Release Note for AlliedWare Plus Software Version 5.4.7-1.x

AlliedWare Plus OPERATING SYSTEM

» SBx8100 Series » SBx908 » DC2552XS/L3 » x930 Series
» x550 Series » x510 Series » IX5 » x310 Series » x230 Series
» IE500 Series » IE300 Series » IE200 Series
» XS900MX Series » GS970MX Series » GS900MX/MPX Series
» FS980M Series » AMF Cloud
» AR2010V » AR2050V » AR3050S » AR4050S
» 5.4.7-1.6 » 5.4.7-1.5 » 5.4.7-1.4 » 5.4.7-1.3 » 5.4.7-1.2 » 5.4.7-1.1

Acknowledgments

Getting the most from this Release Note

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

Content

Content iii

What's New in Version 5.4.7-1.6 1

Introduction 1

Issues Resolved in 5.4.7-1.6 3

Enhancements in 5.4.7-1.6 3

What's New in Version 5.4.7-1.5 1

Introduction 1

Issues Resolved in 5.4.7-1.5 5

What's New in Version 5.4.7-1.4 7

Introduction 7

Enhancements in 5.4.7-1.4 11

Issues Resolved in 5.4.7-1.4 12

What's New in Version 5.4.7-1.3 16

Introduction 16

What's New in Version 5.4.7-1.2 17

Introduction 17

Issues Resolved in Version 5.4.7-1.2. 17

What's New in Version 5.4.7-1.1 18

Introduction 18

New Features and Enhancements 21

Important Considerations Before Upgrading 33

Obtaining User Documentation 49

Verifying the Release File for x930 Series Switches 49

Licensing this Software Version on an SBx908 Switch 51

Licensing this Software Version on an SBx8100 Series Switch Control Card 53

Installing this Software Version 55

Accessing the AR-Series Firewall GUI 57

Installing the Switch GUI 58

What's New in Version 5.4.7-1.6

For:
IE300 Series only

Introduction

This release note describes the issues resolved in AlliedWare Plus software version 5.4.7-1.6. For more information, see the Command Reference for your switch or AR-series firewall. 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. 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 Switch" on page 51 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 53.

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
IE300-12GT IE300-12GP	IE300	10/2017	IE300-5.4.7-1.6.rel	ie300-gui_547_02.jar

Unsupported models

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

Caution: Using a software version file for the wrong switch or AR-series firewall model 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.

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

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	5.4.7-1.1	5.4.7-1.2	5.4.7-1.3	5.4.7-1.4	5.4.7-1.5	5.4.7-1.6
	5.4.7-1.1		C	I	I	I	I
	5.4.7-1.2			C	I	I	I
	5.4.7-1.3				C	I	I
	5.4.7-1.4					C	I
	5.4.7-1.5						I

The issues resolved in software version 5.4.7-1.6 are listed in the section titled: "Issues Resolved in 5.4.7-1.6" on page 3.

Issues Resolved in 5.4.7-1.6

This AlliedWare Plus maintenance version does not include any resolved issues.

Enhancements in 5.4.7-1.6

CR-58424 - For IE300 Series switches:
With this AlliedWare Plus maintenance version, the IE300 variant switches support 256 multicast groups, where previously 64 multicast groups were supported.

What's New in Version 5.4.7-1.5

For:

SwitchBlade x8100 Series
SwitchBlade x908
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 5.4.7-1.5. For more information, see the Command Reference for your switch or AR-series firewall. Software fC613-10526-00-REV 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. 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 Switch" on page 51 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 53.

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	10/2017	GS900-5.4.7-1.5.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	10/2017	FS980-5.4.7-1.5.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M	10/2017	GS970-5.4.7-1.5.rel	GS970-gui_547_03.jar
XS916MXT XS916MXS	XS900MX	10/2017	XS900-5.4.7-1.5.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	10/2017	IE200-5.4.7-1.5.rel	ie200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	10/2017	IE300-5.4.7-1.5.rel	ie300-gui_547_02.jar
IE510-28GSX-80	IE500	10/2017	IE510-5.4.7-1.5.rel	IE510-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	10/2017	x230-5.4.7-1.5.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	10/2017	x310-5.4.7-1.5.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	10/2017	IX5-5.4.7-1.5.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	10/2017	x510-5.4.7-1.5.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	10/2017	x550-5.4.7-1.5.rel	x550-gui_547_02.jar
SBx908 (see Table)	SBx908	10/2017	SBx908-5.4.7-1.5.rel	SBx908-gui_547_01.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	10/2017	x930-5.4.7-1.5.rel	x930-gui_547_01.jar
DC2552XS/L3		10/2017	dc2500-5.4.7-1.5.rel	dc2500-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	10/2017	SBx81CFC400-5.4.7-1.5.rel SBx81CFC960-5.4.7-1.5.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_02.jar
AR4050S AR3050S	AR-series UTM firewalls	10/2017	AR4050S-5.4.7-1.5.rel AR3050S-5.4.7-1.5.rel	See "Accessing the AR-Series Firewall GUI" on page 57
AR2050V AR2010V	AR-series VPN firewalls	10/2017	AR2050V-5.4.7-1.5.rel AR2010V-5.4.7-1.5.rel	See "Accessing the AR-Series Firewall GUI" on page 57
AMF Cloud		10/2017	vaa-5.4.7-1.1.iso (VAA OS) vaa-5.4.7-1.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-1.1.vhd (for Microsoft Azure)	

Unsupported models

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

Caution: Using a software version file for the wrong switch or AR-series firewall model 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.

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

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	5.4.7-1.1	5.4.7-1.2	5.4.7-1.3	5.4.7-1.4	5.4.7-1.5	
	5.4.7-1.1		C	I	I	I	
	5.4.7-1.2			C	I	I	
	5.4.7-1.3				C	I	
	5.4.7-1.4					C	

The issues resolved in software version 5.4.7-1.5 are listed in the section titled: "Issues Resolved in 5.4.7-1.5" on page 5.

Issues Resolved in 5.4.7-1.5

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	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57982	**AMF**	Previously, if more than 20 AMF virtual links were configured, any subsequent virtual links would not work. This issue has been resolved.	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-58042	**AMF**	With this software updated, the stability of an AMF network on x930 and x510 variant switches with nodes that have more than 20 AMF links has been improved. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-57943	**AMF** **SNMP**	Previously, on a SBx81CFC400 controller, AMF SNMP traps for node or link status changes could cause excessive CPU load. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	Y
CR-57848	**Policy based routing**	Previously, packets matching policy-based-routing (PBR) rules may not have been processed correctly. As a result, those packets were not routed correctly via the appropriate next-hop. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-58144	**Port Configuration**	Previously, on x930 variant switches, if the **wrr-queue disable** command was configured on a port, it was possible that the port would no longer correctly respond to link-down events, leaving the port showing as running. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-57957	**PPP**	Previously, when the primary address of an interface was changed dynamically, any static route with a point-to-point (PPP) interface configured as the nexthop could fail to route packets. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-58058	**Radius**	Previously, RADIUS authentication did not accept passwords longer than 16 characters. With this software update, the password length has been increased to 128 characters, which is the maximum length that the RADIUS attribute User-Password allows. 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	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57987	**URL Filtering Logging**	Previously, when using URL Filtering, the **log url-requests** feature would not work for HTTPS requests when NAT was also being used. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-57920	**VCStack Hotswap PBR**	Previously, failing over a stack member with policy-based-routing (PBR) configured and forwarding traffic that was targeting the PBR nexthop could increase the time the failover member took to join the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–

What's New in Version 5.4.7-1.4

For:

SwitchBlade x8100 Series
SwitchBlade x908
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 5.4.7-1.4. For more information, see the Command Reference for your switch or AR-series firewall. 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. 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 Switch" on page 51 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 53.

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	09/2017	GS900-5.4.7-1.4.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	09/2017	FS980-5.4.7-1.4.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M *available Sept 2017	09/2017	GS970-5.4.7-1.4.rel	coming soon
XS916MXT XS916MXS	XS900MX	09/2017	XS900-5.4.7-1.4.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	09/2017	IE200-5.4.7-1.4.rel	ie200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	09/2017	IE300-5.4.7-1.4.rel	ie300-gui_547_02.jar
IE510-28GSX-80	IE500	09/2017	IE510-5.4.7-1.4.rel	IE510-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	09/2017	x230-5.4.7-1.4.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	09/2017	x310-5.4.7-1.4.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	09/2017	IX5-5.4.7-1.4.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	09/2017	x510-5.4.7-1.4.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	09/2017	x550-5.4.7-1.4.rel	x550-gui_547_02.jar
SBx908 (see Table)	SBx908	09/2017	SBx908-5.4.7-1.4.rel	SBx908-gui_547_01.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	09/2017	x930-5.4.7-1.4.rel	x930-gui_547_01.jar
DC2552XS/L3		09/2017	dc2500-5.4.7-1.4.rel	dc2500-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	09/2017	SBx81CFC400-5.4.7-1.4.rel SBx81CFC960-5.4.7-1.4.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_02.jar
AR4050S AR3050S	AR-series UTM firewalls	09/2017	AR4050S-5.4.7-1.4.rel AR3050S-5.4.7-1.4.rel	See "Accessing the AR-Series Firewall GUI" on page 57
AR2050V AR2010V	AR-series VPN firewalls	09/2017	AR2050V-5.4.7-1.4.rel AR2010V-5.4.7-1.4.rel	See "Accessing the AR-Series Firewall GUI" on page 57
AMF Cloud		09/2017	vaa-5.4.7-1.1.iso (VAA OS) vaa-5.4.7-1.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-1.1.vhd (for Microsoft Azure)	

Unsupported models

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

Caution: Using a software version file for the wrong switch or AR-series firewall model 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.

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

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	5.4.7-1.1	5.4.7-1.2	5.4.7-1.3	5.4.7-1.4		
	5.4.7-1.1		C	I	I		
	5.4.7-1.2			C	I		
	5.4.7-1.3				C		

The issues resolved in software version 5.4.7-1.4 are listed in the section titled: "Issues Resolved in 5.4.7-1.4" on page 12.

Enhancements in 5.4.7-1.4

CR	Module	Description	FS980M	FS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-1222	**Multicast Routing**	With this software update, a new command: **`platform stop-unreg-mc-flooding`** has been implemented to stop the flooding of unregistered multicast packets to all VLAN members. This update applies to the SBx908 switch with XEM-2XP, XEM-2XS, XEM-2XT, XEM-12Tv2, XEM-12Sv2, XEM-24T XEM models installed.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
ER-1281	**ACL** **IPv6**	With this software update, it is now possible to configure IPv6 Hardware ACLs on x230 series switches.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
ER-1507	**PoE**	With this software update, PoE firmware on FS980 series switches has been updated.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
ER-1508	**PoE**	With this software update, PoE dynamic mode is now supported on FS980 series switches.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

Issues Resolved in 5.4.7-1.4

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	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57188	**AMF**	Previously, enabling AMF on an IE200 variant switch could cause the switch to lock up. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-57349	**AMF**	Previously, an unexpected termination of background AMF processes could occur on a large AMF network with a VAA master. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-57789	**AMF**	Previously, after the command **`atmf cleanup`** was issued to reset a x230 variant switch to factory default, the autoboot feature would fail to work. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-57601	**AMF**	Previously, on x930 and x550 series switches, the **`show mac address-table`** command did not always reflect what was in the hardware table. This issue only occurred when a MAC address was switched between static and dynamic address allocation. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–	–	–	–
CR-57782	**AMF**	Previously, AMF recovery needed to learn information about the network at startup to allow nodes to join, and contact an AMF Master. This process was being delayed due to the new default startup behaviour. With this software update, more time is provided for the AMF recovery process to complete. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y
CR-56873	**EPSR** **VCStack**	Previously, when adding a data VLAN to a blocked EPSR port in a stacked environment, it was possible that the data VLAN would not be blocked. This issue has been resolved.	Y	–	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-57693	**Firewall**	Previously, the firewall rules using dynamic interfaces would not always work after a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57748	**IP Reputation**	Previously, when IP Reputation started up, it was sometimes possible for erroneous error messages to be generated indicating that each of the IP Reputation categories could not be found. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-58035	**LACP**	Previously, when using a static ARP with a multicast MAC address that used a LACP based aggregator as the nexthop port, the ports used to egress the frames would not be updated when ports were dynamically added or removed from the aggregator by LACP. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-57038	**Logging**	Previously, you could enter a log configuration command to filter by program, for example: **`log (console|buffered|permanent) program...`** with **invalid** parameters. This issue has been resolved and an invalid program parameter is now rejected at the CLI. When running the fixed AlliedWare Plus version for the first time, an error might be logged at startup and the invalid config line will not show up in the running-configuration. After the first successful restart, you should save the running-configuration to the startup-configuration.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
CR-57784	**PIM-SM**	Previously, an IGMP Layer 2 entry could only be flagged as either static or dynamic. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	Y	Y	Y	Y	–	–	Y	Y	Y	–	–	–	Y
CR-57278	**PKI**	This software update will allow logging of all PKI related failures as part of the Common Criteria requirements.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-57282	**PoE**	Previously, a PoE device would not be detected correctly on FS980 series switches. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-57740	**PPP** **USB Modem**	Previously, PPP over 3G USB modems did not have any configured PPP DNS options applied. This issue has been resolved, now PPP over 3G USB modems retain their default PPP DNS option of request.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57674	**PTP Transparent Clock**	Previously, on x930 series switches, port number 1.0.25 and 1.0.26 linked at 10G would exhibit large resident delay values in PTP synchronisation frames when enabled in 1588 Transparent Clock mode. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-57852	**PTP Transparent Clock**	Previously, the synchronisation frame resident time values did not reflect correct timestamps. This issue has been resolved.	–	–	–	–	Y	Y	Y	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-57606	**RADIUS**	Previously, when EAP-TLS and PEAP authentication were disabled in the startup configuration, the switch would still boot-up with a warning message that the EAP-TLS authentication was still enabled. 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-57767	**Restful API**	Previously, a Restful API process could fail when low memory was reported on a device as a result of a large number of neighbours being learnt or timing out. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-57755	**Static Aggregation**	Previously, when using either of the **`arp mac-disparity`** or **`arp A.B.C.D <MULTICAST-MAC>`** commands on device, it was possible for traffic not to egress correctly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-57665	**Switching**	Previously, a "soft" parity error within x930 series switches could result in a continuous output of parity error correction log messages being generated, and this could eventually cause an internal process to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-57771	**Switching**	Previously, port flush times were delayed unnecessarily in a stacking environment This issue has been resolved.	–	Y	Y	Y	–	–	Y	–	Y	Y	Y	–	Y	Y	–	–	–	–	–	–	–
CR-57720	**System**	With this software update, several unnecessary memory allocations have been addressed. 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	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57817	**Unicast Routing**	Previously, in configurations involving recursive routes it was possible for a system reboot to occur during the addition and remove of ECMP routes. 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
CR-57311	**VLAN**	Previously, when a switchport was configured as a private-vlan and in trunk mode, and then the configuration was removed, the port would incorrectly remain configured as a private vlan port. This meant the port would not be able to operate as a regular trunk or access port. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–

What's New in Version 5.4.7-1.3

For: x550 Series only

Introduction

This release note provides support for the x550 Series platform.

The x550 Series platform is a new platform containing two models supported by AlliedWare Plus software release version 5.4.7-1.3.

Product models and 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.

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

Table 1: x550 Series models and software file names

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ	x550	08/2017	x550-5.4.7-1.3.rel	x550-gui_547_02.jar

Caution: Using a software version file for the wrong switch or AR-Series firewall model 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.

What's New in Version 5.4.7-1.2

For: x230 Series only

Introduction

This release note describes the issues resolved in AlliedWare Plus software version 5.4.7-1.2. For more information, see the Command Reference for your switch or AR-series firewall. 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.

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
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	08/2017	x230-5.4.7-1.2.rel	x230-gui_547_01.jar

Unsupported models

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

Caution: Using a software version file for the wrong switch or AR-series firewall model 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

Issues Resolved in Version 5.4.7-1.2.

CR	Module	Description
CR-57789	AMF	Previously, after the command **atmf cleanup** was issued to reset a x230 variant switch to factory default, the autoboot feature would fail to work. This issue has been resolved.

What's New in Version 5.4.7-1.1

For:

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

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.7-1.1. For more information, see the Command Reference for your switch or AR-series firewall. 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.

Caution: Software version 5.4.7-x.x requires a release license for the SBx908 and SBx8100 switches. 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 Switch" on page 51 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 53.

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	07/2017	GS900-5.4.7-1.1.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	07/2017	FS980-5.4.7-1.1.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M *available Sept 2017	07/2017	GS970-5.4.7-1.1.rel	coming soon
XS916MXT XS916MXS	XS900MX	07/2017	XS900-5.4.7-1.1.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2017	IE200-5.4.7-1.1.rel	ie200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	07/2017	IE300-5.4.7-1.1.rel	ie300-gui_547_02.jar
IE510-28GSX-80	IE500	07/2017	IE510-5.4.7-1.1.rel	IE510-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	07/2017	x230-5.4.7-1.1.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2017	x310-5.4.7-1.1.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	07/2017	IX5-5.4.7-1.1.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	07/2017	x510-5.4.7-1.1.rel	x510-gui_547_01.jar

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
SBx908 (see Table 2)	SBx908	07/2017	SBx908-5.4.7-1.1.rel	SBx908-gui_547_01.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2017	x930-5.4.7-1.1.rel	x930-gui_547_01.jar
DC2552XS/L3		07/2017	dc2500-5.4.7-1.1.rel	dc2500-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	07/2017	SBx81CFC400-5.4.7-1.1.rel SBx81CFC960-5.4.7-1.1.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_02.jar
AR4050S AR3050S	AR-series UTM firewalls	07/2017	AR4050S-5.4.7-1.1.rel AR3050S-5.4.7-1.1.rel	See "Accessing the AR-Series Firewall GUI" on page 57
AR2050V AR2010V	AR-series VPN firewalls	07/2017	AR2050V-5.4.7-1.1.rel AR2010V-5.4.7-1.1.rel	See "Accessing the AR-Series Firewall GUI" on page 57
AMF Cloud		07/2017	vaa-5.4.7-1.1.iso (VAA OS) vaa-5.4.7-1.1. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-1.1.vhd (for Microsoft Azure)	

Unsupported models

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

Not all models of XEM are supported in the SwitchBlade x908 by version 5.4.7-x.x. The following table lists which XEMs are and are not supported by version 5.4.7-x.x.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.7-x.x

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

Caution: Using a software version file for the wrong switch or AR-series firewall model 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.

New Features and Enhancements

This section summarizes the new features in 5.4.7-1.1 since 5.4.7-0.1. Some features are also supported in 5.4.7-0.x maintenance releases, as indicated.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 49.

Changes to default start-up behavior

Applies to all AlliedWare Plus devices

From AlliedWare Plus versions 5.4.7-0.4 onwards and 5.4.7-1.1 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, or otherwise the device uses an IP address of 169.254.42.42.

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

AR-Series Firewalls are typically 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**.

For details of the management interface and the new start-up behavior, see "Changes to default start-up behavior" in the "Important Considerations Before Upgrading" on page 33 section of this release note.

Connectivity Fault Management (CFM)

Available on SBx8100, x930, x510, x510L, IX5, x310, x230, IE500, IE300 and IE200 Series Switches

Version 5.4.7-1.1 adds support for 802.1ag and ITU Y.1731 Connectivity Fault Management. For many years, Network Service Providers (NSPs) have managed their networks using the FCAPS model: Fault, Configuration, Accounting, Performance, and Security. CFM is an IEEE 802.1ag and ITU Y.1731 standard for managing connectivity at the Ethernet service level. The 802.1ag standard adds Fault management capabilities to Ethernet, while the ITU Y.1731 standard expands the capabilities to include Performance.

Ethernet CFM provides the network operator with a way to detect faults in the network, and to isolate the location of the fault at either the link level (i.e. port) or at the VLAN level. Y.1731 extends this, and also provides a way to manage Service Level Agreements (SLAs) at the link level, but more importantly at the VLAN level.

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

Support for G.8032 on x310 Series switches

Version 5.4.7-1.1 adds support for G.8032 ring protection on x310 Series switches. A number of other AlliedWare Plus switches already support G.8032.

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 for G.8032, see the G.8032 Feature Overview and Configuration Guide.

Support for IPv6 hardware ACLs on XS900MX Series switches

Version 5.4.7-1.1 adds support for IPv6 hardware ACLs on XS900MX Series switches. AlliedWare Plus x-series and IE-series switches already support IPv6 hardware ACLs.

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

Multicast routing support for VRF-lite on SBx8100

On SwitchBlade x8100 Series, version 5.4.7-1.1 extends support for VRF-lite to include multicast routing. You can now configure IGMP and PIM Sparse Mode on individual VRF-lite instances.

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

For more information and configuration details for IGMP, see the IGMP/MLD Feature Overview and Configuration Guide.

For more information and configuration details for PIM Sparse Mode, see the PIM-SM Feature Overview and Configuration Guide.

Allied Telesis Autonomous Management Framework™ (AMF) enhancements

Multiple Tenants on AMF Public Cloud (Microsoft Azure and Amazon Web Services)

Version 5.4.7-1.1 adds support for multiple tenants on AMF Public Cloud, specifically using the Amazon Web Services and Microsoft Azure cloud platforms. AMF Cloud allows an AMF Master and/or Controller to be virtual appliances, rather than integrated into an Allied Telesis switch or firewall.

Each tenant network (an AMF area) is kept separate from other tenant networks allowing very flexible deployment, and central or individual network management options. The tenants in each AMF area could be branch offices of a single organization, or separate customers managed by a single service provider. A service provider could also provision AMF areas for tenants, and the tenants manage their own network. This is possible because each AMF area is isolated from all others, so any tenant can only view and manage their own network.

The key advantage of hosting multiple tenants on a single VAA, over a traditional AMF installation, is that each tenant network does not require an Allied Telesis Master capable device. This creates a high-value solution for large distributed companies, as well as service providers offering network provisioning and/or management services.

Virtual machines can support a variety of hosting options, including Amazon Web Service (AWS) and Microsoft Azure, which are cloud-based services. The major benefit of cloud-based services is that they are not bound by the constraints of fixed physical local hardware. This reduces the total cost of ownership, with servers and services which can be created/deleted as desired.

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

For instructions about installing the VAA, see the Install Guide: Virtual AMF Appliance (VAA) for AMF Cloud.

AMF Secure Mode

Available on all AlliedWare Plus devices that support AMF.

The AMF secure mode feature improves the security of the AMF network by reducing the risk of your network being compromised through unauthorized access to the AMF network. It achieves this by:

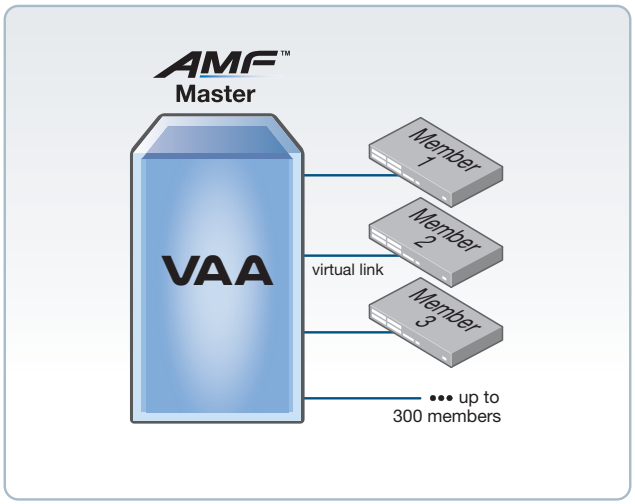
- Adding an authorization mechanism before allowing an AMF member to join an AMF network.
- Encrypting all AMF packets sent between AMF nodes.
- Addition logging, which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

AMF secure mode is optional and enabled from the command line interface. When running in AMF secure mode the AMF controllers and masters in the AMF network form a group of certification authorities. A node may only join a secure AMF network once authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

Support for up to 300 virtual links on Virtual AMF Appliance

Version 5.4.7-1.1 enables you to create up to 300 virtual links between a VAA and other AMF nodes. The VAA must be installed on your own server; installations on Amazon Web Services and Microsoft Azure only support 60 virtual links.

The 300 virtual links feature is supported on topologies where the node at the top is a VAA and the nodes connected through the virtual links are all in separate domains, all at a core distance of 1, as shown in the following figure.



For example, this could be a number of branch office switches connected to a VAA through virtual links. Each branch office switch would have only one AMF link, which is the virtual link to the Master device.

We recommend that the VAA have at least:

- 2 vCPU (Intel Xeon E3-1230v2 or equivalent)
- 2 GB RAM

There are no command changes required to support the increased number of virtual links. For configuration details and more information about virtual links, see the AMF Feature Overview and Configuration Guide.

ECMP routing for dynamically addressed interfaces

Available on AR-Series Firewalls

Version 5.4.7-1.1 adds support for static Equal Cost Multi-path (ECMP) Routing for interfaces whose IP address is typically dynamically assigned, such as PPP interfaces and virtual tunnel interfaces.

This means that if you create two static routes to the same remote destination network, the egress interfaces can be specified as the next hop for the routes, instead of the next hop ip address. The AR-series firewall will then balance traffic flows via the two routing paths. For example, to use ECMP routing via tunnel1 and tunnel2, use commands like the following:

```
awplus(config)#ip route 192.168.2.0/24 tunnel1
awplus(config)#ip route 192.168.2.0/24 tunnel2
```

URL filtering and Web Control categorization of HTTPS web sites using TLS SNI

Available on AR-Series Firewalls

From 5.4.7-1 onwards, the URL filtering feature has been extended to include the ability to filter SSL-protected websites. For HTTPS requests, the original URLs are encrypted, therefore they are not visible for processing. Instead the domain name specified in TLS SNI (Transport Layer Security Server Name Indication) for each HTTPS request is used as the URL for matching. This filtering capability can be used with user defined white-lists/black lists, as well as with Kaspersky black lists.

From 5.4.7-1 onwards, the Web-Control feature has also been extended to include the ability to categorize SSL-protected websites. The categorization is performed based on the Server Name Indication (SNI) field contained within the Client Hello message during the Transport Layer Security (TLS) handshake, as the SNI is in clear-text and represents the domain part of the URL of the HTTPS request.

The SNI field is contained within the Client Hello message supplied during the TLS handshake when a client web browser first attempts to access a secure HTTPS server website. The SNI information is supplied in clear-text, and represents the domain part of the URL of the HTTPS request. The SNI field is used by secure web servers hosting multiple secure websites, and allows a secure web server with a single public IP address to host multiple websites. It allows the secure web server to supply the correct digital certificate containing the correct domain name(s) to the requesting web browser client, so that the negotiation of the encrypted connection to the website can proceed.

For information about using URL filtering or Web-Control, see the URL Filtering Feature Overview and Configuration Guide or the Web Control Filtering Feature Overview and Configuration Guide.

Access the Firewall GUI from an HTTPS port other than 443

Applicable to AR-Series Firewalls

Version 5.4.7-0.3 onwards and version 5.4.7-1.1 onwards enable you to change the HTTPS port used to access the Firewall GUI. The default HTTPS port used by the Firewall GUI is 443.

To change the port, use the following new command:

```
awplus(config)#http secure-port <1-65535>
```

Note that any device on which a non-default secure port is set will have limited capabilities when accessed via Vista Manager. Additionally all external API requests will need to be directed to the configured port, instead of the default port 443.

For more information about the Firewall GUI, see Getting Started with the VPN Firewall GUI and Getting Started with the UTM Firewall GUI.

Firewall logging enhancements

Available on AR-Series Firewalls

Version 5.4.7-1.1 enhances the logging of URL requests and firewall connections.

For details of these enhancements, see the URL Filtering Feature Overview and Configuration Guide and the Firewall and NAT Feature Overview and Configuration Guide.

Note that log messages related to the firewall UTM features are generated by different programs, but from version 5.4.7-0.1 onwards they are all now assigned the facility 'local5'. This means you can easily filter log messages for all UTM messages via a single filter, for instance, to send all UTM log messages from multiple devices to a single destination.

The UTM log messages are generated by these programs:

- The program IPS generates messages for the stream-based security features Intrusion Prevention System, IP Reputation, Malware Protection, URL Filtering.
- The program UTM generates messages for the proxy-based security features Web Control and Anti-virus.

Example To configure an AR-Series firewall to generate log messages for any UTM features that are enabled and send them to a syslog server at IP address 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# log host 192.168.1.1 facility local5
```

URL Filtering: Logging all URL requests

By default, URL filtering only logs dropped requests. However, from version 5.4.7-1.1 onwards, you can turn on additional URL request logging to log all URL requests, including permitted requests. Use the following commands:

```
awplus(config)# url-filter
awplus(config-url-filter)# log url-requests
```

Firewall: Logging connections

Firewall connection logging can now be enabled to provide additional logs that show the start and end of connections passing through the firewall. Like the UTM messages, these messages are assigned facility local5. They have severity 'info' (6).

To enable logging of new connections, closed connections, or both passing through the firewall, use the commands:

```
awplus# configure terminal
awplus(config)# connection-log events {new|end|all}
```

To show the configuration of firewall connection logging, use the following command:

```
awplus# show connection-log events
```

Configurable TCP established session timeout

Available on AR-Series Firewalls

By default, when a TCP session is successfully established through the AR-Series firewall, when the session goes idle it automatically times out of the firewall connection tracking table after 3600 seconds.

In some situations it may be beneficial to time out unused established TCP sessions earlier. For example, in a busy environment where there is an excessive number of sessions being established, the firewall connection tracking table could become oversubscribed, with new connections being blocked until older sessions are timed out.

From version 5.4.7-1.1 onwards, the following new command is available to set a non-default TCP session timeout for established idle sessions:

```
awplus(config)# ip tcp timeout established <1-31536000>
```

4G/LTE USB Cellular Modem Support

Available on AR-Series Firewalls

Version 5.4.7-0.2 onwards and version 5.4.7-1.1 onwards add support for 4G cellular modems, which offer much higher-speed data transfer than older 3G modems. A cellular modem can be used for AR-Series firewalls in remote locations, or as a back-up link to be used when the primary Internet connection is unavailable.

The 4G cellular interface supports the following features:

- Static or dynamic IPv4 addressing via DHCP
- Configuration of the MTU
- Control by firewall
- Traffic Control

For more information and configuration details, see the USB Cellular Modem Feature Overview and Configuration Guide.

Changing the Administrative Distance of a default gateway route learned via DHCP

Applies to all AlliedWare Plus devices

Version 5.4.7-0.2 onwards and 5.4.7-1.1 onwards enable you to change the Administrative Distance of a default gateway route learned via a DHCP client interface.

To do this, use the following command:

```
awplus(config-if)#ip dhcp-client default-route distance <1-255>
```

Previously, when an interface (such as a VLAN, or an AR-Series Firewall ethernet interface, or 4G) was operating as a DHCP client and learned gateway information via DHCP, then an associated default route was added to the RIB with an Administrative Distance (AD) of 1.

This enhancement allows the user to modify the AD of the default route to a non-default value.

This is useful if the interface operating as a DHCP client is being used to provide backup WAN connectivity, as it ensures any pre-existing default routes out other (primary) interfaces which have a higher AD cost value (AD>1) to continue to be used when the DHCP client interface becomes active.

OpenFlow™ enhancements

Available on x930, x510, x510L, IX5, DC2552XS/L3, x310 and x230 Series Switches

Version 5.4.7-1.1 includes several OpenFlow enhancements, which are summarized below. For details of the enhancements, see the OpenFlow Feature Overview and Configuration Guide.

Enhanced security: OpenFlow encryption

Version 5.4.7-1.1 onwards includes TLS Encryption support on AlliedWare Plus OpenFlow devices. This feature secures the OpenFlow control plane connections.

The switch-to-controller connection can be either TCP based, or SSL based. SSL is recommended for security, as the connection link is encrypted and authenticated. In order to set up a secure link, keys and certificates must be defined before the controller is added with the protocol specified as SSL.

Transport Layer Security (TLS) v1.0, TLS v1.1 and TLS v1.2 are supported on secure link(s). The TLS version used between an OpenFlow switch and OpenFlow controller is determined by peer negotiation.

For step-by-step configuration instructions, see the OpenFlow Feature Overview and Configuration Guide.

Inactivity Timeout and Behavior

The OpenFlow controller manages the operation of switch port status and flows. If the connection between the switch and controller is broken, or there are no controllers defined, you can configure the switch to behave in one of two ways: standalone or secure mode.

Standalone mode

In standalone mode, if no message is received from the OpenFlow controller for three times the inactivity probe interval, then the OpenFlow protocol will take over responsibility for setting up flows. The OpenFlow protocol will cause the switch to act like an ordinary MAC-learning switch, but continue to retry connecting to the controller in the background. When the connection succeeds, it will discontinue its standalone behavior.

To specify this mode, use the command:

```
awplus#openflow failmode standalone
```

Secure mode

In secure mode, the OpenFlow protocol will not set up flows on its own when the controller connection fails or when there are no controllers defined. The switch will continue to retry connecting to any defined controllers forever.

This mode is the default, or you can specify it by using the command:

```
awplus#no openflow failmode standalone
```

Inactivity Timeout

Version 5.4.7-1.1 provides support for an inactivity probe. This provides you with better control of switch connections to an OpenFlow controller(s) and reduces the log messages for inactivity until the probe timer expires.

To control how long it will take for the switch to consider its connection to the controller broken, use the command:

```
awplus#openflow inactivity <timeout>
```

where <timeout> is the number of seconds before the switch will send an inactivity probe.

The switch will wait two times the inactivity time before considering that the link has failed.

The default inactivity probe timeout is 10 seconds.

Specify SMTP domain name for email

Available on all AlliedWare Plus devices

Version 5.4.7-1.1 enables you to specify an SMTP server by specifying its domain name (FQDN) instead of its IP address. This makes it possible for your device to send email if you only know the server's domain name.

To configure this, enter the domain name in the command:

```
awplus(config)#mail smtpserver <name>
```

You must also ensure that the DNS client on your device is enabled. It is enabled by default but if it has been disabled, you can re-enable it using the command:

```
awplus(config)#ip domain-lookup
```

Logging to external media

Available on all AlliedWare Plus devices that support an external memory device

Version 5.4.7-1.1 adds support for external logging, which sends syslog messages to a file on a USB memory device or SD card.

It also adds commands to copy the contents of the buffered log (**copy buffered-log**) and permanent log (**copy permanent-log**) to a destination file in a different external or internal location.

For details, see the Logging Feature Overview and Configuration Guide.

Increase in number of ACLs on DC2552XS/L3

With version 5.4.7-0.3 onwards and version 5.4.7-1.1 onwards, you can configure up to 757 hardware ACL entries, instead of the previous limit of 245.

Note that other features (policy-based QoS and DoS) also use hardware ACL entries internally, so configuring those features reduces the number of ACLs you can create.

Addressless IGMP mroute proxy interfaces

Available on all AlliedWare Plus devices that support IGMP snooping querier

From version 5.4.7-1.1 onwards, IGMP mroute proxy interfaces do not have to be configured with an IP address before they can operate. Now it is possible to have an address-less interface to operate as an IGMP mroute proxy interface.

This feature is useful when IGMP-Proxy needs to run on many downstream interfaces. For example, you may want to use it if your device has one subscriber (multicast receiver) per VLAN, and many receivers (many VLANs) connected to the device. In such a situation, assigning IP addresses to each VLAN may not be practicable.

Note that for such interfaces to be able to send queries to hosts directly attached to the interface, it is necessary to enable IGMP snooping querier on the interface, using the command **ip igmp snooping querier**.

An example of an IGMP Proxy configuration is:

```
...
ip multicast-routing
....
!
interface vlan10
 ip address 192.168.10.1/24
 ip igmp
 ip igmp proxy-service
!
interface vlan20,vlan30
 ip igmp
 ip igmp mroute-proxy vlan10
 ip igmp snooping querier
```

VRRPv3 alternate checksum mode

Available on all AlliedWare Plus devices that support VRRPv3

Version 5.4.7-1.1 adds support for an alternate checksum mode for VRRPv3 to allow inter-operability with some other vendors' products. This mode may be required if the other product indicates checksum errors on VRRP packets sent by AlliedWare Plus devices.

To configure the alternative mode (for VRRP instance 1 and VLAN1 in this example), use the commands:

```
awplus#configure terminal
awplus(config)#router vrrp 1 vlan1
awplus(config-router)#alternate-checksum-mode
```

Allow G.8032 and EPSR to protect the same data VLAN

Available on all AlliedWare Plus devices that support G.8032

From version 5.4.7-1.1 onwards, a G.8032 sub-ring may be connected to and interact with an EPSR ring.

In some supported scenarios, you will need to enable an EPSR instance to send out a FLUSH-FDB-PDU message after being notified of a topology change by an ERP instance. To do this, use the following new command:

```
awplus(config)#epsr <epsr-instance-name> topology-change g8032
```

For more information, see the "Connecting G.8032 and EPSR" section of the G.8032 Feature Overview and Configuration Guide.

Minimum password lifetime

Available on all AlliedWare Plus devices

Version 5.4.7-0.2 onwards and version 5.4.7-1.1 onwards allow you to configure a minimum number of days before a password can be changed by a user. With this feature enabled, once a user sets the password, the user cannot change it again until the minimum lifetime has passed.

The minimum lifetime is helpful in conjunction with a security policy that prevents people from re-using old passwords. For example, if you do not allow people to re-use any of their last 5 passwords, a person can bypass that restriction by changing their password 5 times in quick succession and then re-setting it to their previous password. The minimum lifetime prevents that by preventing people from changing their password in quick succession.

To set the minimum lifetime, use the commands:

```
awplus#configure terminal
awplus(config)#security-password min-lifetime-enforce <0-1000>
```

where 0-1000 is the minimum lifetime in days.

Configuring time-out of half-open TCP connections

Available on all AlliedWare Plus devices

Version 5.4.7-1.1 onwards enable you to specify how many times the switch will retry sending a SYN ACK for a TCP connection for which it has received a SYN but not an ACK. Such connections are called half-open TCP Connections. This enhancement allows you to influence how long half-open TCP connections take to time out.

To set how many times to retry sending a SYN ACK for a half-open TCP connection before abandoning it, use the command:

```
awplus#configure terminal
awplus(config)#ip tcp synack-retries <0-255>
```

The default is 5 retries.

The following table shows the approximate correlation between the number of retries and the time half-open TCP connections take to time out.

Number of retries	Approximate lower bound for the timeout
0 retries	1 second
1 retry	3 seconds
2 retries	7 seconds
3 retries	15 seconds
4 retries	31 seconds
5 retries	63 seconds

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, or otherwise the device uses an IP address of 169.254.42.42.

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

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

AR-Series Firewalls are typically 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**.

What is an unconfigured device?

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

1. None of the following files exist in the root directory of /flash:
   - .config
   - .config_backup
   - .cfg files
   - User created folders
2. The device is not set up to use autoboot functionality via external media. This means the device is considered unconfigured if a USB stick or SD card is connected, unless that external media contains a file named autoboot.txt.

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 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 169.254.42.42/16
 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.

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.

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 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 Asyn-based console port only, leaving the network management interface disconnected.

If you have both Asyn and network interfaces connected, you need to be cautious for a few seconds after start-up about entering configuration commands via the Asyn 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

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, and identify that string in the CLI help 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).

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

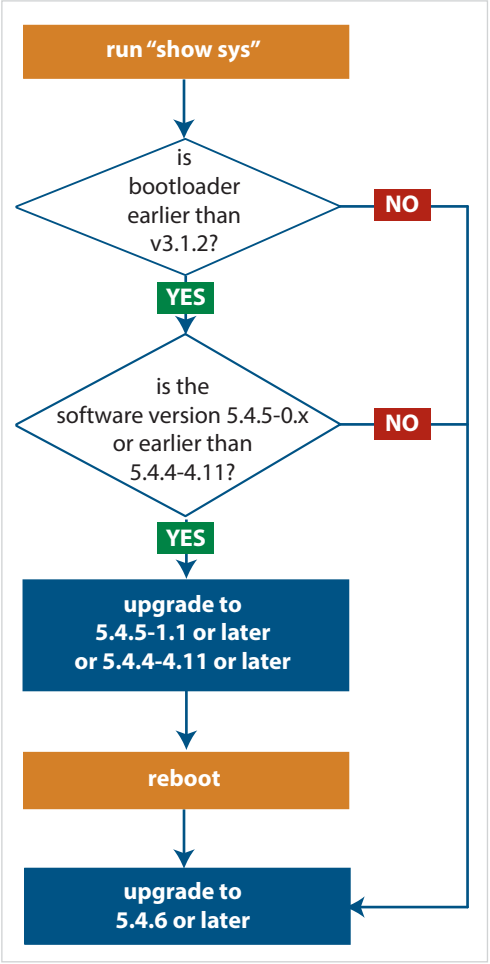
Applies to DC2552XS/L3 switches

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.

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.



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.

Licensing

Applies to SBx908 and SBx8100 Series switches

From software version 5.4.4-0.4 onwards, AlliedWare Plus software releases need to be licensed for SBx908 and SBx8100 switches.

If you are upgrading to 5.4.7-x.x on your SBx908 or SBx8100 switch, please ensure you have a 5.4.7 license on your 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 Switch" on page 51 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 53.

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 5.4.7-1.1 from any previous software version.

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 5.4.7-1.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 5.4.7-1.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 5.4.7-1.x and:

- 5.4.7-0.x
- 5.4.6-2.x, and
- 5.4.6-1.2 and all later 5.4.6-1.x versions.

It is not supported between 5.4.7-0.1 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 5.4.7-1.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 v5.4.7-1.x, and you connect a switch running 5.4.6-1.1 or earlier to the stack, then the v5.4.7-1.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 v5.4.7-1.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 v5.4.7-1.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 v5.4.7-1.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 44 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 v5.4.7-1.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 v5.4.7-1.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 v5.4.7-1.x, and you add a CFC running 5.4.6-1.1 or earlier to the chassis, then the v5.4.7-1.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.

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.

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 5.4.7-1.x, then they **all** must. Otherwise, the "show atmf area nodes" command and the "show atmf area guests" command will not function, and Vista Manager will all 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 5.4.7-1.x, then they all must
- 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)
- If your AMF Master node is running 5.4.7-1.x, then member nodes can run 5.4.7-0.x.

If using none of the above

If none of the above apply, then nodes running version 5.4.7-1.x are compatible with nodes running:

- 5.4.7-0.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.

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 5.4.7-1.1, so you can simply copy and paste that command into the CLI if you wish to verify the file x930-5.4.7-1.1.rel:

```
crypto verify x930-5.4.7-1.1.rel 348e598b051689f35504fd4043bd67a74fb4e65790891a8b3de3f611345eff8a
```

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 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:

```
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              : EPSR-MASTER, IPv6Basic, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, 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
```

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                   : 5.4.7-1
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 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Software Version on an SBx908 Switch" on page 51 and
- "Licensing this Software Version on an SBx8100 Series Switch Control Card" on page 53.

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 FS980-5.4.7-1.5.rel`
GS900MX/MPX series	`awplus(config)# boot system GS900-5.4.7-1.5.rel`
GS970M series	`awplus(config)# boot system GS970-5.4.7-1.5.rel`
XS900MX series	`awplus(config)# boot system XS900-5.4.7-1.5.rel`
x230 series	`awplus(config)# boot system x230-5.4.7-1.5.rel`
IE200 series	`awplus(config)# boot system IE200-5.4.7-1.5.rel`
x310 series	`awplus(config)# boot system x310-5.4.7-1.5.rel`
IE300 series	`awplus(config)# boot system IE300-5.4.7-1.6.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.7-1.5.rel`
x510 series	`awplus(config)# boot system x510-5.4.7-1.5.rel`
x550 series	`awplus(config)# boot system x550-5.4.7-1.5.rel`

Product	Command
IE510-28GSX	`awplus(config)# boot system IE510-5.4.7-1.5.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.7-1.5.rel`
x550 series	`awplus(config)# boot system x550-5.4.7-1.5.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.7-1.5.rel`
DC2552XS/L3	`awplus(config)# boot system DC2500-5.4.7-1.5.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.7-1.5.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.7-1.5.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.4.7-1.5.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.7-1.5.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.7-1.5.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.7-1.5.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.