Release Note for AlliedWare Plus Software Version 5.4.8-1.x

AlliedWare Plus
OPERATING SYSTEM

» SBx8100 Series » SBx908 GEN2 » SBx908

» x930 Series » x550 Series » x510 Series » IX5 Series

» x310 Series » x230 Series » x220-28GS

» IE500 Series » IE300 Series » IE210L Series » IE200 Series

» XS900MX Series » GS970M Series » GS900MX/MPX Series

» FS980M Series » AMF Cloud

» AR4050S » AR3050S » AR2050V » AR2010V

» 5.4.8-1.2 » 5.4.8-1.3 » 5.4.8-1.4 » 5.4.8-1.5 » 5.4.8-1.6

Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.

Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California.

All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see **www.openssl.org/**

Copyright ©1998-2008 The OpenSSL Project. All rights reserved.

This product includes software licensed under the GNU General Public License available from: **www.gnu.org/licenses/gpl2.html**

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

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

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

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

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

Getting the most from this Release Note

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

Content

What’s New in Version 5.4.8-1.6

Product families supported by this version:

FS980M Series
GS900MX/MPX Series
GS970M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220-28GS
x230 Series
x310 Series
IX5-28GPX
x510 Series
x550 Series
x930 Series
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-1.6.

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.

If an SBx908, SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

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 61 and
- “Licensing this Version on an SBx8100 Series Switch Control Card” on page 63.

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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	11/2018	FS980-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2018	GS900-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2018	GS970-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
XS916MXT XS916MXS	XS900MX	11/2018	XS900-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2018	IE200-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
IE300-12GT IE300-12GP	IE300	11/2018	IE300-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
IE210L-10GP IE210L-18GP	IE210L	11/2018	IE210-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
IE510-28GSX-80	IE500	11/2018	IE510-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
x220-28GS	x220	11/2018	x220-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT	x230	11/2018	x230-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2018	x310-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
IX5-28GPX	IX5	11/2018	IX5-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	11/2018	x510-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2018	x550-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2018	x930-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
SBx908 GEN2	SBx908 GEN2	11/2018	SBx908NG-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
SBx908 (see Table 2)	SBx908	11/2018	SBx908-5.4.8-1.6.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	11/2018	SBx81CFC400-5.4.8-1.6.rel SBx81CFC960-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
AR4050S AR3050S	AR-series UTM firewalls	11/2018	AR4050S-5.4.8-1.6.rel AR3050S-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
AR2050V AR2010V	AR-series VPN firewalls	11/2018	AR2050V-5.4.8-1.6.rel AR2010V-5.4.8-1.6.rel	See "Accessing the web-based device GUI" on page 67
AMF Cloud		11/2018	vaa-5.4.8-1.6.iso (VAA OS) vaa-5.4.8-1.6. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-1.6.vhd (for Microsoft Azure)	

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-0.x and 5.4.8-1.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

Note that 5.4.8-1.x is the last supported software stream for the SwitchBlade x908. Version 5.4.8-2.x will not support the SwitchBlade x908.

Support for the SwitchBlade x908 GEN2 is ongoing.

Unsupported devices

Version 5.4.8-1.x does not support DC2552XS/L3 switches.

Enhancements in 5.4.8-1.6

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-2476	**IPv4**	With this software update, route database management on AlliedWare Plus switches has been improved to ensure that a directly connected route entry will not be overlooked after a port is shut down and then brought back up again	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–

Issues Resolved in 5.4.8-1.6

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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61384	**ARP** **VRRP**	Previously, when a VRRP master was not the virtual IP owner and proxy ARP was configured on the VRRP interface, if an ARP for an address in the VRRP interface's subnet was received, the device would perform proxy ARP for that address. This was incorrect and was behaving like "local proxy ARP". The issue has been resolved. Now it only performs proxy ARP for addresses reachable over interfaces other than the VRRP interface (i.e. normal proxy ARP behaviour). ISSU: Effective when ISSU complete.	Y	–	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y
CR-61414	**ARP** **VRRP**	Previously, in a VRRP configuration, if the VRRP interface on each router was also configured with Proxy ARP, the device(s) in the VRRP Backup state would give proxy ARP response with their real MAC address in addition to the proxy ARP replies sent by the Master with the Virtual MAC address. 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
CR-62068	**CLI**	Previously, the **show interface** command would display overflowed interface running time. 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	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60293	**DHCP Server**	With this software update, the DHCPv4 short-lease parameter is now configurable. The following command has been added: **`short-lease-threshold <hours> <minutes>`**. The threshold can be changed between 1 minute to 1 day. By default, the threshold is still 1 minute. Any lease less than this threshold will not be backed up in NVS. ISSU: Effective when ISSU Complete.	–	–	–	–	–	Y	Y	–	–	Y	Y	–	–	Y	Y	–	–	Y	Y	Y	Y	–
CR-61002	**DPI**	Previously, if modifying the configuration of one of the stream based security features (such as Malware Protection, IPS, URL Filtering IP or Reputation) while a device was in the process of transmitting a packet, it was possible for the packet forwarding process to incorrectly think a memory buffer needed to be freed, even though the list of buffers to be freed was actually empty. This could result in a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-61299	**Environmental Monitoring**	With this software update, on IE300 series switches, adding a link-down alarm to an aggregator or VLAN interfaces now no longer adds alarms to all ports. Messages are also now printed if trying to add an alarm to a port that is an aggregator member. This issue has been resolved.	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-61109	**Environmental Monitoring**	Previously on an IE510 switch, the output relays would be deactivated (closed) on power-on. Any alarm state would not be reflected until configuration was complete. This was an issue on backup stack members as the relays on backup members are expected to be open. This issue has been resolved. Now, (in conjunction with required bootloader version 2.0.31 or later), the output relays are activated (opened) within a few seconds of powering on the device and remain active until stack configuration is complete to ensure that the output relays reflect their configuration.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61270	**Environmental Monitoring**	Previously, alarm-monitoring alarms would not be triggered correctly if the **snmp-server source-interface IFNAME** command was used in the device configuration. This issue has been resolved.	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-61315	**IGMP**	Previously, PIM Dense Mode Multicast routes could time out and be deleted even if traffic was still flowing if the source was not directly connected. This resulted in one or more packets being dropped while the route was re-learned. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-61446	**IPSec**	Previously, if an IPsec tunnel had a "dynamic" tunnel destination address, the remote peer was behind a NAT device and that NAT device was given a new IP address from the network, then the local router would detect the change in IP address and update the ISAKMP and IPsec NAT-T SA's, but would fail to update the "dynamic" tunnel interface address. This resulted in the received traffic being dropped even though the IP address was correctly detected. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-62062	**Layer 3 Multicast**	Previously, if multicast traffic needed to be sent to a port on multiple VLANs, and one of those VLANs was the same as the ingress VLAN, the traffic to the ingress VLAN would not be sent. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	Y	–
CR-61365	**PoE**	Previously, the colour display of the PoE LED status was incorrect for Denied and Fault status. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	–	–	Y	–	–	–	–
CR-61229	**Static Aggregation** **VCStack**	Previously, when a link aggregation was configured on a stack, L3 NLB packets were not forwarded if the ingress and egress ports were the same port. This issue has been resolved.	–	–	–	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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60580	**VCStack**	Previously, a late joining stack member on a x550 series stack of switches could cause the switch to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–

What’s New in Version 5.4.8-1.5

Product families supported by this version:

FS980M Series
GS900MX/MPX Series
GS970M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220-28GS
x230 Series
x310 Series
IX5-28GPX
x510 Series
x550 Series
x930 Series
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-1.5.

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.

If an SBx908, SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

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 61 and
- “Licensing this Version on an SBx8100 Series Switch Control Card” on page 63.

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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	11/2018	FS980-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	11/2018	GS900-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	11/2018	GS970-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
XS916MXT XS916MXS	XS900MX	11/2018	XS900-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	11/2018	IE200-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
IE300-12GT IE300-12GP	IE300	11/2018	IE300-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
IE210L-10GP IE210L-18GP	IE210L	11/2018	IE210-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
IE510-28GSX-80	IE500	11/2018	IE510-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
x220-28GS	x220	11/2018	x220-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT	x230	11/2018	x230-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
x310-26FT x310-50FT x310-26FP x310-50FP	x310	11/2018	x310-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
IX5-28GPX	IX5	11/2018	IX5-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	11/2018	x510-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	11/2018	x550-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	11/2018	x930-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
SBx908 GEN2	SBx908 GEN2	11/2018	SBx908NG-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
SBx908 (see Table 2)	SBx908	11/2018	SBx908-5.4.8-1.5.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	11/2018	SBx81CFC400-5.4.8-1.5.rel SBx81CFC960-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
AR4050S AR3050S	AR-series UTM firewalls	11/2018	AR4050S-5.4.8-1.5.rel AR3050S-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
AR2050V AR2010V	AR-series VPN firewalls	11/2018	AR2050V-5.4.8-1.5.rel AR2010V-5.4.8-1.5.rel	See "Accessing the web-based device GUI" on page 67
AMF Cloud		11/2018	vaa-5.4.8-1.5.iso (VAA OS) vaa-5.4.8-1.5. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-1.5.vhd (for Microsoft Azure)	

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-0.x and 5.4.8-1.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

Note that 5.4.8-1.x is the last supported software stream for the SwitchBlade x908. Version 5.4.8-2.x will not support the SwitchBlade x908.

Support for the SwitchBlade x908 GEN2 is ongoing.

Unsupported devices

Version 5.4.8-1.x does not support DC2552XS/L3 switches.

Enhancements in 5.4.8-1.5

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
ER-1485	**AMF**	With this software update, two new CLI commands and associated Web API have been introduced. These commands will manually reset an AMF link (or virtual link) in an attempt to clear an error condition. **1**) **`clear atmf links`** [<*if-range*>|] This will reset all links in the specified interface range. For example: clear atmf links - reset all interfaces clear atmf links port1.0.1-1.0.10 - reset all of the specified interfaces **2**) **`clear atmf links virtual`** [vlinkDDD{,vlinkDDD}|] This will reset all virtual links or the specified virtual link. For example: clear atmf links virtual - reset all virtual links clear atmf links virtual vlink11 - reset specified virtual link clear atmf links virtual vlink11,vlink12 - reset specified virtual links	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ER-2196	**GUI**	With this software update, a GUI release remains after "atmf cleanup"or "erase factory-defaults" is used. This GUI will be available to configure the clean device when it reboots. If multiple GUIs are available on a device, the most appropriate GUI file for the release is automatically selected when "service http" is enabled. ISSU: Effective when CFCs Upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ER-2476	**IPv4**	With this software update, the route database management that affects the handling of connected routes has been improved to prevent a directly connected route entry from being removed after a port is brought down and up again. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–

Issues Resolved in 5.4.8-1.5

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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60995	**AMF**	Previously, an AMF master undergoing a VCS failover could end up with a different restricted login status to the rest of the network. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y
CR-61184	**AMF**	Previously, an SNMP walk of the ATMF MIB (1.3.6.1.4.207.8.4.4.4.603) could result in an atAtmfNodeName being corrupted. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-61092	**AMF** **Logging**	With this software update, the erroneous GUI log message: *"Alert: GUI file not found, no GUI will be available on the clean device"* was removed from AlliedWare Plus devices. 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-60293	**DHCP Server**	With this software update, the IPv4 DHCP short-lease parameter is now configurable. The following command has been added: **`short-lease-threshold`** ***`<hours>`*** ***`<minutes>`***. The threshold can be changed between 1 minute to 1 day. By default, the threshold is still 1 minute. Any lease less than this ***threshold*** will not be backed up in NVS. ISSU: Effective when ISSU complete	–	–	–	–	–	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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61002	**DPI**	Previously, if modifying the configuration of one of the stream based security features (such as Malware Protection, IPS, URL Filtering IP or Reputation) while a device was in the process of transmitting a packet, it was possible for the packet forwarding process to incorrectly think a memory buffer needed to be freed, even though the list of buffers to be freed was actually empty. This could result in a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-60552	**Environmental Monitoring**	Previously, some power supply events were not handled correctly by alarm-monitoring on IE-510 Series switches. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-60246	**Environmental Monitoring**	Previously, voltage alarm detection could sometimes fail to work. This issue has been resolved.	–	–	–	Y	–	–	–	–	Y	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-60475	**HW QoS**	Previously, the QoS Storm Protection for multiple class maps did not work. This issue has been resolved. ISSU: Effective when CFCs Upgraded.	Y	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–
CR-57887	**IPv4** **Unicast Routing**	Previously, if a device had alternative static or dynamic routes for subnets connected to it (i.e. a subnet associated with an interface address), it was possible for the device to lose connectivity with the connected subnet. This occurred when there was an associated interface change.For example, the VLAN goes down and then up, then the ports in the VLAN all go down and then up, resulting in; ■ the alternative route became the preferred route ■ then the connected route became the preferred route again 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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60518	**IPv6**	Previously, if: ■ you enabled IPv6 on an interface without disabling Router-Advertisement reception or Prefix Information Option (PIO) processing, ■ and the device received an RA with PIO containing a prefix with prefix length not equal to 64, ■ then the interface receiving the RA could have been put into an inoperable state. 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-60551	**LACP**	Previously, on an egress port on switches, the VLAN tag of a Connectivity Fault Management (CFM) packet would be incorrectly removed, causing the CFM fail to work. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	–
CR-60529	**LACP** **VCStack**	Previously, on a VCStack, if an LACP trunk with no synchronised ports had a stack member removed followed by a stack failover, then the internal state of the aggregator could result in an inconsistent state between the members. This could cause audit inconsistencies. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-61120	**Logging**	Previously, it was possible for the logwatch process to leak a small amount of memory each time that an authentication failure message 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	–
CR-60432	**Multicast**	Previously, the IGMP query packets were not being sent reliably. This could cause neighbouring devices to stop sending IGMP reports and the groups could time out. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61111	**OSPF**	Previously, if OSPF was configured with VFR-lite, OSPF LSA messages in the VRF-lite domains could sometimes have the DN bit set. This meant that other devices within the OSPF domain ignored those LSAs when calculating the SPF. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-61001	**Ping Polling**	Previously, when a connected link went down, ping-polling could be held in the critical up state that prevented a trigger to work. 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	–
CR-60427	**Pluggable Transceivers**	With this software update, the AT-QSFP-ER4 on switches can now operate with other 40G fiber pluggables.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	Y	–	–	–	–
CR-60403	**Port Configuration** **VCStack**	Previously the Web API for a switchport interface could return an error if provisioned stack ports were present on the switch. This issue has been resolved. ISSU: Effective when CFCs Upgraded.	Y	Y	Y	–	–	–	Y	–	–	Y	Y	–	Y	Y	Y	Y	Y	–	–	–	–	–
CR-60077	**SSL**	This software update address vulnerability CVE-2018-0732. AlliedWare Plus devices are no longer vulnerable to denial of service attacks during a TLS handshake using a large prime from the server. 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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60554	**Switching**	Previously, since 5.4.7-1 release, to reduce CPU load, the default behaviour for handling IP multicast packets with mismatched destination address and destination IP was changed from "flood" to "drop”. However, Microsoft NLB packets were no longer forwarded as a result of that change. With this software update, a new command has been added that can toggle this behaviour: **platform multicast-address-mismatch-action (drop|bridge)** The default behaviour depends on whether: **arp-mac-disparity multicast** or **arp-mac-disparity multicast-igmp** has been configured on an interface. ■ If this has been configured then the default action will be to flood the packets. ■ If this has not been configured then the default action will be to drop the packets. Using the platform command will override the default behaviour regardless of the "arp-mac-disparity" configuration. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–	–
CR-60402	**Switchport**	Previously, under rare occasions, the ports on x230 Series switches would not come up after a power cycle. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-60490	**System**	With this software update, the system stability of the SBx8100 series switches have been improved. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60477	**System**	This software update addresses vulnerability: CVE-2018-5391: ■ Previously, the memory limit for handling IP fragments was 4MB. ■ This has been reduced to 256KB which was the original default value. 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-57109	**System**	This software update addresses vulnerability: CVE-2016-10229: Remote attackers could execute arbitrary code via UDP traffic that triggered an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag. 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-56758	**System**	This software update addresses vulnerability: CVE-2017-6214: In which remote attackers could cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag. 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-59901	**System**	This software update addresses the following security vulnerability: "CERT CVE-2018-1108". 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-61046	**Unicast Forwarding**	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	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-61197	**VLAN**	Previously, you could not rename a VLAN from its default name to one of the same name but in a different case. For example "VLAN0020" could not be renamed to "Vlan0020". 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-61069	**Web Control**	With this software update, the memory handling of the proxy engine has been improved so that it will now use less memory in an idle environment.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

What’s New in Version 5.4.8-1.4

Product families supported by this version:

FS980M Series
GS900MX/MPX Series
GS970M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220-28GS
x230 Series
x310 Series
IX5-28GPX
x510 Series
x550 Series
x930 Series
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-1.4.

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.

If an SBx908, SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

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 61 and
- “Licensing this Version on an SBx8100 Series Switch Control Card” on page 63.

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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	09/2018	FS980-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	09/2018	GS900-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	09/2018	GS970-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
XS916MXT XS916MXS	XS900MX	09/2018	XS900-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	09/2018	IE200-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
IE300-12GT IE300-12GP	IE300	09/2018	IE300-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
IE210L-10GP IE210L-18GP	IE210L	09/2018	IE210-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
IE510-28GSX-80	IE500	09/2018	IE510-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
x220-28GS	x220	09/2018	x220-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT	x230	09/2018	x230-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
x310-26FT x310-50FT x310-26FP x310-50FP	x310	09/2018	x310-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
IX5-28GPX	IX5	09/2018	IX5-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	09/2018	x510-5.4.8-1.4.rel	See "Accessing the web-based device GUI" on page 67

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	09/2018	x550-5.4.8-1.4.rel	See “Accessing the web-based device GUI” on page 67
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	09/2018	x930-5.4.8-1.4.rel	See “Accessing the web-based device GUI” on page 67
SBx908 GEN2	SBx908 GEN2	09/2018	SBx908NG-5.4.8-1.4.rel	See “Accessing the web-based device GUI” on page 67
SBx908 (see Table 2)	SBx908	09/2018	SBx908-5.4.8-1.4.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	09/2018	SBx81CFC400-5.4.8-1.4.rel SBx81CFC960-5.4.8-1.4.rel	See “Accessing the web-based device GUI” on page 67
AR4050S AR3050S	AR-series UTM firewalls	09/2018	AR4050S-5.4.8-1.4.rel AR3050S-5.4.8-1.4.rel	See “Accessing the web-based device GUI” on page 67
AR2050V AR2010V	AR-series VPN firewalls	09/2018	AR2050V-5.4.8-1.4.rel AR2010V-5.4.8-1.4.rel	See “Accessing the web-based device GUI” on page 67
AMF Cloud		09/2018	vaa-5.4.8-1.4.iso (VAA OS) vaa-5.4.8-1.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-1.4.vhd (for Microsoft Azure)	

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-0.x and 5.4.8-1.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

Note that 5.4.8-1.x is the last supported software stream for the SwitchBlade x908. Version 5.4.8-2.x will not support the SwitchBlade x908.

Support for the SwitchBlade x908 GEN2 is ongoing.

Unsupported devices

Version 5.4.8-1.x does not support DC2552XS/L3 switches.

Issues Resolved in 5.4.8-1.4

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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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
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
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	–
CR-60326	**API**	Previously, the application proxy API would display "active ip-filter blocks" incorrectly as "Not_Applicable." 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	–
CR-60332	**DPI** **Web Control**	Previously, if Web-Control or Anti-virus was configured with one or more of DPI, IP Reputation, IPS, Malware Protection, or URL Filtering, then HTTP or HTTPS downloads and general Web browsing could be extremely slow. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-60373	**EPSR**	With this software update, the time taken for EPSR ring to recover from a 100G link (QSFP pluggable) down event has been improved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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-60286	**GUI**	Previously, executing the command **`show platform memory`** could generate some DBG messages due to incorrect index values being used. This issue has been resolved.	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-60432	**Layer 2 Multicast**	Previously, IGMP query packets were not being sent reliably, causing the neighbouring devices to stop sending IGMP reports. As a result, multicast traffic could fail to be forwarded. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	Y	–	–	–	–
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-60302	**Multicast**	Previously, a device could restart unexpectedly when large numbers of multicast groups were being learnt. This issue has been resolved.	–	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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60327	**OSPF**	Previously, when receiving updates for external LSAs for networks with overlapping subnets, 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	–
CR-60457	**OSPFv3** **RIPng**	Previously, the output of the **`show ipv6 route`** command would not show the uptime of dynamically installed routes. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-50732	**Port Security**	Previously, port-security commands were available via the CLI (but not working) on the IE200. Therefore, as the port-security feature is not supported on the IE200 platform, the port-security commands have been removed.	–	–	–	–	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	–
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
CR-59968	**System**	Previously, in rare circumstances, a stack device being configured in a stack may restart unexpectedly after a mirror port was added to a stack member followed by power cycling the stack member. This issue has been resolved. ISSU: Effective when ISSU complete.	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	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60421	**Trigger Script** **VCStack**	Previously, a trigger script might not be executed if a stack member was removed soon after the script was activated. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	Y	Y	Y	–	–	Y	–	–	Y	Y	Y	–	–	Y	Y	Y	Y	–	–	–	–
CR-60334	**Unicast Routing**	Previously, it was possible to add duplicate static blackhole routes where the only difference was whether the interface was spelled "Null" or "null" or some other variation in capitalization. Also, previously, deleting a static blackhole route would only work if the interface name was written with the same capitalization as when the route was added. Both issues have 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-60378	**UTM Offload**	With this software update, the UTM offload resource downloading is now working with firmware downgrading, i.e., the UTM offload resource file should match with the version of the firmware on the UTM device. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-60343	**VCStack**	Previously, members of a VCStack could sometimes unnecessarily separate if one of the stack cables was removed. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–
CR-60208	**VCStack**	Previously, it was possible for configuration scripts to be falsely reported as not being executed on startup for a late joining backup member. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-60347	**VCStack**	Previously, on x930 variant switches, detection of QSFPs on the StackQS would sometimes fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x220	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-60455	**VCStack**	Previously, it was possible for a stack member to lockup during a reboot if the **`show platform full-debug`** command was running at the same time. This issue has been resolved. ISSU: Effective when ISSU complete.	–	Y	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-60223	**Web API**	With this software update, alterations to the switchport configuration will now be reflected in the Vista Manager. 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-60300	**Web API**	With this software update, the *'local-atmf-topology'* field within the Web API is now retained for both an AMF master and an AMF controller. 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-60262	**Web Control**	With this software update, Web-Redirect performance has been increased when used without Antivirus or Web-Control.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

What’s New in Version 5.4.8-1.3

Product families supported by this version:

FS980M Series
GS900MX/MPX Series
GS970M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220-28GS
x230 Series
x310 Series
IX5-28GPX
x510 Series
x550 Series
x930 Series
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-1.3.

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.

If an SBx908, SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

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 61 and
- “Licensing this Version on an SBx8100 Series Switch Control Card” on page 63.

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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	07/2018	FS980-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	07/2018	GS900-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2018	GS970-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
XS916MXT XS916MXS	XS900MX	07/2018	XS900-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2018	IE200-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
IE300-12GT IE300-12GP	IE300	07/2018	IE300-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
IE210L-10GP IE210L-18GP	IE210L	07/2018	IE210-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
IE510-28GSX-80	IE500	07/2018	IE510-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
x220-28GS	x220	07/2018	x220-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT	x230	07/2018	x230-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2018	x310-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
IX5-28GPX	IX5	07/2018	IX5-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	07/2018	x510-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2018	x550-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2018	x930-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
SBx908 GEN2	SBx908 GEN2	07/2018	SBx908NG-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
SBx908 (see Table 2)	SBx908	07/2018	SBx908-5.4.8-1.3.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	07/2018	SBx81CFC400-5.4.8-1.3.rel SBx81CFC960-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
AR4050S AR3050S	AR-series UTM firewalls	07/2018	AR4050S-5.4.8-1.3.rel AR3050S-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
AR2050V AR2010V	AR-series VPN firewalls	07/2018	AR2050V-5.4.8-1.3.rel AR2010V-5.4.8-1.3.rel	See "Accessing the web-based device GUI" on page 67
AMF Cloud		07/2018	vaa-5.4.8-1.3.iso (VAA OS) vaa-5.4.8-1.3. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-1.3.vhd (for Microsoft Azure)	

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-0.x and 5.4.8-1.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

Note that 5.4.8-1.x is the last supported software stream for the SwitchBlade x908. Version 5.4.8-2.x will not support the SwitchBlade x908.

Support for the SwitchBlade x908 GEN2 is ongoing.

Unsupported devices

Version 5.4.8-1.x does not support DC2552XS/L3 switches.

Enhancement in 5.4.8-1.3

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x230	x310	IX5	x510, 510L	x550	x930	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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	–

What’s New in Version 5.4.8-1.2

Product families supported by this version:

FS980M Series
GS900MX/MPX Series
GS970M Series
XS900MX Series
IE200 Series
IE210L Series
IE300 Series
IE510-28GSX-80
x220-28GS
x230 Series
x310 Series
IX5-28GPX
x510 Series
x550 Series
x930 Series
SwitchBlade x908 GEN2
SwitchBlade x908
SwitchBlade x8100 Series
AR4050S
AR3050S
AR2050V
AR2010V
AMF Cloud

Introduction

This release note describes the new features in AlliedWare Plus software version 5.4.8-1.2.

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.

If an SBx908, SBx908 GEN2 or SBx8100 switch already has a version 5.4.8 license installed, that license also covers all later 5.4.8 versions. Such switches do not need a new license before upgrading to this version.

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 61 and
- “Licensing this Version on an SBx8100 Series Switch Control Card” on page 63.

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
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	07/2018	FS980-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	07/2018	GS900-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2018	GS970-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
XS916MXT XS916MXS	XS900MX	07/2018	XS900-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2018	IE200-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
IE300-12GT IE300-12GP	IE300	07/2018	IE300-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
IE210L-10GP IE210L-18GP	IE210L	07/2018	IE210-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
IE510-28GSX-80	IE500	07/2018	IE510-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
x220-28GS	x220	07/2018	x220-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT	x230	07/2018	x230-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2018	x310-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
IX5-28GPX	IX5	07/2018	IX5-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	07/2018	x510-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67

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

Models	Family	Date	Software File	GUI File
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2018	x550-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2018	x930-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
SBx908 GEN2	SBx908 GEN2	07/2018	SBx908NG-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
SBx908 (see Table 2)	SBx908	07/2018	SBx908-5.4.8-1.2.rel	SBx908-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	07/2018	SBx81CFC400-5.4.8-1.2.rel SBx81CFC960-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
AR4050S AR3050S	AR-series UTM firewalls	07/2018	AR4050S-5.4.8-1.2.rel AR3050S-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
AR2050V AR2010V	AR-series VPN firewalls	07/2018	AR2050V-5.4.8-1.2.rel AR2010V-5.4.8-1.2.rel	See "Accessing the web-based device GUI" on page 67
AMF Cloud		07/2018	vaa-5.4.8-1.2.iso (VAA OS) vaa-5.4.8-1.2. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.8-1.2.vhd (for Microsoft Azure)	

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.8-0.x and 5.4.8-1.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

Note that 5.4.8-1.x is the last supported software stream for the SwitchBlade x908. Version 5.4.8-2.x will not support the SwitchBlade x908.

Support for the SwitchBlade x908 GEN2 is ongoing.

Unsupported devices

Version 5.4.8-1.x does not support DC2552XS/L3 switches.

New Products

IE210L Series switches

Industrial-Lite Layer 2 Switches

The IE210L Series Gigabit Layer 2 switches are designed for enduring performance at high ambient temperatures.

The IE210L-10GP is a 10-port managed Layer 2 switch supporting PoE+, with 8 x 10/100/1000T ports and 2 x SFP slots.

The IE210L-10GP is an 18-port managed Layer 2 switch supporting PoE+, with 16 x 10/100/1000T ports and 2 x SFP slots.

For more information, see alliedtelesis.com/products/ie210l-series.

Web-based GUI Enhancements

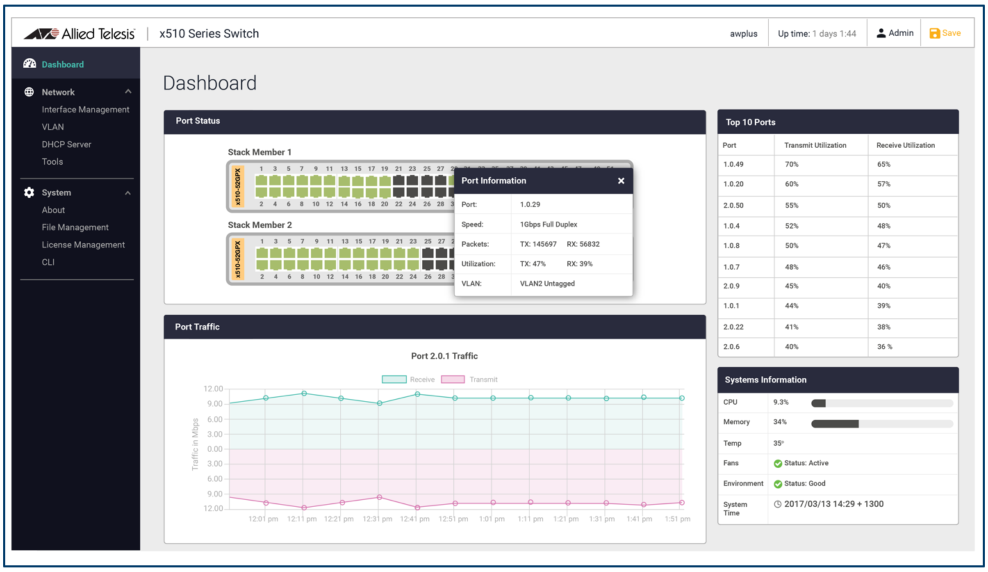
Allied Telesis has recently expanded our new web-based graphical user interface to support AlliedWare Plus switches, as well as AR-Series devices. On Allied Ware Plus switches, the web-based GUI replaces the previous Java-based GUI.

The GUI is a convenient tool for monitoring your device's status and performing basic management tasks and firewall set-up.

The August 2018 release of the GUI operates with 5.4.8-1.2 onwards and includes the following enhancements:

- Support for IE Series switches, SBx8100 Series switches, and SBx908 GEN2 switches. The GUI now supports all AlliedWare Plus devices[1].
- Autonomous Wave Control on SBx908 GEN2 switches, providing setup, monitoring, and automated optimization of your wireless network.
- Automatic setup of your wireless network with a single click. This is supported on AR-Series devices.

To obtain the new GUI, see "Accessing the web-based device GUI" on page 67.



Port Information

Port:	1.0.29
Speed:	1Gbps Full Duplex
Packets:	TX: 145697 RX: 56832
Utilization:	TX: 47% RX: 39%
VLAN:	VLAN2 Untagged

Top 10 Ports

Port	Transmit Utilization	Receive Utilization
1.0.49	70%	65%
1.0.20	60%	57%
2.0.50	55%	50%
1.0.4	52%	48%
1.0.8	50%	47%
1.0.7	48%	46%
2.0.9	45%	40%
1.0.1	44%	39%
2.0.22	41%	38%
2.0.6	40%	36 %

Systems Information

CPU	9.3%
Memory	34%
Temp	35°
Fans	✓ Status: Active
Environment	✓ Status: Good
System Time	2017/03/13 14:29 + 1300

[1] Except original SBx908 switches

New Features and Enhancements

This section summarizes the new features in 5.4.8-1.2 since 5.4.8-0.2:

- "Allied Telesis Autonomous Management Framework (AMF) enhancements" on page 38
- "Autonomous Wave Control (AWC) enhancements" on page 39
- "Software defined WAN (SD-WAN) and Application Awareness enhancements" on page 41
- "UTM Offload" on page 42
- "Enhancements when sending emails from the device" on page 43
- "Web redirect" on page 43
- "Port-protected bridge filtering" on page 44
- "DHCPv6 via PPPoE WAN" on page 44
- "Strict pairing for IPsec tunnels" on page 44
- "Increases in multicast support" on page 45
- "Single supplicant on multiple VLANs" on page 46
- "NTP updates" on page 47
- "G.8032 and Connectivity Fault Management (CFM) on SBx908 GEN2" on page 48
- "The OpenFlow protocol on IE210L and x230L Series switches" on page 48
- "VLAN ID translation on SBx8100 Series switches" on page 48
- "Secure Mode on x550 and XS900MX Series switches" on page 49
- "Multicast routing support for VRF-lite on SBx908 GEN 2 and x930 Series switches" on page 50

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 59.

Allied Telesis Autonomous Management Framework (AMF) enhancements

The Allied Telesis Autonomous Management Framework (AMF) is a suite of features that combine to simplify network management across all supported network equipment from the core to the edge.

AMF provides simplified device recovery and firmware upgrade management, enables you to manage your entire network from any AlliedWare Plus node within the network, enables you to configure multiple devices simultaneously, and makes it easy to add new devices into the network.

Version 5.4.8-1.2 includes the following AMF enhancements.

Support for TQ5403 as a guest node

From 5.4.8-1.2 onwards, the new TQ5403 Access Point is supported as a AMF guest node. You can use AMF to monitor TQ5403 status, backup their configuration, and manually restore the configuration if you need to replace a TQ5403.

VRF-lite interoperation with AMF and SES

From 5.4.8-1.2 onwards, VRF-lite interoperation with AMF and application proxy is supported. This means you can use VRF-lite and Secure Enterprise Software Defined Networking (SES) together.

Note that while VRF-lite and application proxy interoperate, you cannot use overlapping IP address ranges on your VRF instances. This is because SES uses IP addresses to determine when to take actions such as blocking a port. If different VRF instances have overlapping IP addresses, SES cannot determine which instance to act on and may block the wrong port or MAC address.

When using AMF with VRF-lite, the AMF subnet must be in the global VRF domain. The AMF subnet must not be assigned to any other VRF instance.

For information about VRF-lite, see the VRF Feature Overview and Configuration Guide.

Autonomous Wave Control (AWC) enhancements

Allied Telesis Autonomous Wave Control (AWC) manages your wireless network in a way that automatically minimizes coverage gaps and reduces Access Point (AP) interference. It delivers significant improvements in wireless network connectivity and performance, while reducing deployment and operating costs.

Version 5.4.8-1.2 includes the following AWC enhancements.

Easy AP installation with AWC on AR-Series devices

Setup of AWC Lite has been made easier with an auto-setup option to find and configure APs for initial deployment.

To use this, connect your APs to the AR-Series device and use the new command:

```
awplus#wireless auto-config create-new
```

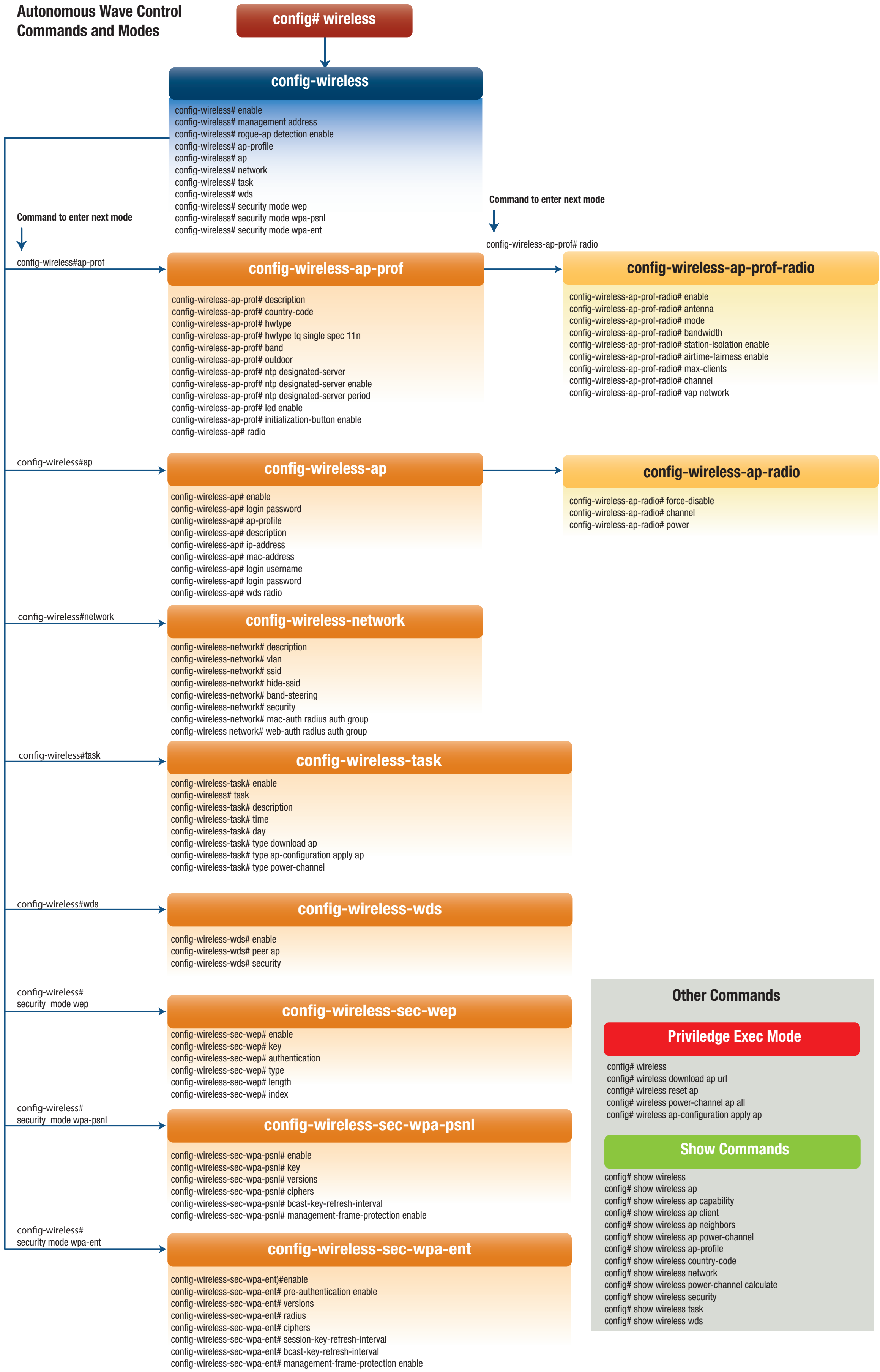
This enhancement will be supported in the Device GUI from August 2018.

For more information, see Getting Started with the Device GUI on VPN Routers or Getting Started with the Device GUI on UTM Firewalls.

AWC on SwitchBlade x908 GEN2

AWC is now available on the SBx908 GEN2, so you can use the SBx908 GEN2 to manage your wireless network. Configuration will be available in the Device GUI from August 2018, or you can use the command line, as summarized on the following page.

Figure 1: AWC Commands and Modes



Autonomous Wave Control Commands and Modes

config# wireless

config-wireless

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

Command to enter next mode

config-wireless#ap-prof

config-wireless-ap-prof

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

Command to enter next mode

config-wireless-ap-prof# radio

config-wireless-ap-prof-radio

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

config-wireless#ap

config-wireless-ap

config-wireless-ap# enable
config-wireless-ap# login password
config-wireless-ap# ap-profile
config-wireless-ap# description
config-wireless-ap# ip-address
config-wireless-ap# mac-address
config-wireless-ap# login username
config-wireless-ap# login password
config-wireless-ap# wds radio

config-wireless-ap-radio

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

config-wireless#network

config-wireless-network

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

config-wireless#task

config-wireless-task

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

config-wireless#wds

config-wireless-wds

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

config-wireless#
security mode wep

config-wireless-sec-wep

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

config-wireless#
security mode wpa-psnl

config-wireless-sec-wpa-psnl

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

config-wireless#
security mode wpa-ent

config-wireless-sec-wpa-ent

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

Other Commands

Priviledge Exec Mode

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

Show Commands

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

Software defined WAN (SD-WAN) and Application Awareness enhancements

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.

Version 5.4.8-1.2 includes the following SD-WAN enhancements.

- You can now use fully qualified domain name (FQDN) lookup for entities to match traffic used by firewall rules, traffic control rules, and PBR rules.

  This is achieved by allowing an entity to store a list of IP addresses that is dynamically updated from DNS. You create firewall entities that specify FQDNs. Then the IP addresses stored in the device's DNS cache (as A and AAAA records) that match the FQDNs are copied into the entity's IP address list for use during packet matching operations. This means the IP addresses associated with a particular Internet service will always be as up-to-date as the addresses that are provided by DNS for that service.
- Application-based aggregation now allows you to send traffic that matches a PBR rule across multiple SD-WAN link members at a time. If you have multiple redundant paths to your destination, you can utilize as much bandwidth of those paths as possible, while still being able to automatically redirect traffic away from links that are determined to be 'bad'.
- You can now use HTTP header requests for probing.

  These probes are intended for use when you have redundant ISP links to the internet and want to prioritize traffic to important cloud services. Traffic can be load balanced across both links automatically, and HTTP probing can be used to automatically fail all traffic over to a single ISP if the service becomes unreachable (or has unacceptable latency) via the other ISP.
- A new probe metric has been added for SD-WAN (linkmon) profiles: consecutive probe loss. This gives you similar functionality to ping-polling, allowing you to determine the availability of a device by sending ICMP packets. We recommend configuring linkmon profiles with this new metric, instead of the old metric of packet loss, which remains available.
- You can now configure triggers that respond to link health monitoring events, produced by a combination of a link health monitoring probe and profile.

  This configuration acts as a more powerful alternative to the already existing ping-poll triggers, because you can use the jitter and latency results from the probe to determine if the path to the destination IP address is bad or good, in addition to determining if the destination is up or down.
- You can now define the destination of a probe with an FQDN.
- The number of unique PBR routes you can create has been increased from 62 to 500.

- The maximum number of link-health monitoring probes you can configure has been restricted to 1000.

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

UTM Offload

Available on AR4050S

Version 5.4.8-1.2 adds support for the UTM Offload feature. UTM Offload improves WAN connection throughput when using multiple security and threat protection features together, or when higher performance is required.

UTM Offload improves the processing ability of the AR4050S by offloading some of its advanced security features to a second physical or virtual machine. This second machine is known as the offload device, and the AR4050S is referred to as the forwarding device.

The forwarding device (AR4050S) functions as a PXE boot server. PXE is short for Pre-Boot Execution Environment. Pronounced pixie, PXE allows a workstation to boot from a server on a network.

- The AR4050S network boots the offload device using PXE, configures the offload device, and then configures itself to send packets to the device.
- The AR4050S then uses the extra memory and CPU resources on the offload device to reduce its load, thereby increasing its performance.

What features can be offloaded?

Security features are configured as normal on the AR4050S device, but whenever UTM Offload is enabled, the following advanced threat protection features are offloaded, if they are configured:

- IPS
- IP-reputation
- Malware-protection
- URL-filtering

The AR4050S automatically manages the offload device for you. You don’t need to configure the second device, as configuration and the status of all features is presented the same whether offloaded or not.

For more information and a configuration example, see the UTM Offload Feature Overview and Configuration Guide.

Enhancements when sending emails from the device

Available on AR2010V, AR2050V, AR3050S, and AR4050S

From 5.4.8-1.2 onwards, you can configure optional authentication and port parameters for your SMTP server, as summarized below. For more detailed information, see the Mail (SMTP) Feature Overview and Configuration Guide.

SMTP server authentication options

Now you can configure your SMTP server with authentication options, by using the new command **mail smtpserver authentication** to add authentication to your SMTP server:

```
awplus(config)#mail smtpserver authentication [crammd5|login|
plain] username <username> password <password>
```

crammd5 is a Challenge Request Authentication Mechanism (CRAM-MD5) and is the most secure.

Each of these new parameters requires a username and password that are registered on your SMTP server.

SMTP server port options

You can now change the SMTP server port from the default port 25. The new command is:

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

Web redirect

Available on AR2010V, AR2050V, AR3050S, and AR4050S

Version 5.4.8-1.2 adds support for the Web Redirect feature. Web Redirect monitors HTTP requests passing through the device, intercepts the request, and replies with an HTTP Redirect message instructing the client to go to a specified URL.

This feature can be used in apartment buildings as part of the Internet gateway service for tenants. You could, for example, redirect users' web-browsers to a site that presents them with advertising information once in a given period. Or you could redirect users to a sign-in or payment page.

The following items can be configured for web redirect:

- The URL to redirect to
- How often each client should be redirected
- How long a client should be idle before they get redirected
- Exclusion lists for IP addresses and subnets
- Exclusion lists for MAC addresses and MAC OUID's/vendor codes
- Redirection of requests that come from hardware devices or system processes rather than web browsers.

Note: Web Redirect is supported for HTTP requests. Redirection of HTTPS is not supported.

For more information and a configuration example, see the Web Redirect Feature Overview and Configuration Guide.

Port-protected bridge filtering

Available on AR2010V, AR2050V, AR3050S, and AR4050S

From 5.4.8-1.2 onwards, it is possible for users to explicitly create internal bridge filters which limit the communication possible between devices attached to specific ports within a bridge.

If you need to block all communications between specific ports within a bridge, then this feature is easy to use and avoids the need for configuring complicated filters.

To enable port-protection on specific interface(s) within a bridge, use the **bridge-group** command with the optional **port-protected** parameter.

```
awplus(config-if)#bridge-group <1-255> port-protected
```

The port-protected parameter ensures that no (unicast, broadcast, or multicast) traffic is forwarded between specific port members within a bridge. Traffic will continue to be forwarded (Layer 2 bridged) between protected and unprotected members within a bridge.

Note that if the port-protected parameter is not used, then (by default) the port is added as an unprotected bridge port member.

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

DHCPv6 via PPPoE WAN

Available on AR2010V, AR2050V, AR3050S, and AR4050S

From 5.4.8-1.2 onwards, router PPPoE WAN interfaces can be configured as DHCPv6 prefix delegation clients.

When configured, PPP IPv6 Control Protocol negotiation occurs, and the IPv6 PPP link is established with link-local addressing only.

The router then requests allocation of a globally-scoped IPv6 prefix from the ISP router.

The dynamically learned IPv6 prefix is then stored within a named DHCPv6 prefix delegation pool, and is used to configure internal LAN interfaces with globally-scoped IPv6 address.

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

Strict pairing for IPsec tunnels

In IPsec, by default, if you specify multiple address selector pairs, the tunnel can permit any combination of matching sources and/or destinations. While this conforms to the RFC, it may not be the expected behavior and may cause the IPsec SA to either fail negotiation or fail to pass traffic correctly.

Version 5.4.8-1.2 adds a new optional command **tunnel selector paired**. This command forces ISAKMP to create individual Phase 2 IPsec SAs for each pair of source and destination selectors that have the same selector ID. Only traffic that matches a selector pair is permitted to flow via the associated SA.

For example, when creating a tunnel between 172.16.1.0/24 and 172.16.2.0/24, and also between 172.16.1.0/24 and any other destination, you can use the following tunnel selector commands:

```
awplus(config)#interface tunnel0
awplus(config-if)#tunnel local selector 2 172.16.1.0/24
awplus(config-if)#tunnel remote selector 2 172.16.2.0/24
awplus(config-if)#tunnel local selector 3 172.16.1.0/24
awplus(config-if)#tunnel remote selector 3 0.0.0.0/0
awplus(config-if)#tunnel selector paired
```

Increases in multicast support

Version 5.4.8-1.2 onwards includes the following increases:

- **SwitchBlade x908 GEN2 switches now support 1024 PIM interfaces.**
- **SwitchBlade x908 GEN2 switches now support 8192 multicast groups.**

  This can be 8192 of any combination of (*,G) and (S,G) entries.
- **SwitchBlade x8100 systems containing SBx81CFC960 and SBx81XLEM cards now support 8192 multicast groups.**

  This can be 8192 of any combination of (*,G) and (S,G) entries. To support 8192 multicast groups on the SwitchBlade x8100, you also need to change to silicon-profile 3 with a routing ratio weighting of multicast. Use the commands:

  ```
  awplus(config)#platform silicon-profile profile3
  awplus(config)#platform routingratio ipv4andipv6 weighting multicast
  ```
- **AR4050S and AR3050S now support 2048 (*,G) and 2048 (S,G) multicast groups.**

Increasing performance in large networks

Version 5.4.8-1.2 also introduces configuration changes on the SBx8100 and SBx908 GEN2 that may help increase performance of large Layer 3 multicast networks:

- ip multicast-routing [vrf <*vrf-name*>] ssm-only-hw

  Use this command in global configuration mode to suppress the creation of the (*,G) entries in hardware, but not suppress the (S,G) entries. This command prevents a large number of (*,G) entries from being created in hardware, which improves the performance when there are many multicast groups with many downstream interfaces. (*,G) entries will still be created as needed in the CPU.

  However, using this command may cause multicast data to be briefly flooded on the incoming interface, if it comes from interfaces other than the “correct” incoming interface. The “correct” incoming interface is determined by Unicast Reverse Path Forwarding (uRPF).
- SBx8100, SBx908 GEN2 and x930 Series now send multicast packets to the CPU at a maximum rate of 100 packets per second by default, instead of the previous limit of 10 pps. If you want to reduce the CPU load on your switch, you can reduce this rate by using the following command:

```
awplus(config)#platform multicast-ratelimit <0-100>
```

For more information about large PIM networks, see the PIM-SM Feature Overview and Configuration Guide.

Single supplicant on multiple VLANs

Available on all AlliedWare Plus switches

From 5.4.8-1.2 onwards, AlliedWare Plus supports packet forwarding on multiple VLANs for an authenticated supplicant attached to a trunked (tagged VLAN) port.

By default, AlliedWare Plus only allows packet forwarding on the VLAN that a device was authenticated on. This enhancement allows packet forwarding to the attached device on any VLAN configured on the switchport. After the device authenticates it will have access to all VLANs configured on the switchport.

To enable this enhancement, use the new **auth multi-vlan-session** command on a trunked (tagged VLAN) port. You can also use it in Authentication Profile mode.

The following example allows packet forwarding on vlan1 (the native vlan), vlan20 and vlan30 for authenticated devices on port2.0.26.

```
radius-server host 192.168.1.40 key test

 aaa authentication dot1x default group radius

 interface port2.0.26
  switchport
  switchport mode trunk
  switchport trunk allowed vlan add 20,30
  dot1x port-control auto
  dot1x control-direction in
  auth host-mode multi-supplicant
  auth multi-vlan-session
```

NTP updates

Available on all AlliedWare Plus devices.

Version 5.4.8-1.2 changes some of the commands used for configuring NTP, as described below. For more information about configuring NTP, see the NTP Feature Overview and Configuration Guide.

New command `ntp rate-limit`

Use this command to enable response rate limiting for NTP packets. Its purpose is to reduce network traffic from misconfigured or broken NTP clients that are polling the server too frequently.

Modified command `ntp restrict`

Some parameters for the ntp restrict command have been changed, as shown in the following table (using 192.168.1.0/24 as an example subnet):

Table 3: Replacement parameters for the **ntp restrict** command

Existing Options	New Options
ntp restrict 192.168.1.0/24	ntp restrict 192.168.1.0/24 allow
ntp restrict 192.168.1.0/24 ignore	ntp restrict 192.168.1.0/24 deny
ntp restrict 192.168.10.1 noquery	ntp restrict 192.168.10.1 query deny
ntp restrict 192.168.20.0/24 noserve	ntp restrict 192.168.20.0/24 serve deny

If your device configuration contains a changed option, it will be converted to the new option when you upgrade.

Some parameters have been obsoleted rather than changed. These are: limited, kod, nomodify, nopeer, notrust.

If your device configuration contains an obsoleted option, that option will be discarded with a warning message.

Obsoleted commands `ntp discard` (replaced by the new **ntp rate-limit** command)

`ntp authenticate` (authentication is now enabled for the NTP service by default)

Updated show commands `show ntp status`

`show ntp associations` (**jitter** parameter replaced by **disp** (dispersion) parameter)

`show ntp counters`

G.8032 and Connectivity Fault Management (CFM) on SBx908 GEN2

Version 5.4.8-1.2 adds support for G.8032 ring protection on Connectivity Fault Management (CFM) on SwitchBlade x908 GEN2 switches. 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.

The OpenFlow protocol on IE210L and x230L Series switches

From 5.4.8-1.2 onwards, AlliedWare Plus supports version 1.3 of the OpenFlow protocol on IE210L and x230L Series switches. A number of other AlliedWare Plus switches already support the OpenFlow protocol.

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 SBx8100 Series switches

From 5.4.8-1.2 onwards, AlliedWare Plus supports VLAN ID translation on SBx8100 Series switches. A number of other AlliedWare Plus switches already support VLAN ID Translation.

VLAN ID translation translates a VLAN’s VLAN ID to another value for use on the wire.

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

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

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

Note that if you configure VLAN ID translation on a port on an SBx81GT40, SBx81XS16 or SBx81CFC960 card, and then mirror that port's traffic, the mirrored traffic may have the original VLAN instead of the translated VLAN. This applies to both port mirroring (on the same switch) and remote mirroring, but only affects the mirrored copy. The original traffic will correctly egress its port with the translated VLAN.

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

Secure Mode on x550 and XS900MX Series switches

Newly available on x550 and XS900MX Series switches. Available in previous releases on x930 Series switches

Version 5.4.8-1.2 supports Secure Mode on x550 and XS900MX Series switches. When in Secure Mode, the following are disabled:

- Telnet
- SSHv1
- SNMPv1/v2
- All privilege levels except 1 and 15
- Algorithms that are not supported under FIPS, including MD5, RSA-1 and DSA
- The ability to store passwords in cleartext and to specify an **enable** password

In Secure Mode, the web server on the switch (used by the Device GUI) only accepts AES128-SHA ciphers.

Entering Secure Mode

1. Obtain the correct release file and its sha256sum file, for example by downloading them from the Allied Telesis Download Center. Save the files on a trusted USB device and connect the USB device to the switch.

2. Before entering Secure Mode, erase the Flash. To do this, boot the device into the bootloader diagnostics menu, using Ctrl-D. Select option 7 'Bootup stage 2 diagnostics menu', and then select option 4 'Erase FLASH (Filesystem only)'.

3. Then select option 0 'Restart' to reboot the device. Enter the main bootloader menu by using Ctrl-B. Select option 1 'Perform one-off boot from alternate source' and then select the 'USB' option and the release you saved in step 1.

4. Once the switch has booted up, save the release file to Flash and verify it, as described in "Verifying the Release File" on page 60.

5. Set the verified release as the boot release. For example, use the following commands:

```
awplus#configure terminal
```

```
awplus(config)#boot system x550-5.4.8-1.2.rel
```

6. Use the following commands to enter secure mode:

```
awplus(config)# crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

7. Use the following command to confirm that the switch is in secure mode:

```
awplus# show secure-mode
```

The following message should be displayed:

```
Secure mode is enabled
```

Leaving Secure Mode

1. If you wish to leave Secure Mode, you should delete all sensitive information first. This means deleting all trustpoints (one by one), by using the commands:

```
awplus# configure terminal
awplus(config)# no crypto pki trustpoint <name>
```

Also, delete all public/private key pairs, by using the commands:

```
awplus# crypto key zeroize all
```

2. Turn off Secure Mode, by using the commands:

```
awplus(config)# no crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

3. Reboot the switch. The switch ***must*** be rebooted after Secure Mode is turned off, and ideally Flash memory should be erased via the bootloader, as described above.

Multicast routing support for VRF-lite on SBx908 GEN 2 and x930 Series switches

Newly available on SBx908 GEN 2 and x930 Series switches. Available in previous releases on SBx8100 Series switches running SBx81CFC960 control cards.

Version 5.4.8-1.2 extends support for VRF-lite to include multicast routing on SBx908 GEN 2 and x930 Series switches. You can now configure IGMP and PIM Sparse Mode on individual VRF-lite instances.

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

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

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

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:

- Spurious log message on failover or hotswap on SBx8100 Series switches
- Device GUI files synchronized across stack members
- Limits for AWC neighbor show commands
- Parameter name change for provisioning SwitchBlade x908 GEN2 switches
- Increase to rate at which multicast packets are sent to the CPU
- Delay at startup before connecting to remote log hosts
- 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
- 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

Spurious log message on failover or hotswap on SBx8100 Series switches

Applies to SBx8100 Series switches

From 5.4.8-1.2 onwards, on CFC failover or linecard hotswap, an error level message like the following will be logged on the (new) active CFC:

"CMSG(1061).platform.n.tipc[18]: Subscriber is not reachable after 10 tries and will be removed."

This message is expected and can be safely ignored.

Device GUI files synchronized across stack members

Applies to AlliedWare Plus switches that support VCStack

From 5.4.8-1.2 onwards, the Device GUI file is automatically synchronized to backup stack members, so they can use the GUI if the stack master reboots.

Limits for AWC neighbor show commands

Applies to AR-Series devices and SBx908 GEN2 switches

From 5.4.8-1.2 onwards, if the total number of Access Point (AP) neighbors in the system exceeds 12500, the following commands will only show the first 12500 neighbors:

- show wireless ap neighbors
- show wireless ap all neighbors

You can specify the AP ID to see all neighbors of each AP.

Parameter name change for provisioning SwitchBlade x908 GEN2 switches

Applies to SBx908 GEN2 switches

From 5.4.8-1.2 onwards, the command for provisioning an SBx908 GEN2 stack member has changed. It is now:

```
awplus(config)#switch <stack-ID> provision sbx908gen2
```

If you upgrade to 5.4.8-1.2 or later and your configuration file includes the previous syntax, AlliedWare Plus will automatically update it to the new syntax.

However, if you upgrade and then later downgrade to 5.4.8-0.x or earlier, your configuration file will keep the new syntax, which the switch will not recognize. After such a downgrade, provisioning also wouldn’t be applied for any provisioned XEMs, because they depend on the switch provisioning, and configuration wouldn’t be applied on provisioned interfaces. You would see error messages to warn you of this.

Increase to rate at which multicast packets are sent to the CPU

SBx8100, SBx908 GEN2 and x930 Series now send multicast packets to the CPU at a maximum rate of 100 packets per second by default, instead of the previous limit of 10 pps. If you want to reduce the CPU load on your switch, you can reduce this rate by using the following command:

```
awplus(config)#platform multicast-ratelimit <0-100>
```

Delay at startup before connecting to remote log hosts

Applies to all AlliedWare Plus devices

When the device boots up, there is a delay before it attempts to connect to remote log hosts. This is to allow time for the device to establish network connectivity to the remote host. During this period, the device buffers log messages and sends them once it has connected to the remote host.

From version 5.4.8-0.2 onwards, this delay is active by default and can't be turned off, and the default delay has been increased. The delay also now applies to event hosts.

The command to configure the delay is:

```
awplus(config)#log host startup-delay [delay <1-600>]
[messages <1-5000>]
```

By default the system will buffer up to 2000 messages and wait 120s from when syslog starts before attempting to filter and transmit the buffered messages to remote hosts. If the default startup delay is not long enough for the boot and configuration process to complete and the links to come up, you may see logging failure messages on startup. In such cases, you can use the command to increase the startup delay.

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 5.4.8-1.2 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.

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 61 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 63.

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.

The tables of Issues Resolved in this release contain the following ISSU information:

- 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.

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

	To Release						
FROM	**Release**	**5.4.8-1.2**	**5.4.8-1.3**	**5.4.8-1.4**	**5.4.8-1.5**	**5.4.8-1.6**	
	5.4.8-1.1	C	I	I	I	I	
	5.4.8-1.2		C	I	I	I	
	5.4.8-1.3			C	I	I	
	5.4.8-1.4				C	I	
	5.4.8-1.5					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 5.4.8-1.x from:

- 5.4.8-0.x, or
- 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 5.4.8-1.x from 5.4.4-0.x or earlier versions.

Forming or extending a VCStack with auto-synchronization

Applies to all stackable AlliedWare Plus switches

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up. Auto-synchronization is supported between 5.4.8-1.x and:

- 5.4.8-0.x
- 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 5.4.8-1.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 5.4.8-1.x are compatible with nodes running:

- 5.4.8-0.x
- 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.

Firewall rules needed to allow access to external services

Applies to AR4050S, AR3050S, AR2050V and AR2010V

You need to create firewall rules 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

You can create rules for each individual type of traffic, or a single rule to cover all traffic generated by the firewall that is destined for external services. For information about how to create the rules, see the "Configuring Firewall Rules for Required External Services" section in the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

Verifying the Release File

On x930, x550 and XS900MX 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 release's sha256sum file, which is available from the Allied Telesis Download Center.

Caution

If the verification fails, the following error message will be generated:
"% Verification Failed"
In the case of verification failure, please delete the release file and contact Allied Telesis support.

All switch models of a particular series run the same release file and therefore have the same checksum. For example, all x930 Series switches 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 61 and
- "Licensing this Version on an SBx8100 Series Switch Control Card" on page 63.

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 FS980-5.4.8-1.6.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.4.8-1.6.rel`
GS970M series	`awplus(config)# boot system GS970-5.4.8-1.6.rel`
XS900MX series	`awplus(config)# boot system XS900-5.4.8-1.6.rel`
x230 series	`awplus(config)# boot system x230-5.4.8-1.6.rel`
IE200 series	`awplus(config)# boot system IE200-5.4.8-1.6.rel`
IE210L series	`awplus(config)# boot system IE210-5.4.8-1.6.rel`
x310 series	`awplus(config)# boot system x310-5.4.8-1.6.rel`
IE300 series	`awplus(config)# boot system IE300-5.4.8-1.6.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.8-1.6.rel`
x510 series	`awplus(config)# boot system x510-5.4.8-1.6.rel`
x550 series	`awplus(config)# boot system x550-5.4.8-1.6.rel`

Product	Command
IE510-28GSX	`awplus(config)# boot system IE510-5.4.8-1.6.rel`
x550 series	`awplus(config)# boot system x550-5.4.8-1.6.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.8-1.6.rel`
SBx908 GEN2	`awplus(config)# boot system SBx908NG-5.4.8-1.6.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.8-1.6.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.8-1.6.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.8-1.6.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.4.8-1.6.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.8-1.6.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.8-1.6.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.8-1.6.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 available for AR-Series UTM firewalls and VPN routers, and AlliedWare Plus switches[1].

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 SBx908 GEN switches and AR-Series devices, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

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*.

[1] Except original SBx908 switches

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, where x is a digit.

   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 (where x is a digit):

   ```
   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.*