Release Note for AlliedWare Plus Software Version 5.4.8-0.x

AlliedWare Plus OPERATING SYSTEM

» SBx8100 Series » SBx908 GEN2 » SBx908 » DC2552XS/L3
» x930 Series » x550 Series » x510 Series » IX5 Series
» x310 Series » x230 Series » x220-28GS
» IE500 Series » IE300 Series » IE200 Series
» XS900MX Series » GS970MX Series » GS900MX/MPX Series
» FS980M Series » AMF Cloud
» AR4050S » AR3050S » AR2050V » AR2010V

» 5.4.8-0.2 » 5.4.8-0.3 » 5.4.8-0.4 » 5.4.8-0.5 » 5.4.8-0.7 » 5.4.8-0.8 » 5.4.8-0.9 » 5.4.8-0.10

Acknowledgments

Getting the most from this Release Note

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

Content

What's New in Version 5.4.8-0.10 3

Introduction 3

Issues Resolved in Version 5.4.8-0.10 6

What's New in Version 5.4.8-0.9 7

Introduction 7

Issues Resolved in Version 5.4.8-0.9 10

What's New in Version 5.4.8-0.8 11

Introduction 11

Issues Resolved in Version 5.4.8-0.8 14

What's New in Version 5.4.8-0.7 15

Introduction 15

Issues Resolved in Version 5.4.8-0.7 18

What's New in Version 5.4.8-0.5 25

Introduction 25

Enhancement in Version 5.4.8-0.5 28

What's New in Version 5.4.8-0.4 29

Introduction 29

Support for x230L switches 31

Issues Resolved in Version 5.4.8-0.4 32

What's New in Version 5.4.8-0.3 33

Introduction 33

New Enhancement 36

Issues Resolved in Version 5.4.8-0.3 37

What's New in Version 5.4.8-0.2 40

Introduction 40

New Products 43

New web-based GUI for switches 44

New Features and Enhancements 45

Important Considerations Before Upgrading 60

Obtaining User Documentation 68

Verifying the Release File for x930 Series Switches 68

Licensing this Version on an SBx908 or SBx908 GEN2 Switch 70

Licensing this Version on an SBx8100 Series Switch Control Card 72

Installing this Software Version 74

Accessing the web-based device GUI..... 76

What's New in Version 5.4.8-0.10

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
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 5.4.8-0.10. 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 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2018	GS900-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	08/2018	FS980-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2018	GS970-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
XS916MXT XS916MXS	XS900MX	08/2018	XS900-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2018	IE200-5.4.8-0.10.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	08/2018	IE300-5.4.8-0.10.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	08/2018	IE510-5.4.8-0.10.rel	IE510-gui_547_01.jar
x220-28GS	x220	08/2018	x220-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230	08/2018	x230-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2018	x310-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
IX5-28GPX	IX5	08/2018	IX5-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
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	08/2018	x510-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	082018	x550-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2018	x930-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
DC2552XS/L3		08/2018	dc2500-5.4.8-0.10.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	08/2018	SBx908NG-5.4.8-0.10.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	08/2018	SBx908-5.4.8-0.10.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	08/2018	SBx81CFC400-5.4.8-0.10.rel SBx81CFC960-5.4.8-0.10.rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	08/2018	AR4050S-5.4.8-0.10.rel AR3050S-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	08/2018	AR2050V-5.4.8-0.10.rel AR2010V-5.4.8-0.10.rel	See "Accessing the web-based device GUI" on page 76

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules

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

Issues Resolved in Version 5.4.8-0.10

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-64237	**ICMP**	Previously, an incorrect source IP address was used in ICMP error packets when these packets were triggered by a VLAN interface that was a member of a VRF domain. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	–	Y	Y	Y	–

What's New in Version 5.4.8-0.9

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
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 5.4.8-0.9. 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 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2018	GS900-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	08/2018	FS980-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2018	GS970-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
XS916MXT XS916MXS	XS900MX	08/2018	XS900-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2018	IE200-5.4.8-0.9.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	08/2018	IE300-5.4.8-0.9.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	08/2018	IE510-5.4.8-0.9.rel	IE510-gui_547_01.jar
x220-28GS	x220	08/2018	x220-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230	08/2018	x230-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2018	x310-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
IX5-28GPX	IX5	08/2018	IX5-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
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	08/2018	x510-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	082018	x550-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2018	x930-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
DC2552XS/L3		08/2018	dc2500-5.4.8-0.9.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	08/2018	SBx908NG-5.4.8-0.9.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	08/2018	SBx908-5.4.8-0.9.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	08/2018	SBx81CFC400-5.4.8-0.9.rel SBx81CFC960-5.4.8-0.9.rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	08/2018	AR4050S-5.4.8-0.9.rel AR3050S-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	08/2018	AR2050V-5.4.8-0.9.rel AR2010V-5.4.8-0.9.rel	See "Accessing the web-based device GUI" on page 76

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules

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

Issues Resolved in Version 5.4.8-0.9

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61201	**Exception Handling**	Previously, a device may restart due to incorrect handling of a received packet. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	–

What's New in Version 5.4.8-0.8

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
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 5.4.8-0.8. 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 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2018	GS900-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	08/2018	FS980-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2018	GS970-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
XS916MXT XS916MXS	XS900MX	08/2018	XS900-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2018	IE200-5.4.8-0.8.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	08/2018	IE300-5.4.8-0.8.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	08/2018	IE510-5.4.8-0.8.rel	IE510-gui_547_01.jar
x220-28GS	x220	08/2018	x220-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230	08/2018	x230-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2018	x310-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
IX5-28GPX	IX5	08/2018	IX5-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
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	08/2018	x510-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	082018	x550-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2018	x930-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
DC2552XS/L3		08/2018	dc2500-5.4.8-0.8.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	08/2018	SBx908NG-5.4.8-0.8.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	08/2018	SBx908-5.4.8-0.8.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	08/2018	SBx81CFC400-5.4.8-0.8.rel SBx81CFC960-5.4.8-0.8.rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	08/2018	AR4050S-5.4.8-0.8.rel AR3050S-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	08/2018	AR2050V-5.4.8-0.8.rel AR2010V-5.4.8-0.8.rel	See "Accessing the web-based device GUI" on page 76

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules

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

Issues Resolved in Version 5.4.8-0.8

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61046	**Unicast Forwarding HW**	Previously, when a switch was configured for jumbo frames and was under a high load of traffic to the CPU, including jumbo frames, the switch might stop receiving traffic to the CPU, thereby causing ARPs to age out and other traffic interruptions to occur. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	–

What's New in Version 5.4.8-0.7

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
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 5.4.8-0.7. 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 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	08/2018	GS900-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	08/2018	FS980-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	08/2018	GS970-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
XS916MXT XS916MXS	XS900MX	08/2018	XS900-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	08/2018	IE200-5.4.8-0.7.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	08/2018	IE300-5.4.8-0.7.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	08/2018	IE510-5.4.8-0.7.rel	IE510-gui_547_01.jar
x220-28GS	x220	08/2018	x220-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230	08/2018	x230-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	08/2018	x310-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
IX5-28GPX	IX5	08/2018	IX5-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
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	08/2018	x510-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	082018	x550-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	08/2018	x930-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
DC2552XS/L3		08/2018	dc2500-5.4.8-0.7.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	08/2018	SBx908NG-5.4.8-0.7.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	08/2018	SBx908-5.4.8-0.7.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	08/2018	SBx81CFC400-5.4.8-0.7.rel SBx81CFC960-5.4.8-0.7.rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	08/2018	AR4050S-5.4.8-0.7.rel AR3050S-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	08/2018	AR2050V-5.4.8-0.7.rel AR2010V-5.4.8-0.7.rel	See "Accessing the web-based device GUI" on page 76

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules

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

Issues Resolved in Version 5.4.8-0.7

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

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59482	**AMF**	Previously, an AMF master could incorrectly display duplicate logs after a node recovery. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-59702	**AMF**	Previously, on some occasions, a stack failover could cause an AMF application proxy process to restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-60260	**AMF**	Previously, an AMF network could become unstable if an invalid hostname was used. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-59829	**AMF** **UTM**	Previously, under rare circumstances, an AMF backup could fail, in particular if the backup was carried out concurrently with a UTM resource update. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-59852	**API**	With this software update, support is added to the API handler to allow the internal redirects of API path for platform sensors. 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-60043	**ARP**	Previously, if the number of learnt ARP entries reach a switch hardware limit, the ARP cache would not be cleared even after it was aged. As a result, no new ARP entries could be added. 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	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59646	**AWC**	Previously, on the MWS-1750 and MWS-600 wireless devices, the power-channel calculation could fail to calculate correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-59817	**AWC**	Previously, a "space" was not allowed in the description for the configuration of a wireless-network. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-59720	**DPI** **IPSec** **L2TP**	Previously, the default tunnel MTU value was incorrect if DPI was enabled, causing unnecessary data loss for large packets. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-60318	**EPSR** **VCStack**	Previously, when an EPSR ring was configured on dynamic aggregators, the ring ports would not be correctly configured after a stack failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	–	–	Y	–	–	Y	Y	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	–
CR-59725	**IGMP**	Previously, NLB traffic would not traverse through a LAG interface. This issue has been resolved.	–	Y	–	–	–	–	Y	–	Y	Y	Y	–	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-59843	**IGMP**	Previously, the device could stop sending PIM join message after a multicast server restart. 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-59919	**IGMP**	Previously, an IGMP snooping device might fail to respond to a Group Specific Query. This could lead to multicast data failing to forward downstream of that device until the next General Query was received by the device. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56625	**IGMP**	Previously, IGMP-Proxy service might send group reports in reply to group (source-group) specific query sent by an upstream IGMP router even though all IGMP-proxy downstream members of the groups had already left. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	–	Y	Y	Y	Y	Y	–	–	Y	Y	–
CR-59926	**IPsec**	Previously, it was possible for an AlliedWare Plus router to restart unexpectedly if an IPsec protected tunnel interface went down, for example by being manually disabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-60068	**IPsec**	With this software update, the tunnel IPsec traffic selectors can now be used in strict pairs with the **`tunnel selector paired`** command.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-60296	**LACP**	Previously, on x550 and x930 series switches, when the 40G ports were used as network ports, the port link could flap once (link down and up) when a stack member rejoined. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–	–	–	–	–
CR-60181	**LACP Logging**	Previously, if a packet with destination MAC of 0180.c200.0003 and 'ethertype' of 88CC (LLDP) was sent to the device, it could be incorrectly classified and an error was logged. 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-59765	**Logging**	Previously, an unnecessary amount of memory consumption could occur if the logging configuration was repeatedly changed. 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-60311	**Logging**	Previously, it was possible for the benign log message "AgentX: requested pdu : 1" to appear in the log during startup. However, as this log is not useful in a networking sense, it has been removed. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56351	**MSS Clamping**	Previously, an incorrect MSS value applied to TCP flows, when **ip tcp adjust-mss** was used on an interface could cause unnecessary fragmentation. resulting in unnecessary latency. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-59915	**NTP Logging**	Previously, it was possible for SYSLOG and NTP to continuously restart every minute after a clock change. 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-60054	**OpenFlow**	With this software update, OpenFlow traffic can be hardware switched.	Y	Y	Y	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	–
CR-60327	**OSPF**	Previously, when receiving updates for external LSAs for networks with overlapping subnets, the OSPF might sometimes fail to install routes for all of the networks in its routing table. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-60308	**PIMv6**	Previously, it was possible for a switch to restart unexpectedly when trying to configure IPv6 PIM interfaces. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-59825	**Pluggables**	With this software update, the AT-QSFPSR optical transceiver is now supported on the x550, x930, and SBx908GEN2 variant switches.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	Y	–	–	–	–
CR-60211	**Policy-based Routing**	Previously, when an ARP entry of a policy-based routing next hop was removed, the entry would not be updated correctly. This could lead to no ARP request and no ARP entry being added for subsequent traffic for the policy-map entry. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–
CR-59885	**Port Authentication**	Previously, web authentication could fail after an ARP entry was refreshed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60165	**Port Authentication**	Previously, it was possible for the command: **`clear mac address-table dynamic`** to cause the authentication process to restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-60049	**SNMP**	Previously, when a supplicant was authorized by MAC-auth, sometimes BRIDGE-MIB and Q-BRIDGE-MIB returned the port number of the supplicant in the FDB table as "0" instead of the actual switch port that the supplicant was connected to. 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-60204	**SNMP**	Previously, an SNMP walk would not return any value on a shutdown port that had the port authentication 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-60272	**SNMP**	Previously, ***snmpbulkwalk*** on the "dot1qTp" MIB table would incorrectly return an error message. 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-60291	**SNMP**	Previously, SNMP "SysObjectID" on GS900 variant switches could return wrong values.	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-59876	**SNMP** **AMF**	Previously, the execution of an SNMP walk/get/get-next command that traversed the atAtmfNodeTable could potentially cause a switch to restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59924	**Software Licensing**	Previously, if an AMF backup was restored onto the same physical device that it was taken from through AMF reincarnation or manual AMF recovery, then the device's external licenses or subscription licenses could be incorrectly erased 28 days later. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-58928	**SSL**	This software update addressed the two security vulnerabilities, reference number CVE-2017-3737 and CVE-2017-3738, listed under Common Vulnerabilities and Exposures (CVE). This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-59991	**Switch**	Previously, if there was an unexpected system reboot, traffic could be incorrectly routed via the CPU rather than being hardware switched. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	–
CR-59757	**System**	Previously, under extremely rare circumstances, the device could restart unexpectedly after executing the **show memory** command. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-60157	**System**	Previously, if a configuration change was saved on a device and then the device was powered off within a very short period of time, it was possible for the configuration file to be deleted or not updated. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-59927	**VCStack**	Previously, under rare circumstances, a stack member leaving a stack could cause a switch to restart unexpectedly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60046	**VCStack**	Previously, under extremely rare circumstances, a stack member leaving a stack could cause the stack to stop working. The issue was only seen on a stack of 3 or more switches. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–	–
CR-59993	**VCStack**	Previously, it was possible for stack members to become stuck in the initialisation state after joining the stack. This issue has been resolved.	–	Y	–	Y	–	Y	–	–	Y	–	Y	Y	Y	–	Y	–	–	–	Y	–	–	–	–
CR-60343	**VCStack**	Previously, members of a VCStack could sometimes separate if one of the stack cables was removed. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–
CR-59976	**VRRP**	Previously, directed broadcast packets received via a non-VRRP interface would not be forwarded to the VRRP interface - even if the interface was configured to allow directed broadcasts. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–

What's New in Version 5.4.8-0.5

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
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 5.4.8-0.5. 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 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2018	GS900-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	06/2018	FS980-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2018	GS970-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
XS916MXT XS916MXS	XS900MX	06/2018	XS900-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2018	IE200-5.4.8-0.5.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	06/2018	IE300-5.4.8-0.5.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	06/2018	IE510-5.4.8-0.5.rel	IE510-gui_547_01.jar
x220-28GS	x220	06/2018	x220-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230	06/2018	x230-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	06/2018	x310-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
IX5-28GPX	IX5	06/2018	IX5-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
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	06/2018	x510-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2018	x550-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	06/2018	x930-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
DC2552XS/L3		06/2018	dc2500-5.4.8-0.5.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	06/2018	SBx908NG-5.4.8-0.5.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	06/2018	SBx908-5.4.8-0.5.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	06/2018	SBx81CFC400-5.4.8-0.5.rel SBx81CFC960-5.4.8-0.5.rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	06/2018	AR4050S-5.4.8-0.5.rel AR3050S-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	06/2018	AR2050V-5.4.8-0.5.rel AR2010V-5.4.8-0.5.rel	See "Accessing the web-based device GUI" on page 76

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules

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

Enhancement in Version 5.4.8-0.5

This AlliedWare Plus maintenance version includes the following enhancement:

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-2113	**PIM**	Enhancement: All platforms With this software update you can statically configure a RP (Rendezvous-Point) address for a given multicast group address prefix. If the platform supports multicast for VRFs then specifying a VRF name will take effect on that VRF and not specifying a VRF will apply it for the global VRF. **The command is:** ip pim [vrf <*vrf-name*>] rp-address <*ip-address*> group-list <ip-address> <subnet> [override] no ip pim [vrf <vrf-name>] rp-address <ip-address> group-list <ip-address> <subnet> ■ **rp-address** - the static RP address to be used as the Rendezvous Point for the specified multicast group ■ **group-list** - prefix that specifies the multicast groups whose RP is specified ■ **override** - if specified, the static RP configuration will override matching dynamic RPs Note: a unique RP address may only be specified once as a static RP. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

What's New in Version 5.4.8-0.4

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
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 5.4.8-0.4. Software file details for this version are listed in Table 1 below.

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

Caution: Software version 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2018	GS900-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	06/2018	FS980-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2018	GS970-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
XS916MXT XS916MXS	XS900MX	06/2018	XS900-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2018	IE200-5.4.8-0.4.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	06/2018	IE300-5.4.8-0.4.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	06/2018	IE510-5.4.8-0.4.rel	IE510-gui_547_01.jar
x220-28GS	x220	06/2018	x220-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230	06/2018	x230-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	06/2018	x310-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
IX5-28GPX	IX5	06/2018	IX5-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
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	06/2018	x510-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2018	x550-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	06/2018	x930-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
DC2552XS/L3		06/2018	dc2500-5.4.8-0.4.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	06/2018	SBx908NG-5.4.8-0.4.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	06/2018	SBx908-5.4.8-0.4.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	06/2018	SBx81CFC400-5.4.8-0.4.rel SBx81CFC960-5.4.8-0.4.rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	06/2018	AR4050S-5.4.8-0.4.rel AR3050S-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	06/2018	AR2050V-5.4.8-0.4.rel AR2010V-5.4.8-0.4.rel	See "Accessing the web-based device GUI" on page 76

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules

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

Support for x230L switches

Enterprise Gigabit Edge Switches

The popular x230 Series of Layer 3 Lite Gigabit edge switches, have two new fan-less models to support silent operation for deployment in work areas, and low running costs.

- x230L-17GT with 16 x 10/100/1000T ports and 1 x 100/1000 SFP uplinks.
- x230L-26GT with 24 x 10/100/1000T ports and 2 x 100/1000 SFP uplinks.

The x230L models are supported from AlliedWare Plus version 5.4.8-0.4 onwards.

Issues Resolved in Version 5.4.8-0.4

This AlliedWare Plus maintenance version includes the following resolved issue:

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59976	**VRRP**	Previously, directed broadcast packets on a non-VRRP interface were not being forwarded to the VRRP interface. This issue has been resolved.	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–

What's New in Version 5.4.8-0.3

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
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 5.4.8-0.3. Software file details for this version are listed in Table 1 below.

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

Caution: Software version 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	06/2018	GS900-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	06/2018	FS980-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	06/2018	GS970-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
XS916MXT XS916MXS	XS900MX	06/2018	XS900-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2018	IE200-5.4.8-0.3.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	06/2018	IE300-5.4.8-0.3.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	06/2018	IE510-5.4.8-0.3.rel	IE510-gui_547_01.jar
x220-28GS	x220	06/2018	x220-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT	x230	06/2018	x230-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	06/2018	x310-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
IX5-28GPX	IX5	06/2018	IX5-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
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	06/2018	x510-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	06/2018	x550-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76

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

Models	Family	Date	Software File	GUI File
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	06/2018	x930-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
DC2552XS/L3		06/2018	dc2500-5.4.8-0.3.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	06/2018	SBx908NG-5.4.8-0.3.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	06/2018	SBx908-5.4.8-0.3.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	06/2018	SBx81CFC400-5.4.8-0.3.rel SBx81CFC960-5.4.8-0.3rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	06/2018	AR4050S-5.4.8-0.3.rel AR3050S-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	06/2018	AR2050V-5.4.8-0.3.rel AR2010V-5.4.8-0.3.rel	See "Accessing the web-based device GUI" on page 76

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules

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

New Enhancement

This section describes the new enhancement in 5.4.8-0.3:

CR	Module	Description
ER-2059	**OpenFlow**	For: x230 Series With this software update, improvements have been made for OpenFlow's utilization of hardware ACL tables.

Issues Resolved in Version 5.4.8-0.3

This AlliedWare Plus maintenance version includes the resolved issue described in the following table, ordered by feature:

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59723	**ACL**	Previously, deleting a static-channel group that had ACLs attached would not remove the ACLs entries. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-59705	**ACL** **SW QoS** **VCStack**	Previously, the ACL action "send-to-vlan-port" for a link aggregation port would not work after failover of a stack backup member. This issue has been resolved.	–	–	Y	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-59687	**ACL** **VCStack**	Previously, ACL counters on a static aggregator would not work after a stack failover, if another ACL had previously been configured on the aggregator. This issue has been resolved.	–	–	Y	–	–	–	Y	–	–	Y	Y	Y	Y	–	Y	–	–	Y	–	–	–	–	–
CR-59755	**ACL** **VCStack**	Previously, if multiple backup members joined a Stack late, then the ACL configuration could be incorrectly applied across the Stack. This issue has been resolved.	–	–	Y	–	–	–	Y	–	–	Y	Y	Y	Y	–	Y	–	–	–	Y	–	–	–	–
CR-59340	**AMF**	Previously, under certain circumstances, if a stack failover occurred, the AMF Application Proxy IP-Filter blocking could sometimes operate incorrectly. 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	–	–	–	–
CR-59471	**AMF**	Previously, if an AMF master failed and was recovered using an SD card, the AMF recovery was successful but the licensing was not transferred correctly on to the reincarnated Master. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	Y	Y	Y	Y	–	–	Y	Y
CR-59773	**CPU Packet Processing**	Previously, under rare circumstances, it was possible for a corrupted packet to get stuck in a loop on the backplane of the CFC980. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-59747	**DPI**	Previously, a Denial of Service attack from an untrusted network was possible even if DPI learning was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58871	**DPI** **Malware Protection**	Previously, when using the AR Series Firewall with any of IP Reputation, IPS, Malware Protection or URL Filtering configured, a memory leak could occur if any traffic used the HTTP "CONNECT" method. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-59715	**Findme**	Previously, on an AlliedWarePlus router, enabling "findme" could cause the device to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-59750	**Firewall**	Previously, a router could fail to boot up if an excessive number of firewall rules (>500) was pre-configured. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-59651	**HW QoS**	Previously, policy-map configurations on aggregators were not being synchronized on late joining stack members. This issue has been resolved.	–	–	Y	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-58650	**IGMP**	Previously, if an IGMP interface had source-timeout configured and there was a 'client leave and rejoin to a group' within the specified source timeout, the data could stop flowing to that group after the next group timeout. 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-59781	**IGMP**	Previously, if an IGMP snooping system had source-timeout configured on an interface and that interface received unregistered multicast data, the system could stop responding to IGMP Queries. 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-59708	**IPSec** **GRE**	Previously, the MTU for a GREv6 and IPsec tunnel was incorrect. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-59694	**LACP**	Previously, it was possible for invalid packets to consume received buffers on a CFC960, preventing CPU traffic reception. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59689	**LACP** **VCStack**	Previously, when a SBx908Gen2 backup member with 6 to 8 XEMs joined the stack, if the ports on the joining stack members were not enabled before the configuration was read, it could allow un-configured ports to link up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-59710	**Pluggable Transceivers**	With this software update, the Finisar FTL4S1QE1C 40G SWDM4 QSFP+ transceiver module is now supported. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	–	–	Y	Y	Y	–	–	–	–
CR-59642	**Port Configuration**	Previously, if there was speed change from 10FULL to 100MFULL fixed between an x510 and x930 device the speed change was not operating correctly. (Force Auto-MDIX issue) This issue has been resolved.	–	–	–	–	–	–	Y	–	Y	–	Y	Y	–	Y	Y	–	–	–	–	–	–	–	–
CR-59672	**Port Security**	Previously, the port learning mode was not set for MAC station movements. This issue has been resolved.	–	–	Y	–	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-59722	**RADIUS**	Previously, deleting the "radius proxy group" from the configuration could result in the device to restart unexpectedly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-59685	**SW QoS** **VCStack**	Previously, when multiple backup stack members joined a stack at slightly staggered times (such as in a rolling reboot), some members could fail to synchronize. This issue has been resolved.	–	–	Y	–	–	–	Y	–	–	Y	Y	Y	Y	Y	–	–	–	–	Y	–	–	–	–
CR-59796	**System**	Previously, when using the **`arp-mac-disparity`** functionality, it was possible for the HSL process to restart unexpectedly. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-59697	**VCStack** **ACL**	Previously, when using the command **`copy-to-mirror`** with VACL, packets were replicated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-58994	**VRRP** **ICMP**	Previously, ICMP redirect was not working with VRRP. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

What's New in Version 5.4.8-0.2

For:

SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
DC2552XS/L3
x930 Series
x550 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x220-28GS
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-0.2.

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

Caution: Software version 5.4.8-x.x requires a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. If you are using any of these switches, make sure that each switch has a 5.4.8 license certificate before you upgrade.

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

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	04/2018	GS900-5.4.8-0.2.rel	GS900-gui_547_02.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	04/2018	FS980-5.4.8-0.2.rel	FS980-gui_547_02.jar
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2018	GS970-5.4.8-0.2.rel	GS970-gui_547_03.jar
XS916MXT XS916MXS	XS900MX	04/2018	XS900-5.4.8-0.2.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	04/2018	IE200-5.4.8-0.2.rel	IE200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	04/2018	IE300-5.4.8-0.2.rel	IE300-gui_547_02.jar
IE510-28GSX-80	IE500	04/2018	IE510-5.4.8-0.2.rel	IE510-gui_547_01.jar
x220-28GS	x220	04/2018	x220-5.4.8-0.2.rel	n/a
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT	x230	04/2018	x230-5.4.8-0.2.rel	See "Accessing the web-based device GUI" on page 76
x310-26FT x310-50FT x310-26FP x310-50FP	x310	04/2018	x310-5.4.8-0.2.rel	x310-gui_547_02.jar
IX5-28GPX	IX5	04/2018	IX5-5.4.8-0.2.rel	IX5-gui_547_02.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	04/2018	x510-5.4.8-0.2.rel	See "Accessing the web-based device GUI" on page 76
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2018	x550-5.4.8-0.2.rel	x550-gui_547_02.jar

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

Models	Family	Date	Software File	GUI File
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	04/2018	x930-5.4.8-0.2.rel	x930-gui_547_01.jar
DC2552XS/L3		04/2018	dc2500-5.4.8-0.2.rel	dc2500-gui_547_01.jar
SBx908 GEN2	SBx908 GEN2	04/2018	SBx908NG-5.4.8-0.2.rel	SBx908NG-gui_547_02.jar
SBx908 (see Table 2)	SBx908	04/2018	SBx908-5.4.8-0.2.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	04/2018	SBx81CFC400-5.4.8-0.2.rel SBx81CFC960-5.4.8-0.2.rel	SBx81CFC400-gui_547_03.jar SBx81CFC960-gui_547_04.jar
AR4050S AR3050S	AR-series UTM firewalls	04/2018	AR4050S-5.4.8-0.2.rel AR3050S-5.4.8-0.2.rel	See "Accessing the web-based device GUI" on page 76
AR2050V AR2010V	AR-series VPN firewalls	04/2018	AR2050V-5.4.8-0.2.rel AR2010V-5.4.8-0.2.rel	See "Accessing the web-based device GUI" on page 76
AMF Cloud		04/2018	vaa-5.4.8-0.2.iso (VAA OS) vaa-5.4.8-0.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-0.2.vhd (for Microsoft Azure)	

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-x.x (Note that this does not include the SBx908 GEN2, which uses XEM2 modules)

Product	Supported in version 5.4.8-x.x
XEM-1XP	No
XEM-2XP	Yes
XEM-2XS	Yes
XEM-2XT	Yes
XEM-12S	No
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

New Products

100Gbps XEM for SwitchBlade x908 GEN2

XEM2-1CQ

The XEM2-1CQ adds 100Gbps connectivity to the SwitchBlade x908Gen2, further expanding the bandwidth capabilities of the core chassis. It can be used for stacking locally or over distance, or high speed Ethernet back-bone links.

Rebooting the switch is required when you hotswap the XEM2-1CQ to or from a different model of XEM2. For more information about replacing the XEM2-1CQ line card, see AT-SBx908 GEN2 Advanced Layer 3+ Modular Switch Hardware Release Notes.

The XEM2-1CQ is supported from AlliedWare Plus version 5.4.8-0.2 onwards.

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

x550-18XSPQm switch

Stackable multi-gigabit intelligent Layer 3 PoE+ switch

The x550-18XSPQm switch offers eight 1G/2.5G/10G (RJ-45) copper ports, eight 1G/10G SFP+ ports and two 40G QSFP ports.

The x550-18XSPQm supports 2.5 Gigabit, making it a convenient and cost-effective way to support high-speed wireless (802.11ac or “Wave2”). Additional features include VCStack, PoE+, OpenFlow v1.3, BGP4, G.8032 Ethernet Ring Protection, and AMF master capability.

The x550-18XSPQm is supported from AlliedWare Plus version 5.4.8-0.2 onwards.

x220-28GS switch

28-port Layer 3 Managed Gigabit Switch with 100/1000X SFPs

The x220-28GS switch offers 24 100/1000M SFP network ports and 4 100/1000M SFP uplink ports.

The x220-28GS switch is a cost-effective managed Layer 3 switch. Key features include eco-friendly power saving options, IEEE 802.1x/MAC/Web authentication support, management stacking, static routing, RIP, and AMF member support.

The x220-28GS is supported from AlliedWare Plus version 5.4.8-0.2 onwards.

New web-based GUI for switches

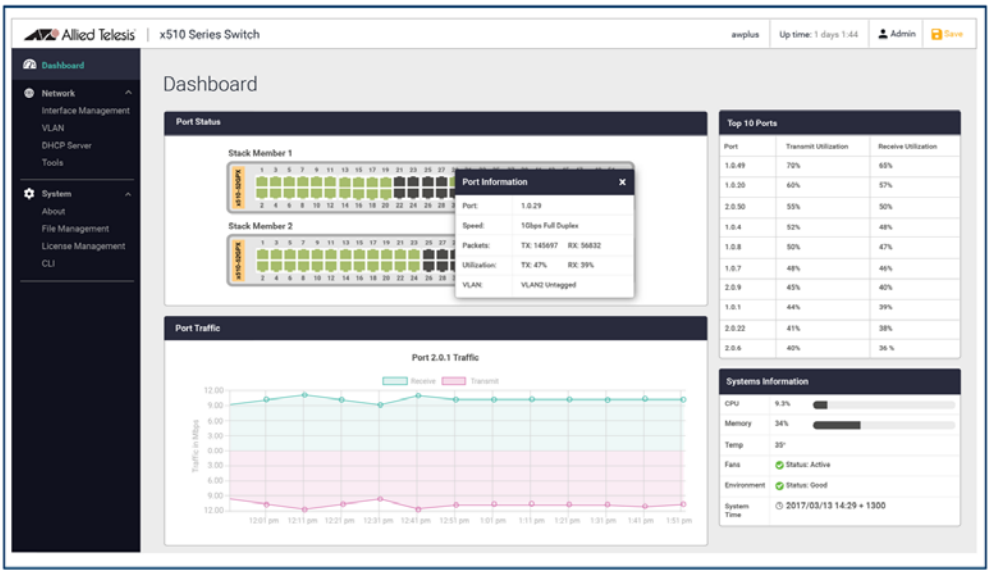
Over the next few months, Allied Telesis is introducing a new web-based graphical user interface for AlliedWare Plus switches, to replace the existing Java-based GUI.

The GUI is a convenient tool for monitoring your switch's status and performing basic management tasks.

The GUI is currently available for x230, x510 and x510L Series switches. It will be released progressively across the remaining AlliedWare Plus switches during 2018.

It requires AlliedWare Plus version 5.4.8-0.2 or later.

To obtain the new GUI, see "Accessing the web-based device GUI" on page 76.



New Features and Enhancements

This section summarizes the new features in 5.4.8-0.2 since 5.4.7-2.6:

- "Allied Telesis Autonomous Management Framework (AMF) enhancements" on page 46
- "Software defined WAN (SD-WAN)" on page 48
- "Advanced bridge filtering" on page 49
- "Dual Stack Lite (DS-Lite)" on page 50
- "Change the HTTP management port and disable HTTP or HTTPS management" on page 50
- "RADIUS proxy server" on page 51
- "VCStack enhancements on SBx908 GEN2 switches" on page 51
- "Over-temperature shutdown on SBx908 GEN2 switches" on page 52
- "MAC authentication enhancement" on page 52
- "Active Fiber Monitoring enhancements" on page 53
- "Route summarization for RIPv2" on page 53
- "OpenFlow connection interruption enhancement" on page 54
- "G.8032 and Connectivity Fault Management (CFM) on SBx81CFC960" on page 54
- "Precision Time Protocol (PTP) and Transparent Clock on x550 and x230 Series switches" on page 55
- "ACL scaling enhancements" on page 55
- "256 BGP routes on IE300 Series switches" on page 55
- "The OpenFlow protocol on SBx908 GEN2" on page 56
- "VLAN ID translation on SBx908 GEN2 and x930 Series switches" on page 56
- "Enhanced show command output includes IPv6 address states" on page 57
- "Displaying files on all stack members" on page 57
- "Inclusion of stackport entry in the configuration file on stack members" on page 58
- ""no terminal monitor" command" on page 58
- "Displaying kernel crash files" on page 58
- "Increased multicast limit on IE300 Series switches" on page 58
- "10Gbps support available in the base license on x510L Series switches" on page 59

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 68.

Allied Telesis Autonomous Management Framework (AMF) enhancements

AMF Cloud on Microsoft Hyper-V

From 5.4.8-0.2 onwards, AMF Cloud virtual AMF appliances are supported on the following Microsoft Hyper-V hypervisors:

- Windows 10
- Windows Server 2012 R2
- Windows Server 2016

The virtual AMF appliance has the following requirements:

- CPU: 2 vCPUs or more depending on AMF network size; maximum of 64 vCPUs
- Memory: 1024MB or more, depending on AMF network size
- Storage: One virtual disk, sized between 8GB and 2TB.
- NIC: Maximum of 8 interfaces.

The following table lists the memory and CPU requirements for different sized AMF networks.

AT MF r ec o very ma	ATM	A TMF r
VAA with up to 120 nodes	2	1GB
VAA with up to 300 nodes	2	2GB
Multi-tenant VAA with up to 1200 nodes, 300 virtual-links and 20 containers	2	4GB
Multi-tenant VAA with up to 1200 nodes, 1200 virtual-links and 60 containers	4	8GB
Multi-tenant VAA with up to 10000 nodes, 2000 virtual-links and 60 containers	8	8GB
Multi-tenant VAA with up to 10000 nodes, 10000 virtual-links and 60 containers	16	8GB
Multi-tenant VAA with up to 18000 nodes, 18000 virtual-links and 60 containers	24	16GB
Multi-tenant VAA with up to 18000 nodes, 18000 virtual-links and 120 containers	24	32GB

New “clear atmf recovery-file” command

From version 5.4.8-0.2, you can use the **clear atmf recovery-file** command to delete all of a node’s recovery files. It deletes the recovery files stored on:

- the local node,
- neighbor nodes, and
- external media (USB or SD card).

You can use the **show atmf recovery-file** command to see the status of a node’s recovery files and the dates they were created.

If AlliedWare Plus detects that a node contains a special link then the following message is displayed:

```
node1#clear atmf recovery-file
% Warning: ATMF recovery files have been removed.
ATMF recovery may fail. Please save running-configuration.
```

Note: This command deletes all of a node's recovery files. If a node still has a special link you must save the node's running configuration after running the **clear** command. Saving creates new recovery files on the node's neighbors and on any attached external media.

For more information see the "Managing AMF recovery files" section of the AMF Feature Overview and Configuration Guide.

Subscription license recovery enhancements

Subscription licenses are keyed to the serial number of a device. From 5.4.8-0.2 onwards, if you replace a device, then AMF recovery automatically transfers these licenses to the replacement device.

AlliedWare Plus grants these subscription licenses a 28-day grace period. During this grace period, subscription features operate as normal. This gives you time to register the licenses to the new device's serial number.

For this feature to work:

- your AMF master/controller must be running 5.4.8-0.2 or newer
- the replaced (failed) device must have been running 5.4.8-0.2 or newer
- AMF must have backed up the replaced device, either automatically or manually, while it was running 5.4.8-0.2 or newer.

Recovery progress indicator

Now available on AR4050S, AR3050S, AR2050V and AR2010V

Already available on Allied Telesis switches (except for the SBx8100)

From 5.4.8-0.2 onwards, AlliedWare Plus adds a recovery progress indicator to the AR-Series UTM firewalls and VPN routers.

This is a visual feature that uses front-panel LEDs to display the recovery status during automatic recovery. This feature uses two distinct flash patterns to indicate the following states:

. onf i gur at i on	. onfigurati on Gi dew .
. onf i gurati on Guidew	. onf igurati on Gui dewand utomatic node
. onf i gurati on Gui	. ofi gurati on Gui dewand utomati c node r ecover y,

For more information on automatic node recovery, see the AMF Feature Overview and Configuration Guide.

Support for 18,000 nodes

Available on all AlliedWare Plus devices

From 5.4.8-0.2 onwards, AMF Cloud supports up 18,000 nodes with the AMF controller and multi-tenanted masters on a Virtual AMF Appliance (VAA). This VAA may be hosted on Amazon Web Service (AWS), Microsoft Azure, or a customer's private server.

The following table lists the system requirements for an AMF network with 18,000 nodes.

ov er red undant W	ov er	o v e r r	ov er r e	ov er
o ver redundant WAN inter faces and VPN l i rk ov er r edundant WAN i rter f aces and VPN l	ov	ov e	c4.4xlarge	e60
e 60 6znd i gdant WAN inter faces and VPN l i rk e60 6znd i gdant WAN i rter f aces and VPN l	e6	e60 6	e60 6zn ct i g	e60
e 60 6znd i gdant WAN inter faces and VPN l i rk e60 6znd i gdant WAN i rter f aces and VPN l i	e6	e60 6	e60 6zn ct i g	e60

Bandwidth requirements

AMF networks that have a large number of virtual-links terminating on the multi-tenant masters use significant amounts of bandwidth while the network is forming. Once the network has reached a steady state the bandwidth usage will drop off to <2% of peak.

To avoid link congestion, and maintain stability of the AMF network, it is important that the available bandwidth is adequate for the size of the AMF network.

Increasing the number of AMF areas while decreasing the number of AMF nodes per area significantly decreases the bandwidth required for a given number of nodes. The following table gives minimum bandwidth requirements for 150 and 300 node areas.

e60 6zn d i gda n t e60 6z n ct i gda n	e60 6z n ct i gda n t WAN int e e60 6z n ct i gda n t WA	e60 6z n ct i gda n t WAN int e e60 6z n ct i gda n t WA
10,000	800 Mbps	500 Mbps
18,000	1000 Mbps	600 Mbps

Software defined WAN (SD-WAN)

Available on AR2010V, AR2050V, AR3050S, and AR4050S

SD-WAN is a series of features working together to provide various solutions that meet modern business intent and reduce costs. Modern applications like Voice over IP (VoIP) calling, videoconferencing, streaming media, and virtual applications and desktops need low latency.

Bandwidth requirements are also increasing, especially for applications featuring high-definition video. Expanding WAN capability can be expensive, and dealing with network management and troubleshooting can be difficult. SD-WAN lets service providers and enterprises use existing physical customer-premises equipment (CPE). This lets you create fully managed multi-site networks, integrating links and optimizing application flows to the Internet and across the enterprise VPN infrastructure.

SD-WAN is a technology which increases performance and/or control of application traffic over redundant WAN interfaces and VPN links.

This first iteration of the Allied Telesis SD-WAN solution is able to make routing decisions based on the quality of redundant virtual private network (VPN) links. To do this, it uses link probing to determine path quality and perform application-aware routing to dynamically redirect performance sensitive application traffic (for example voice or video) via appropriate redundant links that meet its performance requirements. Via enhanced application based Policy Based routing (PBR) rules, it also supports Application Aware Routing of traffic via redundant WAN links.

For more information and configuration examples, see the SD-WAN Feature Overview and Configuration Guide

Advanced bridge filtering

Available on AR2010V, AR2050V, AR3050S, and AR4050S

From 5.4.8-0.2 onwards, the following advanced bridge features are available:

1. Increased number of bridge interfaces

   The maximum number of bridge interfaces (IDs) is increased from 64 to 255.

2. Flexible offset bridge filters

   Offset bridge filtering allows packet filtering on bridge interfaces based on string match at a specific offset of the Ethernet data (payload). This is useful to check certain fields of uncommon protocols such as BACnet encapsulated within Ethernet frames.

3. IPv4/6 L3/L4 protocol bridge filters

   Packet filtering on bridge interfaces by IP protocol supports finer grain filtering on IP protocol number and port numbers.

4. Ethernet protocol bridge filters

   Protocol bridge filters allow/deny Ethernet frame types (e.g. Ethernet 11, SAP, SNAP or Novell). The protocol filters examine bridged traffic before other filters configured by a “rule” command.

   The bridge filter has two phases:

   - Phase 1: limits packets by Ethernet frame type or ether-type/sap-type/snap-type. Permitted packets go to Phase 2 and denied packets are dropped.
   - Phase 2: performs a finer-detailed filtering by smac/dmac/proto, offset or IP match.

5. The command **show mac-filter** is extended to display the following information:

   - protocol-based filters
   - IP/IPv6 based filtering rules
   - offset-based filtering rules

6. Simultaneous support for PPPoE Pass-through and PPPoE Client on bridge

   By default, all Ethernet frames are Layer 2 bridged between bridge port member interfaces. This includes bridging of PPPoE sessions operating between PPPoE clients attached to a bridge interface and a PPPoE Access Concentrator attached to a different interface on the same bridge.

   This is commonly referred to PPPoE Pass-through.

With this update, the bridge itself can also be simultaneously configured as a PPPoE client, used to establish its own PPPoE sessions. If the destination MAC address of the PPPoE frame is the bridge itself, then the PPPoE frame is terminated by the PPPoE client running on the bridge. If the destination MAC address is not the bridge, the frame will pass-through.

This allows PPPoE session traffic to be simultaneously passed through (Layer 2 bridged), whilst simultaneously allowing for IP packets to be Layer 3 routed from other interfaces to the PPPoE client configured on the bridge.

For more information and a configuration example, see the Bridging Feature Overview and Configuration Guide

Dual Stack Lite (DS-Lite)

Available on AR2010V, AR2050V, AR3050S, and AR4050S

From 5.4.8-0.2 onwards, AR-Series devices support DS-Lite. DS-Lite is an IPv4 to IPv6 transition technology used by many service providers. It allows them to continue to use their existing IPv4 network infrastructure, whilst upgrading their infrastructure to IPv6.

DS-Lite allows islands of IPv4 networks (such as within a subscriber's home) to be connected to the IPv4 network via an IPv6 only access line. This line is provided by the service provider.

The IPv4 connections from the subscriber's private network are tunneled using IPv6 Network Address Translation in the service provider's domain before reaching the IPv4 network. The traffic coming back uses Network Address Translation back at the service provider before being tunneled back to the subscriber's private IPv4 network.

IPv6 connections to remote IPv6 networks are transported across the same line seamlessly.

For more information and configuration examples, see the DS-Lite Feature Overview and Configuration Guide

Change the HTTP management port and disable HTTP or HTTPS management

Available on all devices that support the web-based GUI

From 5.4.8-0.2 onwards, it is now possible to configure the HTTP port that the device uses for management via the web-based GUI. Previously, it was possible to configure the HTTPS port, but not the HTTP port. Also, it is now possible to disable either the HTTP or HTTPS port.

This enhancement is also supported in 5.4.7-2.4 onwards.

The default HTTP port used for management is 80. You may wish to change the value if port 80 needs to be used by another service at the same IP address in your network.

To change or disable the HTTP port, use the following new command:

```
awplus(config)#http port {<1-65535>|none}
```

To change or disable the HTTPS port, use the following command:

```
awplus(config)#http secure-port {<1-65535>|none}
```

Setting the port to none disables HTTP or HTTPS management.

Note that if you are using Vista Manager EX and need to change the HTTPS trusted port, you must use certificate-based authorization in Vista Manager EX. See the Vista Manager EX Installation and User Guide for instructions.

RADIUS proxy server

Available on all AlliedWare Plus devices.

From 5.4.8-0.2 onwards, it is possible to configure a RADIUS proxy server so that remote RADIUS servers can hold the user database and validate Network Access Server (NAS) RADIUS requests.

- The NAS sends a RADIUS request to the RADIUS proxy server.
- The proxy server forwards the request to the first available RADIUS server.
- The RADIUS server processes the request and sends the response back to the proxy server.
- The proxy server then forwards the response to the NAS with an accept or reject message.

There are a variety of situations where a RADIUS proxy is useful. For example, multiple RADIUS servers could be configured to each hold a different user database for a specific purpose e.g. one for authenticating switch management sessions, one for authenticating VPN connections, and one for authenticating 802.1X sessions. In this situation it is convenient to use a single IP address on all the NASs to point to the RADIUS proxy server. This server then forwards the request to the correct RADIUS server holding the relevant user database.

For more information about RADIUS proxy see our RADIUS Feature Overview and Configuration Guide.

VCStack enhancements on SBx908 GEN2 switches

VCStack, in conjunction with link aggregation, provides a network with no single point of failure and a resilient solution for high availability applications. Stacks can also be created over long distance fiber links, making SBx908 GEN2 the perfect choice for distributed environments.

For information about how to cable up SBx908 GEN2 stacks, see the VCStack Feature Overview and Configuration Guide.

Stacking over 10Gbps, 40Gbps or 100Gbps links

From 5.4.8-0.2 onwards, it is possible to stack SwitchBlade x908 GEN2 chassis together over 10Gbps, 40Gbps or 100Gbps links. Previously, only 40Gbps links could be used for stacking.

4-unit stacking

From 5.4.8-0.2 onwards, it is possible to stack up to 4 SwitchBlade x908 GEN2 chassis in a VCStack.

Over-temperature shutdown on SBx908 GEN2 switches

From 5.4.8-0.2 onwards, the SBx908 GEN2 will power off if its temperature gets too high (over 80°C).

If the switch detects that its temperature is approaching the temperature limit, it will monitor the temperature closely for a few minutes. During this time, it will log warning messages and generate SNMP traps if SNMP is configured.

If the temperature exceeds the limit, the switch will power off the power supply unit (PSU).

You can turn the switch back on by power cycling the PSU. The first time the switch boots up after power is restored, it will print a message to the console and generate a log message to tell you the reason for the shutdown.

If the switch is in a stack, only the overheated stack member will shut down.

You can disable the over-termperature shutdown by using the new command:

```
awplus(config)#no system overtemperature-shutdown
```

Only do this if the switch's temperature sensors are faulty.

If you disable the over-temperature shutdown, the switch will still generate warning log messages and SNMP traps, to warn you that the temperature is too high. However, it will not power off.

MAC authentication enhancement

Available on all AlliedWare Plus switches. Previously available on IX5, x510, x510L and x230 Series switches

With this enhancement, MAC authentication can use static entries in the FDB.

A new command, **auth-mac static**, configures MAC authentication to use static entries in the FDB. Static entries persist in the FDB, even if there is no traffic flow from the supplicant.

By default MAC authentication supplicants are added to the FDB dynamically. To revert to default behavior, use the **no auth-mac static** command.

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

Active Fiber Monitoring enhancements

Available on all AlliedWare Plus switches that support VCStack.

From 5.4.8-0.2 onwards, Active Fiber Monitoring has the following enhancements:

- You can now set the baseline calculation timer separately from the alarm monitoring timer, by using the command **fiber-monitoring baseline average <number> interval <seconds>**.

  In order to prevent the theoretical possibility of slow clamping, you can set the baseline calculation timer to a large value, so that the baseline average is only updated with the current reading (for example) once per day or once per hour.

  As fiber attenuation can be affected by ambient temperature, take care if changing this value in environments with large daily temperature fluctuations.
- Active Fiber Monitoring can now monitor optical long-distance stacking links.
- You can now configure Active Fiber Monitoring actions (logging, SNMP traps, and port shutdown) to happen continuously (every polling interval) while the sensor is in the alarm state. To do this, use the new **continuous** parameter in the command **fiber-monitoring action**.
- You can now manually clear the fiber-monitoring state for an interface, including resetting the alarm and removing all baseline readings. To do this, use the command **clear fiber-monitoring interface <port>**.

For configuration examples of these enhancements, see the Active Fiber Monitoring section of the Pluggables and Cabling Feature Overview and Configuration Guide.

Route summarization for RIPv2

From 5.4.8-0.2 onwards, you can create an IP summary address for RIPv2. This is often referred to as route summarization.

Route summarization is a technique that helps network administrators in reducing the size of the routing tables by advertising a single super-network that covers a range of subnets.

Why is route summarization useful?

Many large networks have multiple inter-connecting devices with multiple LANs and network segment splits. When this is the case, routing tables become larger and consume vast amounts of memory and processing capability. This means that routing devices will take longer to search their routing table in order to route a packet.

Route summarization improves scalability and efficiency in large networks because it:

- reduces the size of the routing table
- increases router processing capability, as less CPU cycle time needs to be dedicated to route table lookups due to the smaller route table size.

See the RIP Feature Overview and Configuration Guide for details on configuring route summarization for RIPv2.

OpenFlow connection interruption enhancement

From 5.4.8-0.2 onwards, you can set the operation mode for the switch when the Controller connection fails or no Controllers are defined.

If an OpenFlow switch loses contact with all Controllers as a result of echo request timeouts, then the OpenFlow switch goes into fail mode. There are two fail modes available:

- In **standalone** mode, if no message is received from the OpenFlow Controller for three times the inactivity probe interval, then OpenFlow will take over responsibility for setting up flows. OpenFlow 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.

  NOTE: If the OpenFlow switch is in fail mode, and you change the configured fail mode to or from standalone mode, OpenFlow will flush all existing rules.

- In **secure** mode, OpenFlow will not set up new flows on its own when the Controller connection fails or when no Controllers are defined, but all existing flows are left in place. The switch will continue to retry connecting to any defined Controllers forever. When the non-rule-expired option is enabled, existing rules won't be expired regardless of their timeouts while under fail mode. In other words, the OpenFlow switch will ignore timeout values of both idle timeout and hard timeout in existing rules.

The default mode is secure mode.

To set the fail mode to standalone mode, use the command:

```
awplus(config)#openflow failmode standalone
```

To set the mode to secure mode, use the command:

```
awplus(config)#openflow failmode secure non-rule-expired
```

G.8032 and Connectivity Fault Management (CFM) on SBx81CFC960

Version 5.4.8-0.2 adds support for G.8032 ring protection on Connectivity Fault Management (CFM) on SBx8100 systems using CFC960 control cards. A number of other AlliedWare Plus switches already support G.8032 and CFM.

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.

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 G.8032 Feature Overview and Configuration Guide and the CFM Feature Overview and Configuration Guide.

Precision Time Protocol (PTP) and Transparent Clock on x550 and x230 Series switches

Available on x550 and x230 Series switches. Previously available on IE300 and x930 Series switches

From 5.4.8-0.2 onwards, x550 and x230 Series switches support use of PTP and the Transparent Clock in an IEEE 1588 network, to provide:

- End-to-End delay mechanism
- 1-Step based time stamping mode

Precision Time Protocol (PTP) is an Ethernet or IP-based protocol for synchronizing time clocks on a collection of network devices using a Master/Slave distribution mechanism.

PTP is used for applications that require very high precision timing using Ethernet or Ethernet/IP. For example, Telco applications such as cellular, where not only frequency, but also phase precision is needed in order to control hand-off of mobile phones from one cell tower to the next.

The Transparent Clock feature is used by bridges or routers to assist clocks in measuring and adjusting for packet delay. The transparent clock computes the variable delay as the PTP packets pass through the switch or the router.

For more information and configuration details, see the Precision Time Protocol & Transparent Clock Feature Overview and Configuration Guide.

ACL scaling enhancements

Available on x230, x310, IX5, x510L, x510, x930, DC2552XS/L3, SBx908 GEN2, GS970M, GX900MX/MPX, IE200, IE300 and IE510-28GSX-80 switches

From 5.4.8-0.2 onwards, AlliedWare Plus switches handle large numbers of ACLs more quickly:

- internal storage and comparison of port-based ACLs has been improved. This reduces the amount of time to apply a large number of ACLs to a number of port ranges.
- internal handling of VLAN ACLs has been improved. This reduces the time taken to apply a large number of VLAN ACLs.

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

256 BGP routes on IE300 Series switches

Now available on IE300 Series switches. Already available on SBx8100 Series, SBx908, SBx908 GEN2, DC2552XS/L3, x930 Series, x510 Series, x510L Series, x550 Series, AR4050S, AR3050S, AR2050V and AR2010V.

From 5.4.8-0.2 onwards, AlliedWare Plus supports 256 BGP routes on IE300 Series switches, as part of the Premium feature license.

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

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

The OpenFlow protocol on SBx908 GEN2

Now available on SBx908 GEN2 switches. Already available on DC2552XS/L3, IE510-28GSX-80, IE300, x930, x550, x510, x510L, x310, and x230 Series switches

From 5.4.8-0.2 onwards, AlliedWare Plus supports version 1.3 of the OpenFlow protocol on SBx908 GEN2 switches.

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

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

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

VLAN ID translation on SBx908 GEN2 and x930 Series switches

Now available on SBx908 GEN2 and x930 Series switches. Already available on IE510-28GSX-80, x510, x510L and IE300 Series switches

From 5.4.8-0.2 onwards, AlliedWare Plus supports VLAN ID translation on SBx908 GEN2 and x930 Series switches. VLAN ID translation translates a VLAN's VLAN ID to another value for use on the wire.

On x930 Series switches, you need to allocate hardware space to VLAN ID translation by using the command:

```
awplus(config)#platform vlan translation enable
```

When you use this platform command, the number of L2 FDB entries reduces from 60K entries to 52K entries.

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

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

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

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

Enhanced show command output includes IPv6 address states

Available on all AlliedWare Plus devices

From 5.4.8-0.2 onwards, the **show ipv6 interface** and **show interface** commands also return information about the configuration and state of connected IPv6 addresses. A star symbol '*' also indicates an auto-configured address.

What are the IPv6 address states?

The show command output will indicate the state of the address by displaying one of the following:

- Tentative - an address in the process of being verified through duplicate address detection.
- DAD failed - duplicate address detection found that the address is not unique and cannot be used on this interface.
- Preferred - an address that has been verified as unique. Communication with this address is unrestricted.
- Deprecated - if the preferred lifetime of a preferred address times out the address goes into the deprecated state. Communication to/from a deprecated address is valid but discouraged.

The enhanced output is useful for network engineers

This information is useful because only preferred or deprecated addresses are valid for sending and receiving.

IPv6 addresses can be configured manually or automatically. Auto-configured addresses are temporary and should not be treated in the same way as permanent addresses because they may change. Thus, it is useful to be able to easily tell if an address is auto-configured, as well as the IPv6 state of the address.

Displaying files on all stack members

From 5.4.8-0.2 onwards, you can display files on all stack members with one command. To do this, use the new command:

```
dir stack-wide [all] [recursive] [sort [reverse] {name|size|
time}] [<filename>|flash|nvs|card|usb|debug]
```

This new **dir stack-wide** command behaves the same as the existing **dir** command, except for running on all stack members.

Examples

To show files in the current directory across all stack members, use the command:

```
awplus#dir stack-wide
```

To show files in the root flash directory across all stack members, use the command:

```
awplus#dir stack-wide flash
```

To show all files recursively in the root flash directory across all stack members, use the command:

```
awplus#dir stack-wide all recursive flash
```

Inclusion of stackport entry in the configuration file on stack members

Available on all switches that support VCStack

From 5.4.8-0.2 onwards, if a port is being used as for stacking, a "stackport" command entry is included for that port in the configuration file. For example, the configuration file might read:

```
interface port2.0.51
 stackport
 fiber-monitoring action trap
 fiber-monitoring baseline fixed 1200
 fiber-monitoring sensitivity fixed 500
 fiber-monitoring enable
```

This change has been done to enable Active Fiber Monitoring configuration of ports that are used as optical long-distance stacking links.

Previously, only SBx908 GEN2, XS900MX, and x550 included the stackport command in the configuration, because only those switches have user-selectable stack ports. On other switches, you still cannot use the stackport command to select which port you use for stacking; the only commands that you can enter on stacking ports are Active Fiber Monitoring commands, shutdown and no shutdown.

If you have a CFC960 with provisioning entries for its stack neighbors, and you upgrade it to 5.4.8-0.2, this change may result in errors at start-up. You can ignore these errors. See "Startup configuration errors when provisioning stackports on CFC960" on page 61 for more information.

"no terminal monitor" command

From 5.4.8-0.2 onwards, you can use **no terminal monitor** as an alias for the command **terminal no monitor**.

This command stops debug output from displaying on the monitor.

Displaying kernel crash files

From 5.4.8-0.2 onwards, the following commands will include kernel crash files:

- show exception log
- show tech-support

Kernel crash files may be useful for debugging purposes, especially by Allied Telesis support engineers.

Increased multicast limit on IE300 Series switches

From 5.4.8-0.2 onwards, IE300 Series switches support up to 1024 multicast entries. Previously, 256 entries were supported.

10Gbps support available in the base license on x510L Series switches

From 5.4.8-0.2 onwards, Allied Telesis no longer requires you to purchase a license before using 10Gbps SFP+ modules on x510L Series switches. This increases the flexibility and value of the x510L Series.

Important Considerations Before Upgrading

This section describes changes that are new in 5.4.8-x.x and may affect your network behavior if you upgrade. Please read it carefully before upgrading.

It describes the following changes:

- New firewall rule needed to allow access to external services
- x230 Series now support 118 ACLs
- Startup configuration errors when provisioning stackports on CFC960
- IPv6 traffic uses only the first available nexthop in a PBR rule
- DC2552XS/L3 now supports 12000 RIP routes
- Executing WRR queue commands interrupts traffic on SBx908 GEN 2
- Changes to the recommended method of removing a switch from a VCStack

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

- Software Release Licensing
- ISSU (In-Service Software Upgrade) on SBx8100 with CFC960
- Upgrading a VCStack with reboot rolling
- Forming or extending a VCStack with auto-synchronization
- AMF software version compatibility
- Upgrading all switches in an AMF network

If you are upgrading from an earlier version than 5.4.7-2.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.4.7-1.x version, please check the 5.4.7-2.x release note. Release notes are available from our website, including:

- 5.4.7-x.x release notes
- 5.4.6-x.x release notes

New firewall rule needed to allow access to external services

Applies to AR4050S and AR3050S

From 5.4.8-0.2 onwards, you need a firewall rule to permit traffic generated by the firewall that is destined for external services. These services include:

- DNS lookups and DNS relay
- Update Manager
- Web Control queries
- Routing protocols
- Subscription licensing

Previously we provided configuration instructions for creating rules for each individual type of traffic. We now recommend creating a single rule to cover all traffic generated by the firewall that is destined for external services.

For information about how to do this, see the "Configuring Firewall Rules for Required External Services" section in the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

x230 Series now support 118 ACLs

Applies to x230 Series switches

From 5.4.8-0.2 onwards, x230 Series switches support a maximum of 118 user-configurable ACLs. Previously, the maximum was 119.

Startup configuration errors when provisioning stackports on CFC960

Applies to SBx81CFC960

From 5.4.8-0.2 onwards, the stacking ports on provisioned switches and CFC960 control cards are displayed as stackports in the running configuration. Previously, they were displayed as access ports.

On a CFC960, this means that if you save the configuration on a previous release, and then you upgrade to 5.4.8-0.2 or later, the switch may report command errors on start-up. You can ignore these errors.

An example of such errors is:

```
WARNING: Failed to execute the following commands:
 219:  switchport -- % The command is not available for this interface
 220:  switchport mode access -- % The command is not available for
this interface
 304:  switchport -- % The command is not available for this interface
 305:  switchport mode access -- % The command is not available for
this interface
```

You are unlikely to see such errors on other switches. On other switches, if stackports are included in an interface range command with switchports, AlliedWare Plus removes the stackports from the range automatically. Therefore, the commands that generate the errors are not executed.

IPv6 traffic uses only the first available nexthop in a PBR rule

Applies to AR4050S and AR3050S firewalls and AR2050V and AR2010V routers

From 5.4.8-0.2 onwards, if a policy-based routing (PBR) rule contains multiple IPv6 nexthops, the device sends IPv6 traffic only via the first available nexthop in the list.

Previously, although most traffic would take the first available nexthop, a small amount of the traffic would be spread over the remaining nexthops. This meant that some traffic did not take the expected path.

DC2552XS/L3 now supports 12000 RIP routes

Applies to DC2552XS/L3 switches

From 5.4.8-0.2 onwards, DC2552XS/L3 switches support a maximum of 12000 RIP routes. Previously, the maximum was 16000.

Executing WRR queue commands interrupts traffic on SBx908 GEN 2

Applies to SBx908 GEN2 switches

From 5.4.8-0.2 onwards, executing the following commands on an SBx908 GEN2 interrupts traffic flow:

```
wrr-queue weight
no wrr-queue
```

The interruption lasts for less than a second and resolves automatically.

When you enter either of the above commands, the switch displays a message to warn you about the traffic interruption and allow you to abort the command.

Changes to the recommended method of removing a switch from a VCStack

Applies to all switches that support VCStack

Previously, it was possible to enter the **no stack <stack-id> enable** command to remove a switch from a stack while the switch was still an active member of the stack.

From 5.4.8-0.2 onwards, this is no longer possible. Instead, use the following steps to remove a switch from a stack:

1. Shut down all stacking links to the switch you wish to remove from the stack. This is optional but recommended, especially if someone other than you will do the step of physically uncabling the switch.
2. Remove all of the cabling used for stacking links.
3. Re-cable the remaining stack members together correctly.
4. Log into the disconnected device and run the command **no stack <stack-id> enable**.
5. If you want to use the switch as a standalone switch, reset its stack ID to 1. Use the command **stack <old-id> renumber 1**

Software Release Licensing

Applies to SBx908, SBx908 GEN2 and SBx8100 Series switches

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

Please ensure you have a 5.4.8 license on your switch if you are upgrading to 5.4.8-x.x on your SBx908, SBx908 GEN2 or SBx8100 switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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 5.4.8-0.2 from any previous software version.

- 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	5.4.8-0.2	5.4.8-0.3	5.4.8-0.4	5.4.8-0.5	5.4.8-0.7	5.4.8-0.8	5.4.8-0.9	5.4.8-0.10
	5.4.8-0.2		C	I					
	5.4.8-0.3			C	I				
	5.4.8-0.4				C	I			
	5.4.8-0.5					C	I		
	5.4.8-0.7						C	I	
	5.4.8-0.8							C	I
	5.4.8-0.9								C

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 5.4.8-0.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 5.4.8-0.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 5.4.8-0.x and:

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

It is not supported between 5.4.8-0.x and 5.4.6-1.1 or **any** earlier releases.

AMF software version compatibility

Applies to all AlliedWare Plus devices

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

If using an AMF controller

If your Controller or **any** of your Masters are running 5.4.7-1.1 or later, then the Controller and **all** of the Masters must run 5.4.7-1.1 or later. However, the software on Member nodes can be older than 5.4.7-1.1.

Otherwise, the "show atmf area nodes" command and the "show atmf area guests" command will not function, and Vista Manager EX will show incorrect network topology.

If using secure mode

If your AMF network is in secure mode, all nodes must run version 5.4.7-0.3 or later. Upgrade all nodes to 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 as well as the restrictions above:

- All nodes must run version 5.4.7-0.1 or later
- If any Master node or the Controller is running 5.4.7-0.x, then all nodes must also run 5.4.7-0.x

If using none of the above

If none of the above apply, then nodes running version 5.4.8-0.x are compatible with nodes running:

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

Upgrading all switches in an AMF network

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

1. Copy the release .rel files for each product family to the media location you intend to upgrade from (Flash memory, SD card, USB stick etc).
2. Decide which AMF upgrade method is most suitable.
3. Initiate the AMF network upgrade using the selected method. To do this:
   a. create a working-set of the nodes you want to upgrade
   b. enter the command **atmf reboot-rolling <*location*>** or **atmf distribute-firmware <*location*>** where **<*location*>** is the location of the .rel files.
   c. Check the console messages to make sure that all nodes are “release ready”. If they are, follow the prompts to perform the upgrade.

Obtaining User Documentation

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

- **Feature Overview and Configuration Guides** - find these by searching for the feature name and then selecting Feature Guides in the right-hand menu.
- **Datasheets** - find these by searching for the product series and then selecting Datasheets in the right-hand menu.
- **Installation Guides** - find these by searching for the product series and then selecting Installation Guides in the right-hand menu.
- **Command References** - find these by searching for the product series and then selecting Manuals Guides in the right-hand menu.

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.

Caution

If the verification fails, the following error message will be generated:

If the verification fails, the following error message will be generated the same Global revel.

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 Version on an SBx908 or SBx908 GEN2 Switch

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

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

1. Obtain the MAC address for a switch

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

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

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

2. Obtain a release license for a switch

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

3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

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

```
awplus#show license

Board region: Global

Index                          : 1
License name                   : Base License
Customer name                  : Base License
Type of license                : Full
License issue date             : 30-Mar-2018
Features included              : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                                 EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                                 L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                                 RADIUS-100, RIP, VCStack, VRRP

Index                          : 2
License name                   : 5.4.8
Customer name                  : ABC Consulting
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 30-Mar-2018
License expiry date            : N/A
Release                        : 5.4.8
```

Licensing this 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-2018
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                 Virtual-MAC, VRRP

Index                          : 2
License name                   : 5.4.8
Customer name                  : ABC Consulting
Quantity of licenses           : -
Type of license                : Full
License issue date             : 20-Mar-2018
License expiry date            : N/A
Release                        : 5.4.8
```

Installing this Software Version

Caution: Software versions 5.4.8-x.x require a release license for the SBx908, SBx908 GEN2 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- "Licensing this Version on an SBx908 or SBx908 GEN2 Switch" on page 70 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 72.

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 FS980-5.4.8-0.10.rel`
GS900MX/MPX series	`awplus(config)# boot system GS900-5.4.8-0.10.rel`
GS970M series	`awplus(config)# boot system GS970-5.4.8-0.10.rel`
XS900MX series	`awplus(config)# boot system XS900-5.4.8-0.10.rel`
x230 series	`awplus(config)# boot system x230-5.4.8-0.10.rel`
IE200 series	`awplus(config)# boot system IE200-5.4.8-0.10.rel`
x310 series	`awplus(config)# boot system x310-5.4.8-0.10.rel`
IE300 series	`awplus(config)# boot system IE300-5.4.8-0.10.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.8-0.10.rel`
x510 series	`awplus(config)# boot system x510-5.4.8-0.10.rel`
x550 series	`awplus(config)# boot system x550-5.4.8-0.10.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.4.8-0.10.rel`
x550 series	`awplus(config)# boot system x550-5.4.8-0.10.rel`

Product	Command
x930 series	`awplus(config)# boot system SBx930-5.4.8-0.10.rel`
DC2552XS/L3	`awplus(config)# boot system DC2500-5.4.8-0.10.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.4.8-0.10.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.8-0.10.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.8-0.10.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.8-0.10.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.4.8-0.10.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.8-0.10.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.8-0.10.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.8-0.10.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 web-based device GUI

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

The GUI is currently available for AR-Series devices, GS900MX/MPX, FS980M, GS970M, XS900MX Series, and x220, x230, x310, IX5, x510, x510L, x550, and x930 Series switches. It will be released progressively across the remaining AlliedWare Plus switches during 2018.

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

On AR3050S and AR4050S firewalls, you can use the GUI to create an advanced application-aware firewall with features such as Application control and Web control. Alternatively, you can configure real-time threat protection with URL filtering, Intrusion Prevention and Malware protection.

On all AR-Series devices, you can also optimize the performance of your Allied Telesis APs through AWC.

The steps for accessing the GUI depend on whether the GUI has been pre-installed on your device in the factory, and if not, whether you are using a AR-Series device or a switch. See:

- GUI pre-installed at factory: all devices
- GUI not pre-installed or updating the GUI: AR-Series devices
- GUI not pre-installed or updating the GUI: Switches

GUI pre-installed at factory: all devices

Perform the following steps to browse to the GUI if your device came with the GUI pre-installed.

1. Connect to any of the LAN switch ports.
2. Open a web browser and browse to the default IP address for VLAN1. The default address is:

Device	Address
AR-Series	192.168.1.1
Switches	169.254.42.42

   Alternatively, give VLAN1 an IP address of your choice and browse to that address.
3. Log in with the default username of *manager* and the default password of *friend*.

GUI not pre-installed *or* updating the GUI: AR-Series devices

Perform the following steps through the command-line interface if:

- your AR-series device did not come with the GUI pre-installed, or
- you have been running an earlier version of the GUI and need to update it (steps 3 onwards).

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. If you are updating the GUI, stop and restart the HTTP service:

```
awplus# configure terminal
awplus(config)# no service http
awplus(config)# service http
```

5. If you are installing the GUI for the first time, make sure the HTTP service is running:

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

6. Log into the GUI.

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

   The GUI starts up and displays a login screen. Log in with your username and password.

GUI not pre-installed *or* updating the GUI: Switches

Perform the following steps through the command-line interface if:

- your AlliedWare Plus switch did not come with the GUI pre-installed, or
- you have been running an earlier version of the GUI and need to update it.

1. Obtain the GUI file from our Software Download center. The file is named awplus-gui_548_0x.tar.gz.

   The file is not device-specific; the same file works on all devices.

2. Copy the file into Flash memory on your switch. You can copy the file into Flash using any of the following methods:

   - TFTP server
   - USB Flash drive
   - SD card

   For example, to copy the GUI file from your USB Flash drive, use the following commands:

   ```
   awplus>enable
   awplus#copy usb awplus-gui_548_0x.tar.gz flash
   ```

   To view all files in Flash and check that the newly installed file is there, use the following command:

   ```
   awplus#dir
   ```

3. Delete any previous Java switch GUI files.

   If you have been using the previous Java switch GUI, it is advisable to delete the old GUI file to avoid any conflict. To do this, delete any Java files (.jar) from the switches Flash memory. For example:

   ```
   awplus#del x510-gui_547_02.jar
   ```

4. Add an IP address to a VLAN on the switch. For example:

   ```
   awplus#configure terminal
   awplus(config)#interface vlan1
   awplus(config-if)#ip address 192.168.1.1/24
   awplus(config-if)#exit
   ```

5. If you are updating the GUI, stop and restart the HTTP service:

   ```
   awplus# configure terminal
   awplus(config)# no service http
   awplus(config)# service http
   ```

6. If you are installing the GUI for the first time, make sure the HTTP service is running:

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

7. Log into the GUI.

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

   The GUI starts up and displays a login screen. Log in with your username and password.

   The default username is *manager* and the default password is *friend*.