Y	Y	–	–	–	–
CR-58756	**ARP** **Neighbor Discovery**	Previously, Microsoft NLB heartbeat packets could potentially reflect back out the ingress port of the switch and the same packets could potentially fail to egress out ports on other stack members. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-58728	**ARP** **Neighbor Discovery, VRF-lite**	Previously, multicast static ARPs on a VRF interface could be lost when a new stack member joined the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58562	**ARP** **Neighbor Discovery** **VRF-lite**	Previously, when using the flooding nexthop functionality (for example to facilitate Microsoft NLB) on a device, packets were not being inter-VRF routed correctly between VRF interfaces. This issue did not occur for intra-VRF routed packets. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	Y	–	–	–	–	–
CR-58437	**CLI**	Previously, changing console window size while **tech-support** was running in the background could induce a system reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-58729	**Health Check**	Previously, an x510 or x310 variant switch could sometimes fail to generate a core dump file if an operating system process failed. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-58664	**IGMP**	Previously, an interface running an IGMP proxy service could intermittently fail to send membership joins in response to a specific query sent by the querier, even though one or more mroute-proxy interfaces were members of the group specified within the query. 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	–
ER-1701	**IPv4, IPv6**	Enhancement For the x930 series switches. With this software update, the error message "HSL: ERROR: Error Adding ip multicast entry -6 Table full' is no longer being erroneously logged, despite the table not being full.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-58216	**Logging**	Previously, under rare circumstances, during a SBx8100 LIF reboot, an erroneous error message could be logged for an expected behaviour event. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58854	**Logging**	With this software update, the **`log facility local0`** command has now been fully functionally restored. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-58848	**Port Configuration**	Previously, the MRU could not be configured on provisioned interfaces. This issue has been resolved.	Y	Y	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57950	**RADIUS**	With this software update, RADIUS is upgraded to address the following vulnerabilities: CVE-2017-10978 An FR-GV-201 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows " "Read / write overflow in make_secret()" " and a denial of service. CVE-2017-10980 An FR-GV-203 issue in FreeRADIUS 2.x before 2.2.10 allows " "DHCP - Memory leak in decode_tlv()" " and a denial of service. CVE-2017-10981 An FR-GV-204 issue in FreeRADIUS 2.x before 2.2.10 allows " "DHCP - Memory leak in fr_dhcp_decode()" " and a denial of service. CVE-2017-10982 An FR-GV-205 issue in FreeRADIUS 2.x before 2.2.10 allows " "DHCP - Buffer over-read in fr_dhcp_decode_options()" " and a denial of service. CVE-2017-10983 An FR-GV-206 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows " "DHCP - Read overflow when decoding option 63" " and a denial of service. " ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58064	**System**	Previously, a on rare occasions the device may have failed to boot up correctly if there was an I2C bus lockup. This issue has been resolved. SSU: Effective when CFCs upgraded	–	–	Y	–	–	–	–	Y	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-58805	**CLI, System**	Previously, under rare circumstances, a core dump could be generated when logging out of a device which still had an active Telnet session. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-57968	**Unicast Routing**	Previously, the error message "Gateway of last resort is not set" would be displayed even though a last resort gateway was available. 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	–
CR-58520	**VLAN**	Previously, a x230 variant switch could restart silently due to low memory. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-58730	**xSTP**	Previously, when a private VLAN was associated with an MST instance, the **`no spanning-tree mst instance <1-15>`** command would be incorrectly configured for the port belonging to the secondary VLAN. 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	–

What’s New in Version 5.4.7-2.3

For:
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x550 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the issues resolved in AlliedWare Plus software version 5.4.7-2.3. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.Contact your authorized Allied Telesis support center to obtain a license.

Caution: Software version 5.4.7-x.x requires a release license for the SBx908 and SBx8100 switches (but not for the SBx908 GEN2). If you are using either of these switches, make sure that each switch has a 5.4.7 license certificate before you upgrade.

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

- “Licensing this Software Version on an SBx908 or SBx908 GEN2 Switch” on page 44 and
- “Licensing this Software Version on an SBx8100 Series Switch Control Card” on page 46.

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	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	12/2017	GS900-5.4.7-2.3.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	12/2017	FS980-5.4.7-2.3.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M	12/2017	GS970-5.4.7-2.3.rel	GS970-gui_547_03.jar
XS916MXT XS916MXS	XS900MX	12/2017	XS900-5.4.7-2.3.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	12/2017	IE200-5.4.7-2.3.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	12/2017	IE300-5.4.7-2.3.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	12/2017	IE510-5.4.7-2.3.rel	IE510-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	12/2017	x230-5.4.7-2.3.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	12/2017	x310-5.4.7-2.3.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	12/2017	IX5-5.4.7-2.3.rel	IX5-gui_547_01.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	12/2017	x510-5.4.7-2.3.rel	x510-gui_547_01.jar

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ	x550	12/2017	x550-5.4.7-2.3.rel	x550-gui_547_02.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	12/2017	x930-5.4.7-2.3.rel	x930-gui_547_01.jar
DC2552XS/L3		12/2017	dc2500-5.4.7-2.3.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	12/2017	SBx908NG-5.4.7-2.3.rel	SBx908NG-gui_547_01.jar
SBx908 (see Table)	SBx908	12/2017	SBx908-5.4.7-2.3.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	12/2017	SBx81CFC400-5.4.7-2.3.rel SBx81CFC960-5.4.7-2.3.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_03.jar
AR4050S AR3050S	AR-series UTM firewalls	12/2017	AR4050S-5.4.7-2.3.rel AR3050S-5.4.7-2.3.rel	See "Accessing the AR-Series Firewall GUI" on page 50
AR2050V AR2010V	AR-series VPN firewalls	12/2017	AR2050V-5.4.7-2.3.rel AR2010V-5.4.7-2.3.rel	See "Accessing the AR-Series Firewall GUI" on page 50
AMF Cloud			vaa-5.4.7-2.3.iso (VAA OS) vaa-5.4.7-2.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-2.3.vhd (for Microsoft Azure)	

Unsupported models

x610 and x210 Series switches are not supported by version 5.4.7-1.1 and later.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.7-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules)

Product	Supported in version 5.4.7-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

Issues Resolved in Version 5.4.7-2.3

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58784	**AMF**	Previously, under very rare circumstances, the AMF process could restart after logging out from a device. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-58805	**System**	Previously, under very rare circumstances, logging out from a device could cause a system reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

What’s New in Version 5.4.7-2.2

For:
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x550 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the issues resolved in AlliedWare Plus software version 5.4.7-2.2. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.Contact your authorized Allied Telesis support center to obtain a license.

Caution: Software version 5.4.7-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.7 license certificate before you upgrade.

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

- “Licensing this Software Version on an SBx908 or SBx908 GEN2 Switch” on page 44 and
- “Licensing this Software Version on an SBx8100 Series Switch Control Card” on page 46.

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	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	11/2017	GS900-5.4.7-2.2.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	11/2017	FS980-5.4.7-2.2.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M *available Sept 2017	11/2017	GS970-5.4.7-2.2.rel	GS970-gui_547_03.jar
XS916MXT XS916MXS	XS900MX	11/2017	XS900-5.4.7-2.2.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2017	IE200-5.4.7-2.2.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	11/2017	IE300-5.4.7-2.2.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	11/2017	IE510-5.4.7-2.2.rel	IE510-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	11/2017	x230-5.4.7-2.2.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2017	x310-5.4.7-2.2.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	11/2017	IX5-5.4.7-2.2.rel	IX5-gui_547_01.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	11/2017	x510-5.4.7-2.2.rel	x510-gui_547_01.jar

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ	x550	11/2017	x550-5.4.7-2.2.rel	x550-gui_547_02.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2017	x930-5.4.7-2.2.rel	x930-gui_547_01.jar
DC2552XS/L3		11/2017	dc2500-5.4.7-2.2.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	11/2017	SBx908NG-5.4.7-2.2.rel	SBx908NG-gui_547_01.jar
SBx908 (see Table)	SBx908	11/2017	SBx908-5.4.7-2.2.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	11/2017	SBx81CFC400-5.4.7-2.2.rel SBx81CFC960-5.4.7-2.2.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_03.jar
AR4050S AR3050S	AR-series UTM firewalls	11/2017	AR4050S-5.4.7-2.2.rel AR3050S-5.4.7-2.2.rel	See “Accessing the AR-Series Firewall GUI” on page 50
AR2050V AR2010V	AR-series VPN firewalls	11/2017	AR2050V-5.4.7-2.2.rel AR2010V-5.4.7-2.2.rel	See “Accessing the AR-Series Firewall GUI” on page 50
AMF Cloud		11/2017	vaa-5.4.7-2.2.iso (VAA OS) vaa-5.4.7-2.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-2.2.vhd (for Microsoft Azure)	

Unsupported models

x610 and x210 Series switches are not supported by version 5.4.7-1.1 and later.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.7-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules)

Product	Supported in version 5.4.7-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

Issues Resolved in Version 5.4.7-2.2

This AlliedWare Plus maintenance version includes the resolved issues in the following table, ordered by feature.

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58707	**AMF Cloud**	Previously, the interface history monitoring API on VAA was not working correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-58634	**ARP Neighbor Discovery** **Port Authentication**	Previously, when a switch was configured with web authentication, ARP entries were not added correctly in the hardware table, resulting in low switch performance. This was due to traffic being unnecessarily forwarded via software instead of being hardware switched. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	Y	–	–	–	–
CR-58728	**ARP** **Neighbor Discovery, VRF-lite**	Previously, multicast static ARPs on a VRF interface could be lost when a new stack member joined the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	Y	–	–	–	–
CR-58714	**DHCP Server**	Previously, on rare occasions, a DHCP server restart could cause the device to undergo a system reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-58328	**Hot Swap**	Previously, hotswapping a XEM from a SBx908 Generation 2 modular switch could result in erroneous system error log messages. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-58697	**Pluggable Transceivers**	Previously, on a SBx908 Generation 2 modular switch, pluggable diagnostics for QSFP channel sensors were displayed incorrectly. This would also prevent active-fiber-monitoring from working correctly for QSFPS. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58665	**Pluggable Transceivers**	Previously, a 10G fiber SFP or DAC pluggable would not link up correctly after it was inserted into a port that previously had a 1G fiber SFP inserted. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–

What’s New in Version 5.4.7-2.1

For:
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x550 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.7-2.1. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.Contact your authorized Allied Telesis support center to obtain a license.

Caution: Software version 5.4.7-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.7 license certificate before you upgrade.

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

- “Licensing this Software Version on an SBx908 or SBx908 GEN2 Switch” on page 44 and
- “Licensing this Software Version on an SBx8100 Series Switch Control Card” on page 46.

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	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	11/2017	GS900-5.4.7-2.1.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	11/2017	FS980-5.4.7-2.1.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M *available Sept 2017	11/2017	GS970-5.4.7-2.1.rel	GS970-gui_547_03.jar
XS916MXT XS916MXS	XS900MX	11/2017	XS900-5.4.7-2.1.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2017	IE200-5.4.7-2.1.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	11/2017	IE300-5.4.7-2.1.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	11/2017	IE510-5.4.7-2.1.rel	IE510-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	11/2017	x230-5.4.7-2.1.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2017	x310-5.4.7-2.1.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	11/2017	IX5-5.4.7-2.1.rel	IX5-gui_547_01.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	11/2017	x510-5.4.7-2.1.rel	x510-gui_547_01.jar

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ	x550	11/2017	x550-5.4.7-2.1.rel	x550-gui_547_02.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2017	x930-5.4.7-2.1.rel	x930-gui_547_01.jar
DC2552XS/L3		11/2017	dc2500-5.4.7-2.1.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	11/2017	SBx908NG-5.4.7-2.1.rel	SBx908NG-gui_547_01.jar
SBx908 (see Table)	SBx908	11/2017	SBx908-5.4.7-2.1.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	11/2017	SBx81CFC400-5.4.7-2.1.rel SBx81CFC960-5.4.7-2.1.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_03.jar
AR4050S AR3050S	AR-series UTM firewalls	11/2017	AR4050S-5.4.7-2.1.rel AR3050S-5.4.7-2.1.rel	See “Accessing the AR-Series Firewall GUI” on page 50
AR2050V AR2010V	AR-series VPN firewalls	11/2017	AR2050V-5.4.7-2.1.rel AR2010V-5.4.7-2.1.rel	See “Accessing the AR-Series Firewall GUI” on page 50
AMF Cloud		11/2017	vaa-5.4.7-2.1.iso (VAA OS) vaa-5.4.7-2.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-2.1.vhd (for Microsoft Azure)	

Unsupported models

x610 and x210 Series switches are not supported by version 5.4.7-1.1 and later.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.7-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules)

Product	Supported in version 5.4.7-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

New Products

AlliedWare Plus version 5.4.7-2.1 supports the following recently-released product.

SwitchBlade x908 Generation 2

High Capacity Stackable Layer 3+ Modular Switch

The Allied Telesis SBx908 GEN2 is the ideal solution for the modern enterprise network core. This modular switch also has the capacity to support Smart City and IoT networks.

The high-capacity 2.6 Terabit fabric eliminates bottlenecks, effortlessly streams video and ensures all traffic in large networks is delivered reliably. Flexible hot-swappable expansion modules (XEMs) support 10 Gigabit, 40 Gigabit—and 100 Gigabit in the future—to easily expand the SBx908 GEN2 to meet network traffic demands, both now and well into the future.

For more information, see alliedtelesis.com/products/switches/x908-gen2.

New Features and Enhancements

This section summarizes the new features in 5.4.7-2.1 since 5.4.7-1.1:

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 42.

Allied Telesis Autonomous Management Framework (AMF) enhancements

VPN support on the Virtual AMF Appliance for AMF Cloud

From AlliedWare Plus version 5.4.7-2.1 onwards, AMF Cloud includes VPN support, to allow secure encrypted connectivity between a cloud-based AMF Controller/Master and a physical AMF network.

This is achieved by configuring the Virtual AMF Appliance (VAA) with one or more virtual tunnel interfaces (VTIs). Each VTI terminates a single IPsec protected VPN, and securely transports AMF virtual-links between the VAA and a remote AMF network. Previously, a third-party VPN terminator, such as the AWS Virtual Private Gateway, provided this functionality.

The virtual tunnel interface(s) can be configured to provide static L2TPv3 Ethernet pseudo-wires that are IPsec protected. These can be used as part of an AMF multi-tenant environment, with each VPN isolated from every other VPN. Alternatively, the virtual tunnel interface(s) can be configured using native IPsec to allow interoperability with other vendors' VPN implementations as part of an AMF single-tenant solution.

The following four tunnel types are supported on the VAA:

- L2TPv3 IPv4 (IPsec protection optional/recommended)
- L2TPv3 IPv6 (IPsec protection optional/recommended)
- IPsec IPv4
- IPsec IPv6

See the AMF Feature Overview and Configuration Guide and the Install Guide: Virtual AMF Appliance (VAA) for AMF Cloud for details.

Improved auto-recovery of GS900MX/MPX Series switches

From AlliedWare Plus version 5.4.7-2.1 onwards, you can, with some preparation, auto-recover GS900MX/MPX Series switches where a VCStack port has been used as an AMF link. This is achieved by either:

- disabling stacking on the device from the CLI, before using it in a recovery situation, or
- using a USB storage device to provide an autoboot configuration that disables stacking.

See the AMF Feature Overview and Configuration Guide for details on how to prepare your GS900MX/MPX Series switch for auto-recovery.

Improved auto-recovery of AR-series UTM firewalls and VPN routers

From AlliedWare Plus version 5.4.7-2.1 onwards, AMF can perform auto-recovery using factory fresh AR4050S, AR3050S, AR2050V and AR2010V devices. Previously, the **atmf cleanup** command had to be run on these devices before using them to auto-recover a failed device.

Auto-recovery of isolated nodes

Available on AMF Cloud and AlliedWare Plus switches that can form AMF virtual links

From AlliedWare Plus version 5.4.7-2.1 onwards, AMF can automatically recover isolated nodes.

An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link. As it has no physical connection to another AMF member, a recovering, or newly provisioned, isolated node cannot identify its location in the usual way by interrogating its AMF neighbors. Instead, it is identified using an *identity token* stored on the AMF master. This token is saved to the AMF master when the node is backed up and is created using the MAC address of the next-hop on the isolated node's virtual-link interface.

Note: When provisioning a new device, it is possible to optionally specify the new device's serial number, instead of the next-hop MAC address, as the identity token.

In order to initiate a recovery, the AMF master must be accessible to the isolated AMF node. This is achieved by using DHCP to send the URI of the AMF master to the recovering node. This URI must be both resolvable and reachable from the recovering node. See the AMF Feature Overview and Configuration Guide for information on configuring your network to support the auto-recovery of isolated nodes.

Support for 10,000 nodes

Available on all AlliedWare Plus devices

From AlliedWare Plus version 5.4.7-2.1 onwards, AMF Cloud supports up 10,000 nodes with the AMF controller and multi-tenanted masters on a Virtual AMF Appliance (VAA). This VAA may be hosted on Amazon Web Service (AWS), Microsoft Azure, or a customer's private server.

Table 1: 10000 nodes system requirements

AMF NETWORK SIZE	vCPUs	MEMORY	AWS INSTANCE TYPE	AZURE INSTANCE TYPE
Multi-tenant VAA with up to 10,000 nodes, and **less** than 2000 virtual-links	8	8GB	c4.2xlarge	F8
Multi-tenant VAA with up to 10,000 nodes, and **more** than 2000 virtual-links	16	8GB	c4.4xlarge	F16

Support for VCStack on SBx908 GEN2 switches

From software version 5.4.7-2.1 onwards, the SwitchBlade x908 GEN2 provides two-unit Virtual Chassis Stacking (VCStack).

VCStack, in conjunction with link aggregation, provides a network with no single point of failure and a resilient solution for high availability applications. The SBx908 GEN2 can form a VCStack of two units for enhanced resiliency and simplified device management. Stacks can also be created over long distance 40Gbps fiber links, making SBx908 GEN2 the perfect choice for distributed environments.

Upstream Forwarding Only (UFO) for private VLANs

Applies to IE510-28GSX-80, IE300 Series, x510L Series, x510 Series, and x930 Series switches

From AlliedWare Plus version 5.4.7-2.1 onwards, you can use Upstream Forwarding Only (UFO) to create Private VLANs.

Private VLANs are needed because some services need to control connections between the port and upstream device. For example, in applications such as Triple-Play networks, VLANs are often shared across subscribers and provide a specific service or set of services. Such VLANs are called Service VLANs.

For example, an Internet Service VLAN that is shared amongst subscribers needs to block subscribers from sending to other subscribers, while a shared Voice Service VLAN needs to let subscribers forward voice traffic directly with each other. Because these two VLANs often have the same port memberships, there is a need to allow isolated VLANs to co-exist with regular VLANs on the same ports. Enabling Private VLAN UFO on the Internet VLAN will provide isolation, while allowing the Voice VLAN to remain operating as a standard or regular VLAN.

UFO is configured on individual VLANs and blocks or isolates traffic at Layer 2. It blocks the forwarding of Ethernet frames between certain ports of a UFO VLAN while allowing forwarding of others. All data from ports associated with a UFO VLAN must be forwarded only to the upstream port, which is why it is called Upstream Forwarding Only.

UFO is configured on a per VLAN basis, and removes many of the Private VLAN trunk restrictions. This means that:

- Regular VLANs can now coexist with UFO VLANs on the same ports.
- VLANs can belong to different port groups.
- Ports do not all have to be trunk ports.

For configuration details, see the VLANs Feature Overview and Configuration Guide.

Application Awareness

Available on AR2010V, AR2050V, AR3050S, and AR4050S

From AlliedWare Plus version 5.4.7-2.1 onwards, Application Awareness has been expanded. It now supports a built-in list of applications that the device can recognize when Deep Packet Inspection (DPI) is enabled. On the AR3050S and AR4050S, the **provider** command now allows you to select this built-in list as an alternative to the subscription-based list provided by Procera. On the AR2010V and AR2050V, the built-in list of applications can be used to provide application aware firewalling, as these models do not support the subscription-based list from Procera.

To select either Procera or the built-in list, use the commands:

```
awplus(config)#dpi
awplus(config-dpi)#provider {procera|built-in}
awplus(config-dpi)#enable
```

Enhanced information can now be displayed about applications in the list that DPI recognizes. The **show application detail** command now displays the application mark, application name and a brief description. If DPI and Procera are enabled, the description includes a category, and productivity and risk indices.

In addition, policy-based routing (PBR) also supports Application Awareness using both the Procera list and the new built-in provider.

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

Discovering the Web Control category

Available on AR3050S and AR4050S UTM firewalls

From AlliedWare Plus version 5.4.7-2.1 onwards, if Web Control is enabled, a new command allows you to enquire of the web control provider about one or more URLs' web control category. A response back from the web-control provider's server contains the category or categories the URLs belong to. You can use this information to configure web control policies to more closely meet the needs of your organisation.

The new command is:

```
awplus#web-control categorize <url-list>
```

For example, to discover the web control categories for the URLs example1.com and example2.com, use the command:

```
awplus#web-control categorize example1.com example2.com
```

For more information, see the Web Control Feature Overview and Configuration Guide and the Command Reference for your device.

Increased index range for encrypted tunnels

From AlliedWare Plus version 5.4.7-2.1 onwards, the index range for tunnels has increased on AR4050S, AR3050S, AR2050V and AR2010V devices, as shown in the following command:

```
awplus(config)#interface tunnel <0-65535>
```

The maximum number of tunnels has increased to 1000 on the AR4050S. A suitable number of tunnels should still be determined according to the topology of your network. The maximum number of tunnels for other AR series devices has not changed.

Running a trigger when a log message occurs

Available on all AlliedWare Plus products

From AlliedWare Plus version 5.4.7-2.1 onwards, you can configure a trigger to activate a configuration script when a particular string is generated in log messages of severity level notice or higher. The log message string can be filtered by including regular expressions (PCRE). To configure this, use the command:

```
awplus(config-trigger)#type log <log-message-string>
```

For an example of configuring a trigger based on log messages, see the Logging Feature Overview and Configuration Guide.

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

Syslog and emailed log messages: Improved compliance with RFC3164

Available on all AlliedWare Plus devices

From AlliedWare Plus version 5.4.7-2.1 onwards, the format of log messages has been changed when they are sent to a host (for syslog) or an email destination. Previously there was a space after the first field in the message, before the timestamp. That space has been removed.

For full compliance with RFC3164, you need to change the message date format as well, using the command 'log date iso'. This command is now available on all AlliedWare Plus devices. An example of a compliant message is:

```
<13>2017-08-31T14:38:57+12:00 Bchs74 atmffsd: ATMF backup server ID:
2 is now available
```

Most industry tools that take syslog messages as input will now interpret such AlliedWare Plus log messages without any modification.

VRRPv3 preempt delay

Available on all AlliedWare Plus devices that support VRRPv3

From AlliedWare Plus version 5.4.7-2.1 onwards, you can configure a preempt mode delay time. If this is configured, the device will pause for the specified time before preempting the lower priority device and becoming master. The delay time allows the device to become stabilized in the network before preempting the routing role from the lower priority switch.

To configure the delay time, use the following command:

```
awplus(config-router)#preempt-mode true delay-time <seconds>
```

Enhancements to interface statistics

Available on all AlliedWare Plus devices

From AlliedWare Plus version 5.4.7-2.1 onwards, the **show interface** command also returns information about interface statistics, in addition to its other output. It will show the 30 second and 5 minute average input rates, the 30 second and 5 minute average output rates, and the peak input and output rates. These statistics are calculated for switchports on switches, and for all interfaces on routers.

This statistic collection is enabled by default, but can be disabled using the new command **no service statistics interfaces counter**.

Single-signature support for high-power PoE on IE300 Series switches

From AlliedWare Plus version 5.4.7-2.1 onwards, IE300 Series switches support single-signature mode on their high-power ports, along with the previously available dual signature mode. High-power ports can supply up to 60W of Power over Ethernet.

This enables them to support more powered devices (PDs).

If your PD requires single-signature mode, you can enable it on the port that the PD is connected to, by using the following commands. In this example, a high-power camera is connected to port1.0.9 on the IE300 Series switch:

```
awplus(config)#interface port1.0.9
awplus(config-if)#power-inline four-pair mode single-signature
```

The default mode is dual-signature mode. To return to the default, use the following commands:

```
awplus(config)#interface port1.0.9
awplus(config-if)#power-inline four-pair mode dual-signature
```

To display the four-pair mode, use the following command:

```
awplus#show power-inline interface detail
```

You can display the setting for a single command by using the following command:

```
awplus#show power-inline port1.0.9 interface detail
```

Ethernet Ring Protection Switching (G.8032) on x550 Series switches

Now available on x550 Series switches.

Already available since version 5.4.7-0.1 on x930, x510, x510L, IX5, IE500, IE300 and IE200 Series Switches

From version 5.4.7-2.1 onwards, AlliedWare Plus supports G.8032 Version 2 February 2012 edition on x550 Series switches.

G.8032 is an International Telecommunication Union (ITU) standard for Ethernet Ring Protection Switching (ERPS). It prevents loops on a per-VLAN basis with networks that are wired in a simple ring topology, and (with G.8032 Version 2) multiple ring and ladder topologies.

G.8032 offers a rapid detection and recovery time if a link or node fails, in the order of 50 ms, depending on configuration.

For more information and configuration details, see the G.8032 Ethernet Ring Protection Switching Feature Overview and Configuration Guide and the CFM Feature Overview and Configuration Guide.

Multicast VLAN Registration (MVR) Proxy Mode

Available on x510 and x510L Series switches

From version 5.4.7-2.1 onwards, AlliedWare Plus supports MVR proxy mode on x510 and x510L Series switches.

MVR enables the switch to receive one copy of a multicast stream, such as IPTV traffic, and send that copy to multiple hosts, by sending it to multiple VLANs. Without MVR, the switch receives a separate copy of the multicast stream for each VLAN with host(s) requesting it. Using MVR increases network efficiency and reduces cost.

x510 and x510L Series switches will operate in MVR proxy mode. They will receive multicast streams on an upstream VLAN and forward them to the appropriate downstream VLANs.

To configure the upstream VLAN, use the command **mvr source**. To configure the downstream VLANs, use the command **mvr receiver source-interface <source-vlan>**. You also need to enable IP multicast routing.

For example, the following commands enable the switch to receive multicast streams on VLAN10 and send them out VLANs 20, 30 and 40 if those VLANs have joined the streams:

```
awplus(config)#ip multicast-routing

awplus(config)#interface vlan10

awplus(config-if)#mvr source

awplus(config)#interface vlan20,vlan30,vlan40

awplus(config-if)#mvr receiver source-interface vlan10
```

The command **show mvr** displays summary or detailed information about MVR interfaces or multicast groups.

ACL Option to Send Packets to a Port in a VLAN

Now available on GS900MX/MPX, XS900MX, SBx908 GEN2, SBx8100, DC2552XS/L3 and x550 Series switches.

Already available since 5.4.6-2.x on x930, x610, x510, x510L, IX5, x310 and x230 Series switches.

From version 5.4.7-2.1 onwards, AlliedWare Plus adds support for a hardware ACL action named "send-to-vlan-port" to the switches listed above. This option allows you to specify a port that belongs to a specified VLAN. Matching packets will be sent to the specified port, tagged with the specified VLAN.

The send-to-vlan-port action applies to numbered and named IP, MAC and IPv6 hardware ACLs, so you can create ACLs to redirect packets on the basis of IP settings, IPv6 settings, or MAC address. For example, to create an ACL that will redirect packets from the MAC address aaaa.bbbb.00a0 to port 1.0.1 on VLAN 200, use the commands:

```
awplus#configure terminal

awplus(config)#access-list 4000 send-to-vlan-port vlan 200 port
port1.0.1 aaaa.bbbb.00a0 0000.0000.0000 any
```

You can apply the ACL directly to an ingress port, or by using QoS class maps.

Support for IPv6 hardware ACLs on x230 Series switches

Now available on x230 Series switches.

Already available on SBx908 GEN2. SBx908, DC2552XS/L3, SBx8100, x930, x550, x510, x510L, IX5, x310, XS900MX, IE500, IE300, and IE200 Series switches

From AlliedWare Plus version 5.4.7-2.1 onwards, AlliedWare Plus supports IPv6 Hardware ACLs on x230 Series switches. Hardware ACLs are ACLs that you can apply directly to an interface, or use for QoS classifications.

For more information and configuration details, see the ACL Feature Overview and Configuration Guide.

Support for 256 BGP routes on x510, x510L and x550 Series switches

Now available on x510, x510L and x550 Series switches.

Already available on SBx8100 Series, SBx908, SBx908 GEN2, DC2552XS/L3, x930 Series, AR4050S, AR3050S, AR2050V and AR2010V.

From AlliedWare Plus version 5.4.7-2.1 onwards, AlliedWare Plus supports 256 BGP routes on x510, x510L and x550 Series switches, as part of the Premium feature license.

If you already have a Premium license, you can get it upgraded to include BGP by contacting your Allied Telesis representative.

For more information about BGP configuration, see our comprehensive Routing Protocols Guide and Configuring IPv6 Routing solutions using BGP4+.

Support for the OpenFlow protocol on IE510-28GSX-80 and IE300 Series switches

Now available on IE510-28GSX-80 and IE300 Series switches.

Already available on DC2552XS/L3, x930, x550, x510, x510L, x310, and x230 Series switches

From version 5.4.7-2.1 onwards, AlliedWare Plus supports version 1.3 of the OpenFlow protocol on IE510-28GSX-80 and IE300 Series switches.

These switches enable the OpenFlow protocol on a per-port basis, so you can choose which ports of the switch will be controlled by the OpenFlow protocol.

Non-OpenFlow-enabled ports continue to support existing features of the device.

VLAN ID translation on x510 and x510L Series switches

Now available on x510 and x510L Series switches.

Already available on IE510-28GSX-80 and IE300 Series switches

From version 5.4.7-2.1 onwards, AlliedWare Plus supports VLAN ID translation on x510 and x510L Series switches. VLAN ID translation translates a VLAN's VLAN ID to another value for use on the wire.

In Metro networks, it is common for the Network Service Provider to give each customer their own unique VLAN, yet at the customer location, give all the customers the same VLAN ID for tagged packets to use on the wire. VLAN ID translation can be used by the Service Provider to change the tagged packet's VLAN ID at the customer location to the VLAN-ID for tagged packets to use within the NSP's network.

VLAN ID translation is also useful in Enterprise environments where it can be used to merge two networks together without manually reconfiguring the VLAN numbering scheme. This situation can occur if two companies have merged and the same VLAN ID is used for two different purposes.

Similarly, within a Network Service Provider's network, Layer 2 networks may need to be rearranged, and VLAN ID translations make such rearrangement more convenient.

For configuration details, see the VLANs Feature Overview and Configuration Guide.

Important Considerations Before Upgrading

This section describes changes since version 5.4.6-0.1 that may affect your network behavior if you upgrade. Please read it carefully before upgrading.

Changes to default start-up behavior

Applies to all AlliedWare Plus devices

From AlliedWare Plus versions 5.4.7-1.1 and 5.4.7-0.4 onwards, unconfigured devices automatically receive a management IP address on start-up, without any manual configuration. You can optionally set up a DHCP server on your network and have the device obtain an address via DHCP. Otherwise, switches use an IP address of 169.254.42.42/16 and AR-series firewalls use an IP address of 192.168.1.1/24[1].

This automatic address assignment means you can use SSH to manage the device, without the need for an asynchronous console cable.

The device must be unconfigured for this automatic address assignment to occur.

[1] This is the case if the AR-series firewall ships from our factory with 5.4.7-2.1 or later installed. Firewalls that ship with earlier versions cannot use DHCP to obtain an address automatically. They still have a default address of 192.168.1.1/24.

AR Series firewalls

AR-Series Firewalls that come from our factory with 5.4.7-2.1 or later installed use the new start-up behavior. They will be automatically assigned an IP address via DHCP, or will use 192.168.1.1/24.

AR-Series Firewalls that ship from our factory with 5.4.7-1.x or earlier are pre-configured at the factory. Therefore the new start-up behavior does not apply to them unless you manually return them to an unconfigured state by using the command **erase factory-default**. They have a default IP address of 192.168.1.1/24 on VLAN1 (or eth1 on an AR2010V).

What is an unconfigured device?

A device can be considered unconfigured if all of the following conditions apply:

1. The device is not set up to use autoboot functionality via external media. This means either:

   « There is no USB stick or SD card connected, or,

   « If there is a USB stick or SD card connected, it does not contain a file named autoboot.txt.

   Note that:

   « The autoboot.txt file (if present) need not contain anything – it can be an empty file. The presence alone of a file with this name on the external media is enough to stop the automatic address assignment process.

   « Similarly, the autoboot feature need not be enabled on the device in order to stop the automatic address assignment process.

2. None of the following files exist in the root directory of /flash:

   « .config

   « .config_backup

   « .cfg files

   « User created folders

Note that a device is still considered unconfigured if GUI files are present in the root directory /flash memory. However, if the device has been configured to enable the HTTP service, then the device is no longer considered unconfigured.

You can manually return a device to an unconfigured state by using the command **erase factory-default**.

What is the management interface?

The management interface depends on the interfaces available on the device. It is:

- On a switch: the eth0 interface, labeled NET MGMT, if that interface exists
- On a switch or firewall that does not have a NET MGMT interface, but does have switchports: vlan1
- On a firewall with no switchports (AR2010V): the first eth port to go link-up.

How the new start-up process works

The following sequence of events occur when an unconfigured device starts up:

1. Once the management interface comes up:
   - if the management interface is vlan1, then the device waits until the vlan1 switchport has gone into a STP forwarding state.
   - otherwise, the device moves immediately on to step 2.

2. Telnet is disabled, SSH server is enabled, and Loop Protection is enabled (on devices that support it).

3. DHCP and DHCPv6 clients are enabled on the management interface, and the DHCP and DHCPv6 client process is started.

4. An IPv6 link-local address is automatically assigned to the management interface.

5. If the device obtains an address or addresses from DHCP or DHCPv6, then it applies the address to the management interface.

6. If the device does not obtain an IPv4 address via DHCP within10 seconds, then it applies the class B IPv4 link-local address 169.254.42.42/16 (for switches) or 192.168.1.1/24 (for firewalls) to the management interface. The device also disables the IPv4 DHCP client at this point.

You can manage the device by using SSH to connect to the IPv4 or IPv6 address assigned to the management interface. You will need to ensure your management computer is configured with an IP/IPv6 address within the same subnet as the management IP address on the device. Connect using an SSH client, and login using the default username/ password (manager/friend). If you get a hostkey warning message, follow the message's instructions to accept the key.

Configured commands

The following commands are configured:

```
no service telnet
service ssh
ssh server allow-users manager
loop-protection loop-detect fast-block ldf-interval 1
interface <management-interface>
 ip address dhcp
 ipv6 address dhcp
```

Note that some devices (e.g. AR-Series Firewalls) do not support Loop Protection, so will not include the **loop-protection** configuration. If no DHCP address is assigned to the management interface, then the management interface's dynamic configuration is changed to the following commands:

```
interface <management-interface>
 ip address 192.168.1.1/24
 ipv6 address dhcp
```

Further details about the new start-up behavior

Additional notes about the start-up process:

- The process will stop if either of the following events occur during start-up:
  - configuration changes are made by logging in via a console port (see "Configuring the device by the console" on page 36 for details).
  - AMF zero-touch recovery begins. The new start-up process does not stop AMF from treating the device as a clean device and initiating zero-touch recovery.
- Other than the configuration changes specified above, the factory configuration remains unchanged, so protocols such as RSTP remain in their default state.
- On a stack, this new behavior will only be executed on the Stack Master.
- The configuration changes are not automatically saved, so rebooting the device without saving the configuration will trigger the same behavior again.
- The device broadcasts DHCP messages. If the device is attached to existing network infrastructure via multiple switchports, and the existing equipment does not support STP, then there is the potential for a broadcast storm. To ensure loop-free operation with this feature, AlliedWare Plus devices have RSTP enabled by default. Additionally, the Loop Protection feature is now automatically enabled during start-up on devices that support it.
- If using a DHCP or DHCPv6 server for address allocation, we recommend you configure the server to allocate a static IPv4 or IPv6 address binding based on the MAC address of the device. This ensures you know which management address to SSH to.

IGMP and MLD snooping

If the new start-up procedure assigns an address on VLAN1, then IGMP snooping requires you to either:

- ensure that the VLAN has either a statically configured or DHCP assigned IP address in the same subnet as your multicast sources, or
- remove the IPv4 address from VLAN1.

To remove the address, use the following commands:

```
awplus(config)# interface vlan1
awplus(config-if)# no ip address
```

Setting up a number of devices

If you want to attach multiple devices to your network at the same time, there are a couple of things you need to consider:

- You should assign the addresses by DHCP, because otherwise all the new devices will apply the same IP address to the management interface, making the feature unusable.
- Your SSH client may notify you that the host key has changed when you move from one device to the next device. The warning will include a selection option to replace the old host key, or instructions on how to do this. Follow the client's selection option or instructions.

About the 169.254.0.0/16 address range

There are a number of advantages to using the 169.254.0.0/16 range when automatically assigning an address to a switch for management purposes. This section describes these advantages.

1. It is link-local (not routeable). This prevents the switch from being exposed from outside the link before it has been configured with suitable security settings.

2. RFC-conformant host PCs in the link-local subnet deal effectively with IP address collisions, which occur if the host PC and the AlliedWare Plus switch have the same IP address. If a collision occurs, the RFC-conformant host will automatically back off and choose a different IP address in the same subnet, to avoid the collision. Note that AlliedWare Plus switches are designed to not back off, to ensure their address is always predictable.

3. Assigning an IP address from a more commonly-used subnet, such as 192.168.1.1/24, would increase the likelihood of IP address collision. Because AlliedWare Plus switches do not have an automatic back-off mechanism, manual configuration of the host PC would be required.

Preventing the New Start-up Behavior

If you do not want to have the new start-up behavior, you can prevent it by:

- Adding an autoboot file, or
- Configuring the device by the console port instead of the management interface

The following sections describe these options in detail.

Adding an autoboot file

A simple way to prevent the new start-up behavior is to insert a USB stick or SD card containing a file named autoboot.txt. Unless you wish to configure autoboot, leave the autoboot.txt file empty. The file stops the device from being treated as an unconfigured device.

Configuring the device by the console

Another way to prevent the new start-up behavior is to connect via the asynchronous-based console port only, leaving the network management interface disconnected.

If you have both asynchronous and network interfaces connected, you need to be cautious for a few seconds after start-up about entering configuration commands via the asynchronous console interface. During these few seconds, dynamically entering any configuration commands via the console can stop the new start-up behavior. This possibility occurs until the management interface comes up and (for vlan1) a switchport goes into the STP forwarding state. Once STP is in forwarding state, entering configuration via the console will not stop the new start-up behavior.

Performing network management via eth interfaces will start IP address assignment more quickly than via vlan1. This is because (unlike switchports within a VLAN) eth interfaces do not use STP, so there is no additional delay waiting for the STP state change.

Monitoring

There are no **show** commands specific to this feature. The following messages are output to the console (if connected) after the management interface goes link-up:

```
IP address assignment underway:
Password change is strongly recommended
```

A message is output when an address is assigned to the management interface, such as:

```
Interface vlan1 address set to 169.254.42.42/16
```

Changes to handling of characters in strings

Applies to all AlliedWare Plus devices

Interface descriptions

From version 5.4.7-1.1 onwards, interface descriptions can only contain printable ASCII characters (ASCII 32-126).

If you have interface descriptions that contain other characters, change them before you upgrade. Otherwise, the descriptions will be removed from your configuration when you upgrade.

To specify the interface description, use the **description** command in interface mode, like the following example:

```
awplus(config)# interface port1.0.2
awplus(config-if)# description camera-1
```

AMF group names

From version 5.4.7-1.1 onwards, AMF group names can only contain alphanumeric characters, hyphens and underscores.

If you have group names with other characters, change them before you upgrade. Otherwise, such group names will be removed from your configuration when you upgrade.

PPP usernames, service-names and hostnames

Prior to version 5.4.7-1.1, PPP did not always read escaped special characters (double-quotes, backslashes or spaces) correctly in usernames, service-names or hostnames. This has been corrected. PPP now handles all combinations of printable ASCII characters (ASCII 32-126) correctly, so you can use all printable ASCII characters in these names. No other characters are allowed.

This means that if your PPP configuration currently contains names with double-quotes, backslashes or spaces, the value used by PPP may change when you upgrade to version 5.4.7-1.1 or later.

If the name contains the special characters backslash, double-quote or space, those characters should be escaped with a backslash (e.g. three\ word\ name). However, if the name contains a literal backspace character, escaping the backspace character is optional. For example, entering either domain\\user or domain\user results in PPP reading domain\user.

Strings identified as WORD in CLI help

Many AlliedWare Plus commands allow you to enter a user-specified string, for example to name something. For such commands, the CLI help identifies that string with the placeholder WORD (for example, the command **username WORD**). From version 5.4.7-1.1 onwards, fewer characters are accepted as valid for WORD. The changes are:

- You can only enter printable ASCII characters (ASCII 32-126), not extended ASCII characters
- You cannot end the WORD with a single backslash
- You cannot use unmatched double-quote characters. For example, previously "example would have been accepted. Now it is not accepted
- You cannot use a WORD made up only of double-quote characters (e.g. """")
- You cannot end a WORD with a single space, even if preceded by a backslash. You should use quotes instead if you require a space.

If your configuration currently contains any of these disallowed options in a WORD, you need to reconfigure the WORD before you upgrade to version 5.4.7-1.1 or later.

The special characters backslash, double-quote and space should be avoided in the WORD if possible. If you cannot avoid these characters, the CLI parser will accept them if you escape them with a backslash (e.g. three\ word\ name).

SNMP passwords

Because of the change described above, you can only enter double quote or backslash characters in SNMP passwords if you escape the characters with a backslash.

In version 5.4.7-1.x, an issue meant that escaping these characters did not work correctly, so double quotes and backslashes could not be used in SNMP passwords. This issue has been resolved in version 5.4.7-2.1. You can now use these characters in SNMP passwords as long as you escape them with a backslash.

NVS memory is not supported on x230 Series switches

Applies to x230 Series switches

From version 5.4.7-0.2 onwards, x230 Series switches no longer use a separate internal NVS (Non-Volatile Storage) memory device. Instead, data that was stored in NVS is now stored in a special area in Flash memory. This change does not affect how you display log messages and other data that was previously stored in NVS.

When you upgrade to version 5.4.7-0.2 or later, all files in NVS are deleted. If you had stored files in NVS yourself and you want to keep those files, save them to Flash memory before upgrading.

Removing VLAN port membership may appear to take longer

Applies to all AlliedWare Plus switches that support VCStack

From version 5.4.7-1.1 onwards, you may find that the **switchport trunk allowed vlan remove** command appears to take longer to execute on a VCStack if you are configuring a large number of switchports. This is because the command now stops you from using the CLI until removal of VLAN port membership has finished on all stack members.

Precedence when matching by VLAN in a QoS policy-map on IE200 Series

Applies to IE200 Series switches

From version 5.4.7-1.1 onwards, if you use both an ACL and a **match vlan** clause to match by VLAN in a QoS policy-map on an IE200 Series switch, the ACL now takes precedence.

Packet forwarding when MTU is small on FS980M Series

Applies to FS980M Series switches

On FS980M Series switches, from version 5.4.7-1.1 onwards, if the MTU of a VLAN is set to less than 1500 bytes, all packet forwarding to that VLAN will be done using the slow path forwarding (via the CPU). This ensures that packets are fragmented correctly. Previously, packets sized 1500 bytes or more were hardware switched without being fragmented.

CPU usage graphs displaying higher values than previously

Applies to SBx81CFC960, x930 Series switches, and AR-series firewalls

Previously, output of the commands **show cpu** and **show cpu history** reported incorrectly low CPU usage values on devices that use multi-core CPUs. This has been corrected in version 5.4.7-1.1 onwards, so you may now see higher values reported, even though the CPU load has not increased.

Changes to OpenFlow support

Applies to x930, x510, x510L, IX5, DC2552XS/L3, x310, x230, GS900MX/MPX and XS900MX Series Switches

Version 5.4.7-0.1 removes support for some OpenFlow features:

- The hairpin link is no longer supported; the hybrid port is instead. When upgrading from 5.4.6-2.x or earlier to 5.4.7-0.1 or later, special care will have to be taken if a hairpin link is present. Please contact Allied Telesis Support for assistance on this.
- AMF guest nodes on ports using the OpenFlow protocol are no longer supported.

Traffic Control is disabled by default for bridged traffic

Applies to AR-Series Firewalls

On AR-series firewalls, version 5.4.7-0.1 onwards makes it possible for users to explicitly enable traffic control for bridged traffic per bridge interface.

Previously, traffic control was enabled by default on all bridge interfaces, which caused performance loss with heavy bridged traffic when traffic control or Unified Threat Management (UTM) was configured.

Now, traffic control is disabled by default for bridged traffic. To enable it, use the following new command in interface mode for the desired bridge:

```
awplus(config-if)#l3-filtering enable
```

We do not recommend shaping bridged traffic on firewalls that are running Unified Threat Management (UTM) features, because both Traffic Control and UTM require significant CPU resources.

Traffic Shaping commands have been deleted

Applies to AR3050S and AR4050S Firewalls

On AR4050S and AR3050S UTM firewalls, earlier releases deprecated Traffic Shaping and replaced it with Traffic Control. In version 5.4.7-0.1, Traffic Shaping commands have been deleted.

If you are running Traffic Shaping and you want to upgrade to 5.4.7-x.x from 5.4.5-x.x or an earlier version, upgrade to a 5.4.6-x.x version first and then save your configuration. AlliedWare Plus will convert your configuration automatically to a Traffic Control configuration.

See the Traffic Control Feature Overview and Configuration Guide for Traffic Control configuration details.

Reduction in number of IPv4 unicast/multicast route entries with some SBx8100 silicon profiles

Applies to SBx8100 switches

Version 5.4.7-0.1 reduces the total number of available IPv4 unicast/multicast route entries in the system by 4, when running silicon profiles default, profile1, or profile2.

Using the switch GUI with TACACS+ command authorization

Applies to AlliedWare Plus switches

If the switch GUI is being used when TACACS+ command authorization is enabled, from version 5.4.7-0.1 onwards, you need to configure the server to authorize the command **snmp-server configure-for-gui-access** for the GUI user.

In addition, the switch GUI uses a lot of standard CLI commands for its internal operation. This means that a user of the GUI will generally be limited to the same kind of operations they are limited to on the CLI. However, some GUI functionality is implemented using alternative mechanisms like SNMP and TFTP. This functionality will not be covered by command authorization.

This new requirement does not apply to the GUI on AR-series firewalls.

Changes to NTP configuration in AMF networks

Applies to all AlliedWare Plus devices

From version 5.4.7-0.1 onwards, the behavior of NTP has changed in AMF networks.

Previously, you needed to configure at least one external NTP server on only one of your AMF masters. Directly-connected nodes would also automatically NTP peer with each other.

Now all AMF nodes will only automatically receive time from the AMF master's NTP server. Nodes no longer peer with directly connected nodes. NTP now also synchronizes faster with the AMF master.

You now need to configure at least one external NTP server on all AMF masters in your network to ensure accurate logging, and consistent timestamps between all AMF nodes. Configuration of three or more NTP servers is considered best practice. Configured servers do not need to be the same between AMF Masters. One option is to use the pool of NTP servers provided by the NTP Pool Project (www.pool.ntp.org).

In some networks, the AMF masters may not have a path to such NTP servers. This may be due to ensuring the AMF masters and core of the network are locked down with no internet access. If so, a local NTP server, or AMF node which does have internet access, can be configured as the desired NTP server.

In this situation, configure the AMF masters to use the local server or other AMF node as its NTP server. Ensure the AMF Masters have IP reachability to the NTP server’s address.

When you have multiple AMF masters, the AMF masters will act as NTP peers of each other, and other nodes will use the AMF masters as NTP servers. This happens automatically; you do not have to configure it.

DC2552XS/L3 reboot history now stored in NVS

Applies to DC2552XS/L3 switches

When you upgrade a DC2552XS/L3 switch from 5.4.5-x.x or earlier to 5.4.7-x.x or 5.4.6-x.x, the switch's reboot history is reset. The ongoing reboot history will be stored in NVS. If you need to view the previous reboot history, see the file reboot.log in the Flash file system.

Change to login if a device does not boot up fully

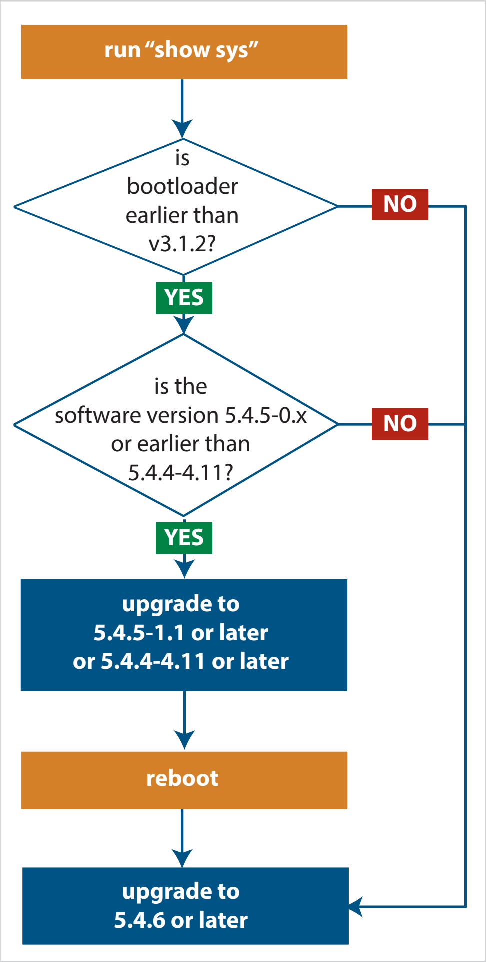
Applies to all AlliedWare Plus devices

In rare circumstances, a device may not boot up fully, in which case you may be able to press Ctrl-c to log into the device. This may mean that the device's configuration has not been run. From version 5.4.7-2.1 onwards, only the "manager" user can log in if this occurs.

Bootloader compatibility for SBx81CFC960

Applies to SBx8100 Series switches

On the AT-SBx81CFC960, please check your bootloader and current software version before you upgrade to AlliedWare Plus software version 5.4.6 or later.


run "show sys"
is bootloader earlier than v3.1.2?
NO
YES
is the software version 5.4.5-0.x or earlier than 5.4.4-11?
NO
YES
upgrade to 5.4.5-1.1 or later or 5.4.4-4.11 or later
reboot
upgrade to 5.4.6 or later

If your bootloader is older than 3.1.2, you can only upgrade to 5.4.6 or later from the following software versions:

- 5.4.5-1.1 or higher (including 5.4.5-2.x and 5.4.5-3.x)
- 5.4.4-4.11 or higher

If your bootloader is older than 3.1.2, your switch must be running one of the above versions when you upgrade to 5.4.6 or later.

Note that you cannot upgrade to 5.4.6 or later directly from 5.4.5-0.x.

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

```
awplus# show system
```

If you experience issues when upgrading, please contact your Allied Telesis support team. See our website at alliedtelesis.com/support.

Software Release Licensing

Applies to SBx908 and SBx8100 Series switches

AlliedWare Plus software releases need to be licensed for SBx908, SBx908 GEN2 and SBx8100 switches.

Please ensure you have a 5.4.7 license on your switch if you are upgrading to 5.4.7-x.x on your SBx908, 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 Software Version on an SBx908 or SBx908 GEN2 Switch" on page 44 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 46.

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

ISSU is available on standalone SBx8100 Series switches with dual CFC960 control cards, and on switches using VCStack Plus™ to create a single virtual unit out of two chassis (where each chassis has a pair of CFC960 control cards). ISSU allows you to upgrade the software release running on the CFCs with no disruption to network traffic passing through the chassis.

You cannot use ISSU to upgrade to 5.4.7-2.1 from any previous software version.

For each issue resolved on these platforms, the resolution will take effect as indicated when:

- CFCs upgraded: The issue will be resolved once all CFCs have rebooted and are running the same SW version.
- ISSU Complete: The issue will be resolved once all cards in the system are running the same SW version. This maintenance release cannot be upgraded from any previous release using ISSU.

Please refer to the ISSU compatibility matrix below to determine ISSU release compatibility. C= Compatible, I = Incompatible.

	To Release						
FROM	**Release**	**5.4.7-2.1**	**5.4.7-2.2**	**5.4.7-2.3**	**5.4.7-2.4**		
	5.4.7-2.1		C	I			
	5.4.7-2.2			C			
	5.4.7-2.3				C		
	5.4.7-2.4						

The issues resolved in software version 5.4.7-2.4 are listed in the section titled: "What's New in Version 5.4.7-2.4" on page 1.

Upgrading a VCStack with reboot rolling

Applies to all stackable AlliedWare Plus switches

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack. You can use the **reboot rolling** command to upgrade to 5.4.7-2.x from:

- 5.4.7-x.x, or
- 5.4.6-x.x, or
- 5.4.5-x.x, or
- 5.4.4-1.x or later.

To use reboot rolling, first enter the **boot system** command, which will install the new release file on all stack members. Then enter the **reboot rolling** command. Note that reboot rolling is not supported on SBx8100.

You cannot use rolling reboot to upgrade directly to 5.4.7-2.x from 5.4.4-0.x or earlier versions.

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. Auto-synchronization is supported between 5.4.7-2.x and:

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

It is not supported between 5.4.7-x.x and 5.4.6-1.1 or **any** earlier releases.

If your switch is currently running 5.4.6-1.1 or earlier...

On VCStacks

If you are working with a VCStack:

- If you want to upgrade an existing VCStack to 5.4.7-2.x, this should not cause any problems. The **boot system** command will automatically copy the new software release to all stack members. Do not reboot any individual stack members after installing the new release - instead reboot the stack as a whole.

  If you encounter any errors from the **boot system** command, then check that the release file was copied to all stack members before rebooting. If it was not, then address any problems reported, such as freeing up space in Flash for the new release file, and then repeat the **boot system** command again.
- If a stack is running v5.4.7-2.x, and you connect a switch running 5.4.6-1.1 or earlier to the stack, then the v5.4.7-2.x software will not be automatically copied over to the newly-added stack member, even if **stack software-auto-synchronize** has been enabled on the stack. Instead, upgrade the switch that is to be added to the stack to v5.4.7-2.x before you add it to the stack.
- If a stack is running 5.4.6-1.1 or earlier, and you connect a switch running v5.4.7-2.x to the stack, then the older software cannot be automatically copied over to the newly-added stack member, even if **stack software-auto-synchronize** has been enabled on the stack. Instead, downgrade the switch that is to be added to the stack to the older release before you add it to the stack.
- If you do boot up a stack with a switch running an incompatible version, the incompatible switch will boot up as a standalone unit. To recover, simply leave the incompatible switch cabled into the stack, log into it, upgrade or downgrade it to the desired release, and reboot the switch.

On a VCStack Plus Pair of SBx8100 chassis

If you are working with a VCStack Plus, what you need to do depends on whether you are installing a new CFC or a whole new chassis:

- If you want to upgrade an existing SBx8100 VCStack Plus system to v5.4.7-2.x, this should not cause any problems. The **boot system** command will automatically copy the new software release to all stack members. Do not reboot any individual CFCs or stack members after installing the new release - instead reboot the stack as a whole.

If you encounter any errors from the **boot system** command, then check that the release file was copied to all CFCs. If it was not, then address any problems reported, such as freeing up space in Flash for the new release file, and then repeat the **boot system** command again.

- If you want to insert a new dual CFC into a chassis that is part of an existing VCStack Plus system, refer to "Upgrading an SBx8100 chassis or adding a CFC to an SBx8100 chassis" below.
- If you want to insert a new SBx8100 chassis into a VCStack Plus system, refer to "On VCStacks" on page 46 above.

Upgrading an SBx8100 chassis or adding a CFC to an SBx8100 chassis

If you want to upgrade an existing SBx8100 that has two CFCs installed to v5.4.7-2.x, this should not cause any problems. The **boot system** command will automatically copy the new software release to both CFCs. Do not reboot any individual CFCs after installing the new release - instead reboot the chassis as a whole.

If you encounter any errors from the **boot system** command, then check that the release file was copied to both CFCs. If it was not, then address any problems reported, such as freeing up space in Flash for the new release file, and then repeat the **boot system** command again.

If you want to insert a new CFC into a chassis, then:

- If a standalone SBx8100 has a CFC installed that is running 5.4.6-1.1 or earlier, and you add a CFC running v5.4.7-2.x to the chassis, then the older software cannot be automatically copied over to the newly-added CFC.
- If a standalone SBx8100 has a CFC installed that is running v5.4.7-2.x, and you add a CFC running 5.4.6-1.1 or earlier to the chassis, then the v5.4.7-2.x software cannot be automatically copied over to the newly-added CFC.
- If you connect a CFC running an incompatible release to an SBx8100 chassis, you will be unable to log into the added CFC. For example, if the Active CFC is running v5.4.7-0.1 and another CFC joins with 5.4.6-0.x, the error you get is:

```
======
cfc960 login: manager
Password:
Last login: Thu Mar 23 02:15:21 UTC 2017 on ttyS0
All 1 lines for VR:PVR are busy. Try again later
======
```

To recover from this situation, see "Upgrading/downgrading a CFC" below.

To determine what release a CFC is running without logging in, look for the "Current release filename" console output when the CFC first boots up, e.g.

```
           ______________   ____
        /\ \            / /______\
      /   \ \_      __/ /| ______ |
    /      \ |     |  /  | ______ |
  /         \ \   / /     \ ____ /
/______/\____\ \/ /____________/

Allied Telesis Inc.
AlliedWare Plus (TM) v5.4.7
Current release filename: SBx81CFC400-5.4.7-0.1.rel
```

Upgrading/downgrading a CFC

If auto-synchronization is not available, you have manually upgrade or downgrade the CFC to match your existing SBx8100. This section describes two different ways to do this:

Option 1: Insert the new CFC into the chassis. Load the desired software version onto a USB stick and insert the USB stick into the chassis. Via the bootloader menu (CTRL+B), perform a one-off boot (option 1), select USB, then select the desired software version. Both CFCs should detect each other. Log in and enter **boot system** to ensure the desired software version is set on the new CFC.

Option 2: Remove the new CFC if you had already inserted it. Upgrade or downgrade the existing SBx8100 so that it is running the same software version as the new CFC. Reinsert the new CFC. Both CFCs should then detect each other successfully. You can then log in and set the desired software version on both CFCs.

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

If using an AMF controller

If you use an AMF Controller and **any** of your Controller or Area Master nodes are running 5.4.7-2.x, then they **all** must run 5.4.7-1.1 or later. Otherwise, the “show atmf area nodes” command and the “show atmf area guests” command will not function, and Vista Manager EX will show incorrect network topology.

If using secure mode

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

If using Vista Manager EX

If you are using Vista Manager EX, then:

- All nodes must run version 5.4.7-0.1 or later
- If any of your Controller or Area Master nodes are running 5.4.7-2.x, then they all must run 5.4.7-1.1 or later
- If your Master node is running 5.4.7-0.x, then all other nodes must also run 5.4.7-0.x (not 5.4.7-1.x or 5.4.7-2.x)
- If your AMF Master node is running 5.4.7-2.x, then member nodes can run 5.4.7-0.x or 5.4.7-1.x.

If using none of the above

If none of the above apply, then nodes running version 5.4.7-2.x are compatible with nodes running:

- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 5.4.4-x.x, and
- 5.4.3-2.6 or later.

Upgrading all switches in an AMF network

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

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

2. Decide which AMF upgrade method is most suitable.

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

x610 Series switch as AMF master

Versions 5.4.7-1.1 and later do not support x610 Series switches. If your network is using an x610 Series switch as an AMF master, you may not be able to upgrade any devices in your AMF network to 5.4.7-1.1 or later. This is because if your member devices run a newer version than the master, then compatibility issues may occur - see “AMF software version compatibility”.

To take advantage of AMF enhancements, we recommend replacing your x610 Series switch with a supported AMF master switch, such as an x930 Series switch.

Obtaining User Documentation

For full AlliedWare Plus documentation, see our online documentation Library. For AlliedWare Plus products, the Library includes the following documents:

- **Feature Overview and Configuration Guides** - find these by clicking here and searching for the feature name.
- **Datasheets** - find these by clicking here and searching for the product series.
- **Installation Guides** - find these by clicking here and searching for the product series.
- **Command References** - find these by clicking here and searching for the product series.

Verifying the Release File for x930 Series Switches

On x930 Series switches, 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 enter the following command to verify the SHA256 checksum of the file:

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

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

This command compares the SHA256 checksum of the release file with the correct checksum for the file.

The correct checksum is listed in the x930-<*relnum*>.sha256sum file, which is available on the Software Downloads page.

The following command contains the hash for 5.4.7-2.2, so you can simply copy and paste that command into the CLI if you wish to verify the file x930-5.4.7-2.2.rel:

```
crypto verify x930-5.4.7-2.2.rel b4880fa1c361f46f2386c6a63c1f6cabd1a3793b83aa1ec6746315875c979fc4
```

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 x930 Series switch models run the same release file and therefore have the same checksum.

Verifying the release on subsequent boot-ups

Once the switch has successfully verified the release file, it adds the **crypto verify** command to the running configuration.

If the switch is in secure mode, it will verify the release file every time it boots up. To do this, it runs the **crypto verify** command while booting. Therefore, you need to copy the **crypto verify** command to the startup configuration, by using the command:

```
awplus#copy running-config startup-config
```

If the **crypto verify** command is not in the startup configuration, the switch will report a verification error at bootup.

If there is a verification error at bootup, the switch produces an error message and finishes booting up. If this happens, run the **crypto verify** command after bootup finishes, to verify the running release file. If verification of the running release file fails, delete the release file and contact Allied Telesis support.

Licensing this Software Version on an SBx908 or SBx908 GEN2 Switch

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

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

1. Obtain the MAC address for a switch

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

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

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

2. Obtain a release license for a switch

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

3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. **Confirm release license application**

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

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

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

```
awplus#show license

Board region: Global

Index                          : 1
License name                   : Base License
Customer name                  : Base License
Type of license                : Full
License issue date             : 30-Nov-2017
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                   : 5.4.7
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 30-Nov-2017
License expiry date            : N/A
Release                        : 5.4.7
```

Licensing this Software Version on an SBx8100 Series Switch 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 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-2017
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.4.7-rl
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2017
License expiry date            : N/A
Release                        : 5.4.7
```

Installing this Software Version

Caution: Software versions 5.4.7-x.x require a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 or SBx908 GEN2 Switch" on page 52 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 54.

To install and enable this software version, use the following steps:

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

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

```
awplus# show file systems
```

To list files, use the command:

```
awplus# dir
```

To delete files, use the command:

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

You cannot delete the current boot file.

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

```
awplus# copy tftp flash
```

Follow the onscreen prompts to specify the server and file.

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

```
awplus# configure terminal
```

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

Product	Command
FS980M series	`awplus(config)# boot system FS980-5.4.7-2.4.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.4.7-2.4.rel`
GS970M series	`awplus(config)# boot system GS970-5.4.7-2.4.rel`
XS900MX series	`awplus(config)# boot system XS900-5.4.7-2.4.rel`
x230 series	`awplus(config)# boot system x230-5.4.7-2.4.rel`
IE200 series	`awplus(config)# boot system IE200-5.4.7-2.4.rel`
x310 series	`awplus(config)# boot system x310-5.4.7-2.4.rel`
IE300 series	`awplus(config)# boot system IE300-5.4.7-2.4.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.7-2.4.rel`
x510 series	`awplus(config)# boot system x510-5.4.7-2.4.rel`

Product	Command
x550 series	`awplus(config)# boot system x550-5.4.7-2.4.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.4.7-2.4.rel`
x550 series	`awplus(config)# boot system x550-5.4.7-2.4.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.7-2.4.rel`
DC2552XS/L3	`awplus(config)# boot system DC2500-5.4.7-2.4.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.4.7-2.4.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.7-2.4.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.7-2.4.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.7-2.4.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.4.7-2.4.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.7-2.4.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.7-2.4.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.7-2.4.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 the AR-Series Firewall GUI

This section describes how to access the firewall GUI, to manage and monitor your AR-series firewall. The GUI provides setup of the firewall, enabling the configuration of entities (Zones, Networks and Hosts) and then creating firewall and NAT rules for traffic between these entities.

Advanced firewall features can be enabled, configured and customized for a comprehensive security solution, such as Application control and Web control, as well as threat management features such as Intrusion Prevention, Malware protection, and Antivirus. Various other features can be managed through the GUI, and the dashboard provides at-a-glance monitoring of traffic, application use, and threat protection statistics.

If your AR-series firewall came with the GUI pre-installed, perform the following steps to browse to the GUI:

1. Connect to any of the LAN switch ports
2. Open a web browser and browse to https://192.168.1.1. This is the pre-configured IP address of VLAN1. The default username is *manager* and the default password is *friend*.

If your AR-series firewall did not come with the GUI pre-installed, perform the following steps through the command-line interface:

1. Create one or more IP interfaces and assign them IP addresses, including configuring WAN connectivity. For information about configuring PPP, see the PPP Feature Overview and Configuration Guide. For information about configuring IP, see the IP Feature Overview and Configuration Guide.
2. If you plan to enable the firewall functionality, first create a firewall rule to allow traffic from the Update Manager to pass through the firewall. This is needed because AR-series firewalls block all traffic by default. The following figure shows a recommended example configuration, when WAN connectivity is through ppp0:

```
zone public
 network wan
  ip subnet 0.0.0.0/0 interface ppp0
  host ppp0
   ip address dynamic interface ppp0

firewall
 rule 10 permit dns from public.wan.ppp0 to public.wan
 rule 20 permit https from public.wan.ppp0 to public.wan
 protect
```

3. Use the following command to download and install the GUI:

```
awplus# update webgui now
```

4. Enable the HTTP service:

```
awplus# configure terminal
```

```
awplus(config)# service http
```

5. Log into the GUI.

   Start a browser and browse to the firewall'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.

Installing the Switch GUI

This section describes how to install and set up the java-based GUI for switches. The GUI enables you to monitor and manage your AlliedWare Plus switch from your browser.

To install and run the GUI, you need the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up
- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

To install the GUI on your switch, use the following steps:

1. Copy to the GUI Java applet file (**.jar** extension) onto your TFTP server, SD card or USB storage device.

2. Connect to the switch's management port, then log into the switch.

3. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

4. Assign an IP address for connecting to the GUI. Use the commands:

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)#ip address <address>/<prefix-length>
   ```

   Where <*address*> is the IP address that you will subsequently browse to when you connect to the GUI Java applet. For example, to give the switch an IP address of 192.168.2.6, with a subnet mask of 255.255.255.0, use the command:

   ```
   awplus(config-if)# ip address 192.168.2.6/24
   ```

5. If required, **configure a default gateway for the switch.**

   ```
   awplus(config-if)# exit
   awplus(config)# ip route 0.0.0.0/0 <gateway-address>
   ```

   Where <*gateway-address*> is the IP address for your gateway device. You do not need to define a default gateway if you browse to the switch from within its own subnet.

6. Copy the GUI file onto your switch from the TFTP server, SD card, or USB storage device.

   TFTP server: Use the command:

   ```
   awplus# copy tftp://<server-address>/<filename.jar> flash:/
   ```

   SD card: use the command:

   ```
   awplus# copy card:/<filename.jar> flash:/
   ```

   USB storage device: use the command:

   ```
   awplus# copy usb:/<filename.jar> flash:/
   ```

   where *<server-address>* is the IP address of the TFTP server, and where *<filename.jar>* is the filename of the GUI Java applet.

7. Ensure the HTTP service is enabled on your switch. Use the commands:

   ```
   awplus# configure terminal
   ```

   ```
   awplus(config)# service http
   ```

   The HTTP service needs to be enabled on the switch before it accepts connections from a web browser. The HTTP service is enabled by default. However, if the HTTP has been disabled then you must enable the HTTP service again.

8. Create a user account for logging into the GUI.

   ```
   awplus(config)# username <username> privilege 15 password
                        <password>
   ```

   You can create multiple users to log into the GUI. For information about the **username** command, see the AlliedWare Plus Command Reference for your switch.

9. Start the Java Control Panel, to enable Java within a browser

   On your PC, start the Java Control Panel by opening the Windows Control Panel from the Windows Start menu. Then enter Java Control Panel in the search field to display and open the Java Control Panel.

   Next, click on the ‘Security’ tab. Ensure the ‘Enable Java content in the browser’ checkbox is selected on this tab.

10. Enter the URL in the Java Control Panel Exception Site List

    Click on the ‘Edit Site List’ button in the Java Control Panel dialog Security tab to enter a URL in the Exception Site List dialog. In the ‘Exception Site List’ dialog, enter the IP address you configured in Step 4, with a http:// prefix.

    After entering the URL click the Add button then click OK.

11. Log into the GUI.