Allied Telesis™

Release Note for AlliedWare Plus Software Version 5.4.7-0.x

AlliedWare Plus OPERATING SYSTEM

» SBx8100 Series » SBx908 » DC2552XS/L3 » x930 Series
» x610 Series » x510 Series » IX5 » x310 Series » x230 Series
» x210 Series » IE500 Series » IE300 Series » IE200 Series
» XS900MX Series » GS970MX Series » GS900MX/MPX Series
» FS980M Series » AMF Cloud
» AR2010V » AR2050V » AR3050S » AR4050S

5.4.7-0.4 » 5.4.7-0.3 » 5.4.7-0.2 » 5.4.7-0.1

Acknowledgments

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

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

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

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

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

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

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

Getting the most from this Release Note

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

Content

New Features in Version 5.4.7-0.4

For:
SwitchBlade x8100 Series
SwitchBlade x908
DC2552XS/L3
x930 Series
x610 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x210 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AR4050S
AR3050S
AR2050V
AR2010V

Introduction

This release note describes the new features and enhancements in AlliedWare Plus 5.4.7-0.4. For more information, see the Command Reference for your switch or AR-series firewall. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.

⚠ **Caution: Software version 5.4.7-0.4 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.7-0.4 license certificate before you upgrade.**

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	06/2017	GS900-5.4.7-0.4.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	06/2017	FS980-5.4.7-0.4.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M *available Sept 2017	06/2017	GS970-5.4.7-0.4.rel	coming soon
XS916MXT XS916MXS	XS900MX	06/2017	XS900-5.4.7-0.4.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	06/2017	IE200-5.4.7-0.4.rel	ie200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	06/2017	IE300-5.4.7-0.4.rel	ie300-gui_547_02.jar
IE510-28GSX-80	IE500	06/2017	IE510-5.4.7-0.4.rel	IE510-gui_547_01.jar
x210-9GT x210-16GT x210-24GT	x210	06/2017	x210-5.4.7-0.4.rel	x210-gui_547_02.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	06/2017	x230-5.4.7-0.4.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	06/2017	x310-5.4.7-0.4.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	06/2017	IX5-5.4.7-0.4.rel	IX5-gui_547_01.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	06/2017	x510-5.4.7-0.4.rel	x510-gui_547_01.jar

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
x610-24Ts x610-24Ts-PoE+ x610-24Ts/X x610-24Ts/X-PoE+ x610-24SPs/X x610-48Ts x610-48Ts-PoE+ x610-48Ts/X x610-48Ts/X-PoE+	x610	06/2017	x610-5.4.7-0.4.rel	x610-gui_547_01.jar
SBx908 (see Table 2)	SBx908	06/2017	SBx908-5.4.7-0.4.rel	SBx908-gui_547_01.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	06/2017	x930-5.4.7-0.4.rel	x930-gui_547_01.jar
DC2552XS/L3		06/2017	dc2500-5.4.7-0.4.rel	dc2500-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	06/2017	SBx81CFC400-5.4.7-0.4.rel SBx81CFC960-5.4.7-0.4.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_02.jar
AR4050S AR3050S	AR-series UTM firewalls	06/2017	AR4050S-5.4.7-0.4.rel AR3050S-5.4.7-0.4.rel	See "Accessing the AR-Series Firewall GUI" on page 58
AR2050V AR2010V	AR-series VPN firewalls	06/2017	AR2050V-5.4.7-0.4.rel AR2010V-5.4.7-0.4.rel	See "Accessing the AR-Series Firewall GUI" on page 58
AMF Cloud		06/2017	vaa-5.4.7-0.4.iso (VAA OS) vaa-5.4.7-0.4. vhd and upload_vhd.py (for AWS) vaa_azure-5.4.7-0.4.vhd (for Microsoft Azure)	

Under version 5.4.7, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.7.

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

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

Caution: Using a software version file for the wrong switch or AR-series firewall model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

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.

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

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

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

	To Release				
From	**Release**	**5.4.7-0.1**	**5.4.7-0.2**	**5.4.7-0.3**	**5.4.7-0.4**
	5.4.7-0.1		I	I	
	5.4.7-0.2			C	
	5.4.7-0.3				C

Additional information

For more information about ISSU, see the ISSU Commands chapter in the SwitchBlade x8100 Series Command Reference for AlliedWare Plus.

ISSU is not supported on other platforms.

You may also find the following How To Note useful:

- How to Use the In-Service Software Upgrade (ISSU) Feature

New Features and Enhancements

This section summarizes the new features in 5.4.7-0.4.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 50.

Change in default start-up behavior

Available on all AlliedWare Plus devices

From AlliedWare Plus version 5.4.7-0.4 onwards, unconfigured devices automatically receive a management IP address on start-up, without any manual configuration. You can optionally set up a DHCP server on your network and have the device obtain an address via DHCP, or otherwise the device uses an IP address of 169.254.42.42.

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

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

AR-Series Firewalls are typically pre-configured at the factory. Therefore the new start-up behavior does not apply to them unless you manually return them to an unconfigured state by using the command **erase factory-default**.

What is an unconfigured device?

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

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

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

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

What is the management interface?

The management interface depends on the interfaces available on the device.

It is:

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

How the new start-up process works

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

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

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

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

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

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

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

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

Configured commands

The following commands are configured:

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

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

```
interface <management-interface>
 ip address 169.254.42.42/16
 ipv6 address dhcp
```

Further details about the new start-up behavior

Additional notes about the start-up process:

- The process will stop if either of the following events occur during start-up:
  - configuration changes are made by logging in via a console port (see "Configuring the device by the console" on page 9 for details).
  - AMF zero-touch recovery begins. The new start-up process does not stop AMF from treating the device as a clean device and initiating zero-touch recovery.
- Other than the configuration changes specified above, the factory configuration remains unchanged, so protocols such as RSTP remain in their default state.
- On a stack, this new behavior will only be executed on the Stack Master.
- The configuration changes are not automatically saved, so rebooting the device without saving the configuration will trigger the same behavior again.
- The device broadcasts DHCP messages. If the device is attached to existing network infrastructure via multiple switchports, and the existing equipment does not support STP, then there is the potential for a broadcast storm. To ensure loop-free operation with this feature, AlliedWare Plus devices have RSTP enabled by default. Additionally, the Loop Protection feature is now automatically enabled during start-up on devices that support it.
- If using a DHCP or DHCPv6 server for address allocation, we recommend you configure the server to allocate a static IPv4 or IPv6 address binding based on the MAC address of the device. This ensures you know which management address to SSH to.

Setting up a number of devices

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

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

Preventing the New Start-up Behavior

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

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

The following sections describe these options in detail.

Adding an autoboot file

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

Configuring the device by the console

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

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

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

Monitoring

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

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

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

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

New Features in Version 5.4.7-0.3

For:
SwitchBlade x8100 Series
SwitchBlade x908
DC2552XS/L3
x930 Series
x610 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x210 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AMF Cloud
AR4050S
AR3050S
AR2050V
AR2010V

Introduction

This release note describes the new features and enhancements in AlliedWare Plus 5.4.7-0.3. For more information, see the Command Reference for your switch or AR-series firewall. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.

Caution: Software version 5.4.7-0.3 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.7-0.3 license certificate before you upgrade.

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	03/2017	GS900-5.4.7-0.3.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	03/2017	FS980-5.4.7-0.3.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M *available Sept 2017	03/2017	GS970-5.4.7-0.3.rel	coming soon
XS916MXT XS916MXS	XS900MX	03/2017	XS900-5.4.7-0.3.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2017	IE200-5.4.7-0.3.rel	ie200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	03/2017	IE300-5.4.7-0.3.rel	ie300-gui_547_02.jar
IE510-28GSX-80	IE500	03/2017	IE510-5.4.7-0.3.rel	IE510-gui_547_01.jar
x210-9GT x210-16GT x210-24GT	x210	03/2017	x210-5.4.7-0.3.rel	x210-gui_547_02.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	03/2017	x230-5.4.7-0.3.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2017	x310-5.4.7-0.3.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	03/2017	IX5-5.4.7-0.3.rel	IX5-gui_547_01.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	03/2017	x510-5.4.7-0.3.rel	x510-gui_547_01.jar

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
x610-24Ts x610-24Ts-PoE+ x610-24Ts/X x610-24Ts/X-PoE+ x610-24SPs/X x610-48Ts x610-48Ts-PoE+ x610-48Ts/X x610-48Ts/X-PoE+	x610	03/2017	x610-5.4.7-0.3.rel	x610-gui_547_01.jar
SBx908 (see Table 2)	SBx908	03/2017	SBx908-5.4.7-0.3.rel	SBx908-gui_547_01.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2017	x930-5.4.7-0.3.rel	x930-gui_547_01.jar
DC2552XS/L3		03/2017	dc2500-5.4.7-0.3.rel	dc2500-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	03/2017	SBx81CFC400-5.4.7-0.3.rel SBx81CFC960-5.4.7-0.3.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_02.jar
AR4050S AR3050S	AR-series UTM firewalls	03/2017	AR4050S-5.4.7-0.3.rel AR3050S-5.4.7-0.3.rel	See "Accessing the AR-Series Firewall GUI" on page 58
AR2050V AR2010V	AR-series VPN firewalls	03/2017	AR2050V-5.4.7-0.3.rel AR2010V-5.4.7-0.3.rel	See "Accessing the AR-Series Firewall GUI" on page 58
AMF Cloud		03/2017	vaa-5.4.7-0.3.iso	n/a

Under version 5.4.7, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.7.

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

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

Caution: Using a software version file for the wrong switch or AR-series firewall model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

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.

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

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

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

	To Release			
From	Release	5.4.7-0.1	5.4.7-0.2	5.4.7-0.3
	5.4.7-0.1		I	I
	5.4.7-0.2			C

Additional information

For more information about ISSU, see the ISSU Commands chapter in the SwitchBlade x8100 Series Command Reference for AlliedWare Plus.

ISSU is not supported on other platforms.

You may also find the following How To Note useful:

- How to Use the In-Service Software Upgrade (ISSU) Feature

New Features and Enhancements

This section summarizes the new features in 5.4.7-0.3.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 50.

AMF Secure Mode

Available on all AlliedWare Plus devices that support AMF.

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

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

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

Other Enhancements

CR	Module	Description
ER-1226	**Firewall**	For: AR2010V, AR2050V, AR3050s, AR4050s. With this software update, a new command has been added: **http secure-port <1-65535>** When configured, this allows the Firewall GUI on Routers to be accessed through an HTTPS port other than the default 443. All other external RESTful API operations must also be directed to this configured port.
ER-1248	**QoS** **Hardware**	For: XS900MX With this software update, the XS900 series switch will now support IPv6 Hardware ACLs..

New Features in Version 5.4.7-0.2

For:
SwitchBlade x8100 Series
SwitchBlade x908
DC2552XS/L3
x930 Series
x610 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x210 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
GS970M Series
FS980M Series
AMF Cloud
AR4050S
AR3050S
AR2050V
AR2010V

Introduction

This release note describes the new features and enhancements in AlliedWare Plus 5.4.7-0.2. For more information, see the Command Reference for your switch or AR-series firewall. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.

Caution: Software version 5.4.7-0.2 requires a release license for the SBx908 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.4.7-0.2 license certificate before you upgrade.

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

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

Note: This software release is not ISSU compatible.

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	03/2017	GS900-5.4.7-0.2.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	03/2017	FS980-5.4.7-0.2.rel	FS980-gui_547_01.jar
GS970M/10PS* GS970M/10 GS970M/18PS* GS970M/18 GS970M/28PS* GS970M/28	GS970M *available Sept 2017	03/2017	GS970-5.4.7-0.2.rel	coming soon
XS916MXT XS916MXS	XS900MX	03/2017	XS900-5.4.7-0.2.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2017	IE200-5.4.7-0.2.rel	ie200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	03/2017	IE300-5.4.7-0.2.rel	ie300-gui_547_02.jar
IE510-28GSX-80	IE500	03/2017	IE510-5.4.7-0.2.rel	IE510-gui_547_01.jar
x210-9GT x210-16GT x210-24GT	x210	03/2017	x210-5.4.7-0.2.rel	x210-gui_547_02.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	03/2017	x230-5.4.7-0.2.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2017	x310-5.4.7-0.2.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	03/2017	IX5-5.4.7-0.2.rel	IX5-gui_547_01.jar

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
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	03/2017	x510-5.4.7-0.2.rel	x510-gui_547_01.jar
x610-24Ts x610-24Ts-PoE+ x610-24Ts/X x610-24Ts/X-PoE+ x610-24SPs/X x610-48Ts x610-48Ts-PoE+ x610-48Ts/X x610-48Ts/X-PoE+	x610	03/2017	x610-5.4.7-0.2.rel	x610-gui_547_01.jar
SBx908 (see Table 2)	SBx908	03/2017	SBx908-5.4.7-0.2.rel	SBx908-gui_547_01.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2017	x930-5.4.7-0.2.rel	x930-gui_547_01.jar
DC2552XS/L3		03/2017	dc2500-5.4.7-0.2.rel	dc2500-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	03/2017	SBx81CFC400-5.4.7-0.2.rel SBx81CFC960-5.4.7-0.2.rel	SBx81CFC400-gui_547_02.jar SBx81CFC960-gui_547_02.jar
AR4050S AR3050S	AR-series UTM firewalls	03/2017	AR4050S-5.4.7-0.2.rel AR3050S-5.4.7-0.2.rel	See “Accessing the AR-Series Firewall GUI” on page 58
AR2050V AR2010V	AR-series VPN firewalls	03/2017	AR2050V-5.4.7-0.2.rel AR2010V-5.4.7-0.2.rel	See “Accessing the AR-Series Firewall GUI” on page 58
AMF Cloud		03/2017	vaa-5.4.7-0.2.iso	n/a

Under version 5.4.7, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.7.

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

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

Product	Supported in version 5.4.7-x.x
XEM-12T	No
XEM-12Sv2	Yes
XEM-12Tv2	Yes
XEM-24T	Yes

Caution: Using a software version file for the wrong switch or AR-series firewall model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

New Products

AlliedWare Plus version 5.4.7-0.2 supports the following recently-released products.

CentreCOM GS970M

The CentreCOM GS970M Series of Layer 3 switches provide high performance with gigabit to the desktop, the ability to connect and power endpoints, and lower management costs—a high value network edge solution from Allied Telesis.

Overview

- Reduce costs and automate network and device management with the Allied Telesis Management Framework (AMF)
- Flexible deployment with 10, 18 and 28 port models
- High-speed gigabit network access for power users
- Support converged networks with PoE+ to power devices like wireless access points, digital surveillance cameras and IP phones (available June 2017)

For more information, see alliedtelesis.com/products/switches/gs970m-series.

New Features and Enhancements

This section summarizes the new features in 5.4.7-0.2.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 50.

4G/LTE USB Cellular Modem Support

Available on AR-Series Firewalls

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

The 4G cellular interface supports the following features:

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

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

Other Enhancements

CR	Module	Description
ER-1134	**User Management**	For: FS980M, GS900MX/MPX, GS970M, XS900MX, IE200, IE300, IE500, x210, x230, x310, IX5, x510, x610, x930, DC2552XS/L3, SBx908, SBx81CFC400, SBx81CFC960, AR2010V, AR2050V, AR3050S, AR4050S, AMF Cloud With this software update, a new command is added to configure the minimum interval a password can be changed by a user. With this command enabled, once a user sets the password the user cannot change it again for a minimum of 1 day and a maximum of 1000 days. This restriction can be enabled using the following command: **security-password min-lifetime-enforce <0-1000>** And, can be disabled using: **no security-password min-lifetime-enforce**

ER-1210	**DHCP Client**	For: FS980M, GS900MX/MPX, GS970M, XS900MX, IE200, IE300, IE500, x210, x230, x310, IX5, x510, x610, x930, SBx908, SBx81CFC400, SBx81CFC960, AR2010V, AR2050V, AR3050S, AR4050S, AMF Cloud With this software update, the command "ip dhcp-client default-route distance <1-255>" is now supported. This command allows the user to change the Administrative Distance of a default gateway route learned via a DHCP client interface. Previously, when an interface (such as a vlan, or an AR-Series Firewall ethernet, or 4G) was operating as a DHCP client and learned gateway information via DHCP, then an associated default route was added to the RIB with an Administrative Distance (AD) of 1. This enhancement allows the user to modify the AD of the default route to a non-default value. This is useful if the interface operating as a DHCP client is being used to provide backup WAN connectivity, as it ensures any pre-existing default routes out other (primary) interfaces which have a higher AD cost value (AD>1) to continue to be used when the DHCP client interface becomes active.
ER-1287	**GUI**	For: FS980M, GS900MX/MPX, GS970M, XS900MX, IE200, IE300, IE500, x210, x230, x310, IX5, x510, x610, x930, DC2552XS/L3, SBx908, SBx81CFC400, SBx81CFC960, AR2010V, AR2050V, AR3050S, AR4050S With this software update, the GUI file selection algorithm has now been improved to ensure the GUI file with the highest compatible firmware version, and the highest GUI version, is always chosen.

New Features in Version 5.4.7-0.1

For:
SwitchBlade x8100 Series
SwitchBlade x908
DC2552XS/L3
x930 Series
x610 Series
x510 Series
IX5-28GPX
x310 Series
x230 Series
x210 Series
IE510-28GSX-80
IE300 Series
IE200 Series
XS900MX Series
GS900MX/MPX Series
FS980M Series
AMF Cloud
AR4050S
AR3050S
AR2050V
AR2010V

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.4.7-0.1. For more information, see the Command Reference for your switch or AR-series firewall. Software file details for this version are listed in Table 1 below.

You can obtain the software files from the Software Download area of the Allied Telesis website. Log in using your assigned email address and password.

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

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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/ MPX	03/2017	GS900-5.4.7-0.1.rel	GS900-gui_547_01.jar
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	03/2017	FS980-5.4.7-0.1.rel	FS980-gui_547_01.jar
XS916MXT XS916MXS	XS900MX	03/2017	XS900-5.4.7-0.1.rel	XS900-gui_547_01.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	03/2017	IE200-5.4.7-0.1.rel	ie200-gui_547_01.jar
IE300-12GT IE300-12GP	IE300	03/2017	IE300-5.4.7-0.1.rel	ie300-gui_547_01.jar
IE510-28GSX-80	IE500	03/2017	IE510-5.4.7-0.1.rel	IE510-gui_547_01.jar
x210-9GT x210-16GT x210-24GT	x210	03/2017	x210-5.4.7-0.1.rel	x210-gui_547_01.jar
x230-10GP x230-18GP x230-18GT x230-28GP x230-28GT	x230	03/2017	x230-5.4.7-0.1.rel	x230-gui_547_01.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	03/2017	x310-5.4.7-0.1.rel	x310-gui_547_01.jar
IX5-28GPX	IX5	03/2017	IX5-5.4.7-0.1.rel	IX5-gui_547_01.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	03/2017	x510-5.4.7-0.1.rel	x510-gui_547_01.jar

Table 1: Models and software file names

Models	Family	Date	Software File	GUI File
x610-24Ts x610-24Ts-PoE+ x610-24Ts/X x610-24Ts/X-PoE+ x610-24SPs/X x610-48Ts x610-48Ts-PoE+ x610-48Ts/X x610-48Ts/X-PoE+	x610	03/2017	x610-5.4.7-0.1.rel	x610-gui_547_01.jar
SBx908 (see Table 2)	SBx908	03/2017	SBx908-5.4.7-0.1.rel	SBx908-gui_547_01.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	03/2017	x930-5.4.7-0.1.rel	x930-gui_547_01.jar
DC2552XS/L3		03/2017	dc2500-5.4.7-0.1.rel	dc2500-gui_547_01.jar
SBx81CFC400 SBx81CFC960	SBx8100	03/2017	SBx81CFC400-5.4.7-0.1.rel SBx81CFC960-5.4.7-0.1.rel	SBx81CFC400-gui_547_01.jar SBx81CFC960-gui_547_01.jar
AR4050S AR3050S	AR-series UTM firewalls	03/2017	AR4050S-5.4.7-0.1.rel AR3050S-5.4.7-0.1.rel	See "Accessing the AR-Series Firewall GUI" on page 58
AR2050V AR2010V	AR-series VPN firewalls	03/2017	AR2050V-5.4.7-0.1.rel AR2010V-5.4.7-0.1.rel	See "Accessing the AR-Series Firewall GUI" on page 58
AMF Cloud		03/2017	vaa-5.4.7-0.1.iso	n/a

Under version 5.4.7, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.7.

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

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

Caution: Using a software version file for the wrong switch or AR-series firewall model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

New Products

AlliedWare Plus version 5.4.7-0.1 supports the following recently-released products.

CentreCOM FS980M/9 and FS980M/9PS

Fast Ethernet Managed Access Switches

FS980M switches provide high-performance Fast Ethernet connectivity right where you need it—at the network edge. Flexible and robust, the FS980M series provide total security and management features for enterprises of all sizes. They also support video surveillance and Point of Sale (POS) applications.

Completing the FS980M series of 18, 28 and 52 port switches, are the new compact 9 port models. The FS980M/9 switches offer 8 × 10/100TX Fast Ethernet ports and one copper/ fiber combo SFP port, while the FS980M/9PS PoE switches support the IEEE 802.3at (PoE+) standard, delivering up to 30 Watts of power per port for video surveillance and security applications.

For more information, see alliedtelesis.com/products/fs980m-series.

New Features and Enhancements

This section summarizes the new features in 5.4.7-0.1.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 50.

AMF enhancements

Multiple Tenants on AMF Cloud

AMF Cloud allows an AMF Master and/or Controller to be virtual appliances, rather than integrated into an Allied Telesis switch or firewall. With version 5.4.7-0.1 you can run multiple tenants (up to 60) on a single Virtual AMF Appliance (VAA).

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

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

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

64-bit Virtual AMF Appliance (VAA)

From version 5.4.7-0.1 onwards, the Virtual AMF Appliance is 64 bit.

If you are installing the VAA on VMWare, this means that VMware's "Guest Operating System" should be set to a 64 bit operating system instead of a 32 bit one.

If available, select **Version Other 3.x Linux (64-bit)**.

If version 3.x is not available, such as on earlier versions of vSphere, select Other 2.6x Linux (64-bit).

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

Copying files onto multiple nodes simultaneously

Available on all AlliedWare Plus devices

Version 5.4.7-0.1 enables you to use the command **copy force** to copy files onto multiple nodes in an AMF network. Previously, distributing or copying files within an AMF working-set was not allowed.

To copy files onto multiple devices, create a working-set containing the desired devices and use the following command:

```
network-name[80]#copy force <source> <destination>
```

Parameter	Meaning
<source>	The name of the files or directories to copy.
<destination>	The source filename can include the wildcard *. Use the wildcard with caution, because this command does not ask for confirmation before copying files. If the specified file or files already exist, they are overwritten without question or warning.

This feature is particularly useful because it allows you to distribute a file from any node within the AMF network, to all other AMF nodes. This includes copying files to nodes within the network which are layer 2 only (but part of the AMF network). Note that distributing files to nodes which only have layer 2 reachability requires the file's source to be on an AMF member in the AMF network.

To distribute a file from a node, you need to specify the file location on the source node, starting with "<node-name>.atmf", as shown in the following examples.

Note that you may have to enter Ctrl-C after the command has run, to return to the command prompt.

Example 1 To distribute the file "file.txt" to the top level of flash memory on all nodes from the top level of flash memory on the node named "master", use the commands:

```
master#atmf working-set group all
network-name[80]#copy force master.atmf/flash:/file.txt flash
```

Example 2 To distribute the file "file.txt" to all nodes from a USB stick on the node named "node1", use the commands:

```
master#atmf working-set group all
network-name[80]#copy force node1.atmf/usb:/file.txt file.txt
```

Example 3 You can also copy from an external server. For example, to use TFTP to copy the file test.scp into the top level of Flash memory on the nodes in the working set "building1", from the server at 10.0.0.1, use the commands:

```
master#atmf working-set group building1
network-name[20]#copy force tftp://10.0.0.1/test.scp test.scp
```

Note that in this example, all destination nodes require layer 3 reachability to the external server. Layer 2 AMF nodes in the working-set will fail to receive the file.

To copy the file onto Layer 2 nodes, first copy the file onto a node with layer 3 connectivity, then follow example 1 or 2 above to distribute the file onto the layer 2 nodes.

Dynamic DNS client

Available on AR-Series Firewalls

Version 5.4.7-0.1 adds support for Dynamic Domain Name System (DDNS). DDNS is a mechanism that allows a DDNS client to automatically update a DNS entry hosted by a DDNS Provider. When DDNS is configured on an AR-Series Firewall, DNS requests are automatically directed to the configured host name regardless of Dynamic IP address changes.

Hosting your own web server normally requires a static IP address from your ISP to ensure that your services are always reachable. Your domain name maps your static IP address to your domain (via DNS). Home users or small offices may not want to pay for a static IP address so can use DDNS with a dynamic IP address instead.

DDNS is a method of updating DNS records without the need for manual editing. DDNS provides a consistent domain name for a host that may have its global IP address changed at any time. The DDNS client updates the service providers records to keep the domain name pointing to the correct IP address.

For more information and configuration details, see the new Domain Name Server (DNS) for AlliedWare Plus AR-Series Firewalls Feature Overview and Configuration Guide.

Change to default route on 3G USB cellular modem

Available on AR-Series Firewalls

When a PPP link is established over 3G, it creates a default route with administrative distance of 100. This route was previously invisible, but from version 5.4.7-0.1 you can view it by using the **show ip route** command, as shown in the following example:

```
Client#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, D - DHCP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external 
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*       0.0.0.0/0 [100/0] via 172.16.1.1, ppp0
C        172.16.1.1/32 is directly connected, ppp0
C        172.16.2.1/32 is directly connected, ppp0
C        192.168.2.0/24 is directly connected, vlan1
```

If you need to use another default route via a different interface, configure the default route via the other interface with a lower administrative distance. Use the command:

```
awplus#ip route <subnet&mask> {<gateway-ip>|<interface>}
<distance>
```

Subnet-based NAT and Source and Destination NAT (Double NAT)

Available on AR-Series Firewalls

Version 5.4.7-0.1 adds support for Subnet-based NAT and Source and Destination NAT (also known as Double NAT).

Subnet-based NAT translates just the network portion of a packet's source or destination IP address to a different network address—the host portion of the address is unchanged. There is a one-to-one mapping from addresses in one subnet to the other. Subnet-based NAT allows a user to perform NAT translation on all hosts between two network entities. Configuring a NAT rule with the netmap option, you can modify the source subnet or destination subnet for a range of addresses.

Source and Destination NAT allows the firewalls to translate both the source address and the destination address of incoming and outgoing connections. To configure it, the usual NAT rules are used with port forwarding and masquerade options.

For more information and configuration details, see the new Firewall and Network Address Translation Feature Overview and Configuration Guide. This Guide also covers Source-based NAT, configuring NAT loopback with DMZ, configuring Static NAT with proxy ARP, and configuring a range of firewall functionality.

Additional encryption options for OpenVPN data channel

Available on AR-Series Firewalls

Version 5.4.7-0.1 enables you to select AES-128 or AES-256 as the encryption algorithm for the OpenVPN data channel. Previously, only AES-128 was available.

Version 5.4.7-0.1 also enables you to select SHA1 or SHA256 as the data channel authentication digest.

To select the encryption algorithm, use the following command in interface mode for the desired tunnel:

```
awplus(config-if)#tunnel openvpn cipher [aes128|aes256]
```

The default is AES-128.

To select the authentication digest, use the following command in interface mode for the desired tunnel:

```
awplus(config-if)#tunnel openvpn authentication [sha1|sha256]
```

The default is SHA1.

You need to configure clients to use the same algorithms as configured on the server.

Increased number of concurrent VPN tunnels on AR4050S firewalls

Version 5.4.7-0.1 supports up to 1000 concurrent VPN tunnels on AR4050S firewalls.

By default, client keys are renegotiated after an hour. This can be changed on all AR-series firewalls by using the following command in interface mode for the desired tunnel:

```
awplus(config-if)#tunnel openvpn expiry-seconds <0-4294967295>
```

Version 5.4.7-0.1 includes a new option of 0 seconds, which means that keys are not renegotiated after the VPN is formed. Otherwise, setting the expiry-seconds to a non-zero timer value will cause a rekey when that time is exceeded.

If you intend to use greater than 100 concurrent tunnels on an AR4050S, we recommend you change to rekeying based on data usage per VPN tunnel instead of timer-based rekeying. Each VPN tunnel will then independently rekey once it reaches the data limit. This prevents all tunnels from rekeying at the same time.

To rekey based on data usage per VPN, use the following command in interface mode for the desired tunnel:

```
awplus(config-if)#tunnel openvpn expiry-bytes <0-4294967295>
```

A value of 0 bytes means that keys are not renegotiated after the VPN is formed. To return to default timer-based renegotiation, use the following command:

```
awplus(config-if)#no tunnel openvpn expiry-bytes
```

Shaping bridged traffic with the traffic control feature

Available on AR-Series Firewalls.

Version 5.4.7-0.1 makes it possible for users to explicitly enable traffic control for bridged traffic per bridge interface.

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

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

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

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

Disabling MAC-learning on bridges

Available on AR-Series Firewalls

Version 5.4.7-0.1 supports disabling of FDB MAC address learning on bridges. In some circumstances, FDB MAC address learning on a software-based router bridge is not useful, and it is better to flood the traffic within interfaces associated with the bridge instance, to ensure the traffic reaches its destination.

To turn learning on and off, use the new mac-learning command for the desired bridge interface. For example, to turn off learning on bridge 2, use the following commands:

```
awplus(config)#interface br2
awplus(config-if)#no mac-learning
```

To turn on learning on bridge 2:

```
awplus(config)#interface br2
awplus(config-if)#mac-learning
```

Learning is enabled by default.

Allowing partial sessions through the firewall

Available on AR-Series Firewalls

With version 5.4.7-0.1, firewall rules now have an optional "no-state-enforcement" option.

.

To specify the option, use the new **no-state-enforcement** option in the following command:

```
awplus(config-firewall)#rule {permit|deny|reject|log}
<application_name> from <source_entity> to
<destination_entity> [no-state-enforcement]
```

Enhanced logging of firewall Unified Threat Management (UTM) events

Available on AR4050S and AR3050S Firewalls

Software version 5.4.7-0.1 expands the number of threat management messages that the AR-series UTM firewalls log. This includes messages from the following features:

Feature	Example message
Intrusion Prevention System (IPS)	`2016 Nov 17 03:08:01 local5.info awplus IPS[2064]: [Drop] IPS: icmp-decoder-events ICMPv4 unknown type [icmp] 192.168.92.1 -> 172.16.92.2`
IP Reputation	`2016 Nov 17 02:48:01 local5.info awplus IPS[2014]: [Drop] IPREP: DDoSAttacker: IPREP DDoS Source [icmp] 172.16.92.2 -> 172.16.92.1`
Malware Protection	`2016 Nov 17 02:32:02 local5.info awplus IPS[2014]: [Drop] MALWARE: Virus detected by signature [tcp] 172.16.92.2:42168 -> 192.168.92.1:45528`
URL Filtering	`2016 Nov 17 02:02:21 local5.info awplus IPS[2039]: [Drop] URLFILTER: URL:http:/kdskspb.ru/ [http] 192.168.1.1:58272 -> 172.16.1.2:80`
Web Control	`2016 Nov 26 08:11:15 local5.warning awplus UTM[828]: Web_Control: BLOCK http://www.piracy.com/ requested by 192.168.1.1: Piracy, 0`
Antivirus	`2016 Nov 25 10:15:51 local5.warning awplus UTM[802]: antivirus: Virus EICAR-Test-File[certain] detected in http://www.example.com/data/infected/sample.txt to 192.168.1.1`

You can also filter all UTM log messages easily, because all UTM messages are now labelled with **facility local5**. You can display all UTM messages by creating a filter as shown in the following table:

Log	Commands to create a filter to see only UTM logs
buffered	`awplus(config)#log buffered facility local5`
console	`awplus(config)#log console facility local5`
email	`awplus(config)#log email facility local5`
host (syslog)	`awplus(config)#log host <server-ipaddr> facility local5`
monitor	`awplus(config)#log monitor facility local5`
permanent	`awplus(config)#log permanent facility local5`

Note that firewall log messages are labelled with **facility kern**.

For IPS, IP reputation, Malware Protection and URL Filtering, **show** command output now displays the number of events that have generated an alert or a packet drop since the last reboot. The following commands display the event count:

- show ips
- show ip-reputation
- show malware-protection
- show url-filter

Precision Time Protocol (PTP) and Transparent Clock

Available on IE300 and x930 Series Switches

Version 5.4.7-0.1 supports use of PTP and the Transparent Clock on IE300 Series switches in an IEEE 1588 network, to provide:

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

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

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

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

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

Scripting for Video VLAN support

Available on IE500, IE300 and IE200 Series Switches

Version 5.4.7-0.1 adds support for Scripting for Video-VLAN.

Today’s distributed video surveillance networks can require a large number of switches, which each connect to a group of cameras. This type of deployment can significantly increase the workload of network administrators, therefore it is desirable to have a mechanism that reduces the effort required to configure each switch.

Designed to ease the administrative burden on the network administrator, Scripting for Video-VLAN is an additional component that can be used with AlliedWare Plus products, without modifying or upgrading the current software. It utilizes existing CLI commands and features, such as the trigger mechanism, to auto-configure an interface when certain devices, such as IP cameras, are detected.

For more information, see the Scripting for Video-VLAN Feature Overview and Configuration Guide. This guide describes how to customize, distribute, and activate Scripting for Video-VLAN.

Hybrid OpenFlow™ and OpenFlow™ Local Port

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

Version 5.4.7-0.1 adds support for the following extensions to the OpenFlow protocol:

- A new type of OpenFlow protocol port, the hybrid port, is supported. Hybrid ports allow for a number of VLANs on a port using OpenFlow technology, to be reserved for management purposes. Only tagged traffic on explicitly defined VLANs will be treated as legacy traffic, all other traffic will be treated as OpenFlow technology Controller traffic. Note that AMF traffic on specially reserved VLANs will also be treated as legacy (that is, AMF) traffic, and not as OpenFlow protocol traffic.
- The local port has been supported. This allows OpenFlow protocol rules with an input port or output port specified as Local. The purpose of this is to allow the OpenFlow protocol to control traffic to and from the network stack of the switches operating under the OpenFlow specification.

  The local port manifests itself as an interface called "of0" in the switch. The of0 interface can have IP addresses assigned to it, and can also have sub-interfaces added to it based on VLAN ID.

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

Version 5.4.7-0.1 also removes support for some features:

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

Ethernet Ring Protection Switching (G.8032)

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

Version 5.4.7-0.1 adds support for G.8032 Version 2 February 2012 edition.

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

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

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

Enhancements to IPv6 default behavior

Available on all AlliedWare Plus devices that support IPv6.

From version 5.4.7-0.1 onwards, the default behavior when you enable IPv6 has changed. Enabling IPv6 on an interface now enables all the following behaviour:

- A link-local address is added in EUI-64 format
- Duplicate Address Detection (DAD) and Neighbor Discovery (ND) are enabled
- Router Advertisements (RAs) are processed when received
- Addresses are auto-configured from the prefixes received in RAs, through Stateless Address Autoconfiguration (SLAAC)
- The MTU is set from received RAs
- Default route(s) are added that point to RA source(s)

This new behaviour happens when you enter any command that enables IPv6, including the following commands:

- ipv6 enable
- ipv6 address <X:X::X:X/M>
- ipv6 address dhcp
- ipv6 dhcp client pd

Because SLAAC is enabled by default, the command **ipv6 address autoconfig** is no longer required. If you have this command in a configuration file, the device will replace that command with **ipv6 enable**.

You can disable parts of this functionality.

To disable link-local address generation in EUI-64 format, use the following new command:

```
awplus(config-if)#no ipv6 eui64-linklocal
```

To stop the device from processing prefix information (routes and addresses) from received Router Advertisements, use the following new command:

```
awplus(config-if)#no ipv6 nd accept-ra-pinfo
```

To disable addition of default routes based on received Router Advertisements, use the following pre-existing command:

```
awplus(config-if)#no ipv6 nd accept-ra-default-routes
```

If you disable EUI-64 link-local address generation, you can assign an address manually, by using the following command:

```
awplus(config-if)#ipv6 address <ipv6-address>
```

Note that if you configure a non-EUI-64 address on an interface, you also need to use the command **no ipv6 nd accept-ra-pinfo**. Otherwise the interface will get an EUI-64 address as well as the configured address.

Creating a host key for SSH automatically when replacing devices

Available on all AlliedWare Plus devices

From version 5.4.7-0.1 onwards, if the SSH service is enabled on a device and that device detects that the host key is missing, the device generates a new host key automatically instead of terminating SSH.

This means users can replace a failed device and copy the old device's configuration onto the replacement device, so this enhancement makes it easier to remotely access the replacement device.

The auto-generated host key will use RSA with 1024-bit key generation by default, except for x930 series switches in secure mode, which use ECDSA with a curve length of 384.

If you need to replace an x930 series switch in secure mode and copy its existing configuration file, please use the following steps:

1. copy the configuration file to the flash file system of the new device, then
2. set the copied file as the boot configuration file, then
3. reboot the new device.

Because the hostkey is new on the device, if a remote user tries to connect to the new device with existing SSH credentials, the SSH client will notice that the hostkey for the device is different and may give a warning. The warning will include a selection option to replace the old hostkey, or instructions on how to do this. Follow the client's selection option or instructions.

For example, a Linux client displays the following warning.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-
middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
55:7d:82:00:7e:6f:ac:ac:de:1c:f1:53:08:51:1c:68.
Please contact your system administrator.
Add correct host key in /Users/fergus/.ssh/known_hosts to get
rid of this message.
Offending RSA key in /Users/fergus/.ssh/known_hosts:12
RSA host key for 192.168.1.1 has changed and you have requested
strict checking.
Host key verification failed.
```

Dynamic changes to QoS policy maps and VLAN access maps

Available on SBx8100 Series, SBx908, DC2552XS/L3, x930 Series, x610 Series, x510 Series, IX5-28GPX, x310 Series, x230 Series, IE510-28GSX-80, IE300 Series, and IE200 Series switches

Version 5.4.7-0.1 enables you to modify the following Quality of Service elements even when they are already attached to interfaces:

- class maps
- policy maps
- hardware ACLs that are attached to QoS policy maps
- hardware ACLs that are attached to VLAN access maps (when they are attached to a VLAN through a VLAN filter)

Previously, you had to detach these elements from the interface before modifying them.

This enhancement makes it simpler to modify QoS configurations, and prevents traffic from being incorrectly classified during the period between removing a rule and reapplying the changed rule.

Deleting files from all VCStack members

Available on all stackable AlliedWare Plus switches

Version 5.4.7-0.1 introduces a simple method to delete files from all members of a stack.

To do this, use the following new command:

```
awplus#delete stack-wide force [recursive] <name>
```

Parameter	Meaning
`recursive`	Delete directories that match the name, including their contents.
`<name>`	The name of the files or directories to delete. The filename can include the wildcard *. Use the wildcard with caution, because this command does not ask for confirmation before deleting files.

This a non-interactive command, so if the specified file or files exist, they are deleted without question or warning. This is indicated by the mandatory **force** parameter.

You can use this command within an AMF working set.

Examples

To delete a file test.scp that is located in Flash memory on all stack members, use the command:

```
awplus#delete stack-wide force test.scp
```

To remove directories output1 and output2 from an external card on all stack members, use the command:

```
awplus#delete stack-wide force recursive card:output*
```

VCStack via RJ-45 ports on XS900MX series switches

Version 5.4.7-0.1 enables the CentreCOM XS900MX Series switches to stack two units using RJ-45 copper ports, as well as SFP+ ports. As the units house a mix of copper and fiber ports, this provides flexibility in which ports are used for stacking, and which remain available for network connectivity.

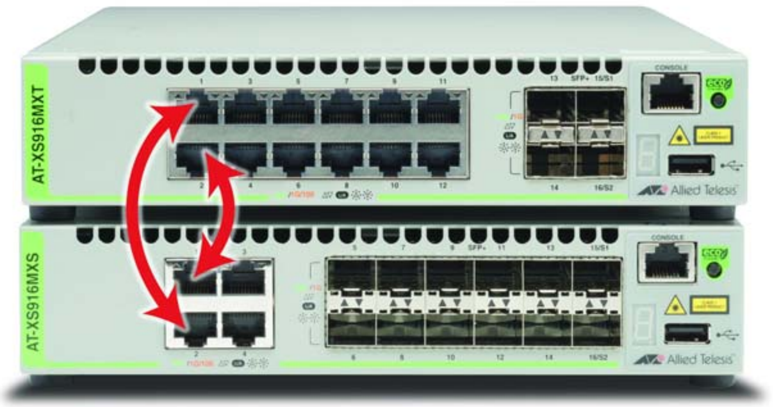
To enable an RJ-45 copper port to become a stacking port, you must first configure its interface for stacking, using the following command:

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

Therefore, you can now use either of the following cables to stack XS900MX Series switches:

- AT-SP10TW1-1 meter SFP+ direct attach cable.
- RJ-45 cable - copper cable Cat 6a or above

The stacking cables must form a ring, for example as shown in the diagram below, which shows stacking through RJ-45 ports 1 and 2:



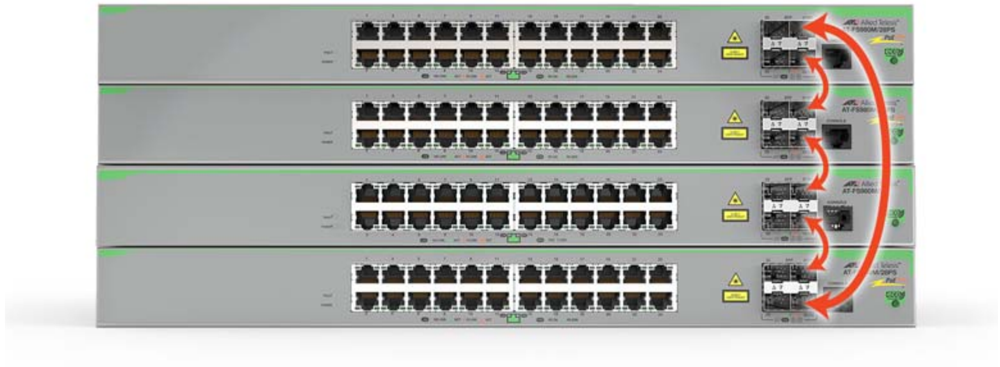
4-Unit VStack on FS980M series switches

Version 5.4.7-0.1 enables the CentreCOM FS980M Series switches to stack up to 4 units using front-port stacking, providing 4Gbps bandwidth. The FS980M Series have four 1GbE SFP ports, two of which may be used for stacking instead of network connectivity.

Use the AT-SP10TW1-1 meter SFP direct attach cable to stack FS980M Series switches.

In a stack of four FS980M/28, connect the cables as follows:

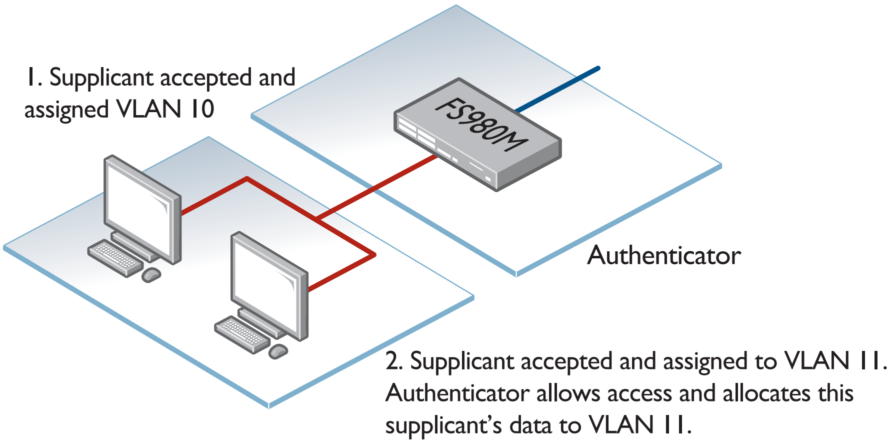
- port1.0.28 <--> port2.0.27
- port2.0.28 <--> port3.0.27
- port3.0.28 <--> port4.0.27
- port4.0.28 <--> port1.0.27



Dynamic VLAN assignment of multiple supplicants via port authentication on FS980M series switches

Version 5.4.7-0.1 enables port authentication to assign different VLANs to different supplicants downstream of the same port on FS980M series switches. This applies to 802.1x, MAC-based and web-based port authentication. This feature was previously only available on x210, x230, x310, x510, x600, x610 and x930 switches.

Figure 1: Dynamically assign multiple VLANs to one port


1. Supplicant accepted and assigned VLAN 10
FS980M
Authenticator
2. Supplicant accepted and assigned to VLAN 11. Authenticator allows access and allocates this supplicant's data to VLAN 11.

On FS980M series switches, you cannot use this feature and VLAN classifier rules on the same port. VLAN classifier rules enable you to create Protocol-based VLANs.

FS980M series switches also do not support using IP subnet-based VLANs at the same time as dynamic VLAN assignment of multiple supplicants.

Configuring dynamic VLAN assignment

Step 1: Enable dynamic VLAN configuration on the switch

On the switch, use the command:

```
awplus(config-if)#auth dynamic-vlan-creation rule permit type
multi
```

Step 2: Use RADIUS attributes to specify the desired VLAN

Configure your RADIUS server to reply in Access-Accept packets with the attributes in the following table. The desired VLAN is specified with the Tunnel-Private-Group-ID attribute.

Attribute	Value
Tunnel-Type	VLAN (13)
Tunnel-Medium-Type	IEEE-802 (6)
Tunnel-Private-Group-ID	The VID or VLAN name

Valid supplicants' packets will be assigned to the desired VLAN after port authentication.

Changes to display of ports on SBx81CFC960

With version 5.4.7-0.1, on a CFC960 control card running silicon profile 3 with stacking disabled, the front ports on the card are now displayed in output of various **show interface** commands. Previously, they were not displayed.

These ports cannot be used as network ports with silicon profile 3 (only as stacking ports), so they are displayed with a status of “err-disabled”. The output of the **show interface err-disable** command will show that they are not supported by silicon profile 3.

BPDU forwarding on SBx908 and SBx8100 switches

Version 5.4.7-0.1 enables SBx908 and SBx8100 series switches to forward STP BPDU frames even when STP is disabled. This may be needed for correct STP operation in complex networks.

To configure a switch to forward BPDU frames, use the command:

```
awplus(config)#spanning-tree bpdu {forward|forward-untagged-
vlan|forward-vlan}
```

To configure a switch to discard BPDU frames (the default setting), use the command:

```
awplus(config)#spanning-tree bpdu discard
```

Parameter	Description
`discard`	Discards all ingress BPDU frames. This is the default setting.
`forward`	Forwards any ingress BPDU frames to all ports, regardless of any VLAN membership.
`forward-untagged-vlan`	Forwards any ingress BPDU frames to all ports that are untagged members of the ingress port’s native VLAN.
`forward-vlan`	Forwards any ingress BPDU frames to all ports that are tagged members of the ingress port’s native VLAN.

You must disable STP with the **no spanning-tree rstp enable** command before you can use this command.

MIB object and type change for SP10ZR80/I

The Allied Telesis SP10ZR80/I is a hot-pluggable 10Gbps small form factor transceiver module.

Prior to version 5.4.7, the SP10ZR80/I displayed "unknown" for the transceiver type in the output from the **show system pluggable** command. It will now show "10GBASE-ZR", as shown in the Type field of the following example output.

```
awplus#show system pluggable

System Pluggable Information

Port   Vendor Device         Serial Number    Datecode   Type
--------------------------------------------------------------------
1.0.25 ATI    AT-SP10ZR80/I  04780R124700005  121126     10GBASE-ZR
--------------------------------------------------------------------
```

The SP10ZR80/I now has a atPortInfoTransceiverType OID of sfpp-zr(40).

Extended hardware switching on x310 Series switches

Version 5.4.7-0.1 enables x310 Series switches to hardware-switch individual hosts in remote networks that are not covered by any routes in the hardware route table. Without this enhancement, x310 switches route packets via the CPU if they were destined to remote networks that were not added to the IP route table in hardware.

To enable the extended hardware switching, use the following new command:

```
awplus(config)#fib cache-remote-host
```

Issues Resolved in Version 5.4.7-0.3

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

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56932	**AMF**	Previously, the **copy force** command had been allowed in AMF working sets when it should not have been, as the command relies on interactive device activity. Use of this command could result in the CLI becoming unresponsive. This issue has been resolved. Now the **copy force** command is no longer available from within an AMF working set. 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-57136	**AMF**	Previously, not all AMF nodes were joining after enabling or disabling secure-mode. 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
CR-57176	**AMF**	Previously, AMF auto recovery would not work with secure-mode VMAC enabled. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	–	–	Y	–	–	Y	Y	–	Y	Y	Y	–	Y	Y	Y	Y	Y	Y

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57135	**AMF** **Stacking**	Previously, an AMF working-set operation could occasionally fail to include all nodes after a stack master failover. This issue manifested itself in only forming a working-set of the top level domain nodes when issued from the new stack master. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	–	–	Y	–	–	Y	Y	Y	–	Y	Y	Y	Y	Y	–	–	–	Y
CR-57154	**AMF** **VCStack**	Previously, the RESTful API on the AMF master was not updated with the correct stack information after the old stack master rejoined the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-57191	**Antivirus** **Web Control**	With this software update, Antivirus will now handle large files being transferred through the device more efficiently. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-57205	**ARP** **Neighbor Discovery**	Previously, the NLB non IP multicast IP/MAC was not installed for XLEM line card. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-57085	**Firewall**	Previously, asymmetrically configured VoIP traffic could be incorrectly dropped by the NGFW routers. The behavior of the Firewall VoIP ALG traffic helper has been enhanced to resolve this issue.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR--56456	**IDS/IPS, PPP**	Previously, when using stream-based UTM features (IPS, IP Reputation, Malware Protection, URL Filtering, DPI) with a PPP WAN interface, UTM processing would be performed twice on outgoing packets. This could cause unnecessary CPU load and in some cases could cause packets to be dropped due to IPS falsely detecting problems with the packet flow characteristics. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-57067	**LED**	Previously, the ECO friendly LED on the stacking backup member was not reflecting the correct state after a master 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	Y	–
CR-57171	**NAT**	Previously, when configuring a NAT **portfwd** rule with **dports** value, the **dport** value was incorrectly changed to the NAT rule number, this could be observed in the running configuration. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56963	**OSPFv2**	Previously, during a master failover, OSPF, BGP and OSPFv3 could sometimes be delayed from entering graceful restart by up to 15 seconds if configuration changes were made just prior, or during the failover (e.g, from a trigger script). In most cases this delay was not necessary, and so OSPF, BGP and OSPFv3 would only delay entering graceful restart if truly necessary. Also, during a master failover where OSPF has been delayed entering graceful restart, it could sometimes prematurely send LSA updates to other OSPF speakers in the network, which could lead to sub-optimal routing for a period of time after the master failover. These issues have been resolved, OSPF will now send routing updates at the correct time during the graceful restart procedure.	–	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-57272	**RADIUS**	Previously, the RADIUS accounting packet did not to have the attributes specific to "Acct-Status" type. This issue has been resolved. ISSU: Effective when CFC upgraded.	Y	–	Y	–	–	–	–	–	–	–	–	–	Y	–	Y	–	Y	Y	–	–	–	–
CR-56950	**Stacking**	Previously, when the VCS master failover was in progress, executing the "write" command could sometimes result in loss of OSPF configuration from the startup config. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	Y	Y	–	–	Y	–	–	Y	Y	Y	–	–	Y	Y	Y	Y	–	–	–	–
CR-57157	**Unicast Routing**	Previously, an ECMP network would become unreachable after one of the multi-paths was removed and then re-added. 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	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57238	**URL Filtering**	Previously, under heavy load with large number of flows, it was possible for the stream engine flow time-out mechanism to fail. Eventually the flow memory capacity limit would be reached, resulting an all new flows being denied until the device was rebooted. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-57174	**VCStack**	Previously, when stacking was disabled on an XS900 series switch, the **stack-port** setting would not be updated. This issue has been resolved.	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-57103	**Web control**	Previously, the Web-control (Proxy Server) processes could consume unnecessary memory. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-57128	**xSTP**	Previously, executing the command **spanning-tree transmit-holdcount** could result in an unexpected restart of the device. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y

Issues Resolved in Version 5.4.7-0.2

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

CR	Module	Description	FS980M	GS900MX	GS970M	XS900MX	IE200	IE300	IE500	x210	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR00057023	**AMF** **CLI**	Previously, it was sometimes possible for the erroneous message "Enter configuration commands..." to be displayed in the command shell window as a result of entering the command **atmf distribute firmware**. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00056956	**AMF** **File System**	Previously, the **delete stack-wide** command did not produce any output due to it being a non-interactive command. This issue has been resolved, the command will now generate output consistent with the **delete force** command.	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y
CR00057002	**Bootup**	Previously, in rare circumstances, the device could lockup during a failover while rarely used diagnostic show commands were being executed. This issue has been resolved.	Y	Y	–	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR00057070	**Bootup**	Previously, on x230 variant switches, an unnecessary NVRAM error was displayed during boot-up. This issue has been resolved, the NVSRAM has been disabled.	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR00056990	**Deep Packet Inspection** **Traffic Control**	Previously, some of the DPI applications were not triggering associated traffic control rules. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	GS900MX	GS970M	XS900MX	IE200	IE300	IE500	x210	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR00056714	**OSPFv2**	Previously, when OSPF went through graceful restart as a result of a stack failover, occasionally the device would fail to correctly detect that a topology change had occurred as a result of the failover. This would mean graceful restart would persist until the time out period expired (default 3 minutes), which could result in incorrect routing decisions and packet loss during this time. This issue has been resolved.	–	–	–	–	–	Y	Y	–	–	Y	–	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	–
CR00056991	**Port Configuration**	Previously, ports on SBx81XLEM/XT4 line cards sometimes would not link up when the port speed was changed to 1G. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–
CR00056841	**Port Security**	Previously, if port-security aging was disabled, the lock action would not work correctly. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR00056647	**Stacking** **OSPF**	Previously, in an environment where stacked devices running OSPF in a non-symmetrical topology when the stack goes through a failover process, the OSPF process in the new master might, in a rare occasion, fail to exchange OSPF information via grace-LSA for up to 180 seconds. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–
CR00056071	**System**	Previously, there was a small chance that the SBx81LIFv1 variant line cards would not be initialized correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–

CR	Module	Description	FS980M	GS900MX	GS970M	XS900MX	IE200	IE300	IE500	x210	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	x908Gen2	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR00056801	**User Management** **ATM**	Previously, the command shell imi process would restart unexpectedly at "timeout" when using the command: **atmf remote-login**. This issue has been resolved.	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y
CR00053470	**VCStack**	Previously, on rare occasions, an unexpected restart of some processes could occur on a switch. This issue has been resolved.	–	–	–	–	–	–	–	Y	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–	–

Important Considerations Before Upgrading

Changes to start-up behavior

Available on all AlliedWare Plus devices

From AlliedWare Plus version 5.4.7-0.4 onwards, unconfigured devices automatically receive a management IP address on start-up, without any manual configuration. You can optionally set up a DHCP server on your network and have the device obtain an address via DHCP, or otherwise the device uses an IP address of 169.254.42.42.

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

For details see "Change in default start-up behavior" on page 6.

Changes to OpenFlow support

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

Version 5.4.7-0.1 removes support for some OpenFlow features:

- The hairpin link is no longer supported; the hybrid port is instead (see "Hybrid OpenFlow™ and OpenFlow™ Local Port" on page 25). When upgrading from 5.4.6-2.x or earlier to 5.4.7-0.1 or later, special care will have to be taken if a hairpin link is present. Please contact Allied Telesis Support for assistance on this.
- AMF guest nodes on ports using the OpenFlow protocol are no longer supported.

Traffic Control is disabled by default for bridged traffic

Applies to AR-Series Firewalls

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

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

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

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

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

Traffic Shaping commands have been deleted

Applies to AR3050S and AR4050S Firewalls

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

If you are running Traffic Shaping and you want to upgrade to 5.4.7-0.x from 5.4.5-x.x or an earlier version, upgrade to a 5.4.6-x.x version first and then save your configuration. AlliedWare Plus will convert your configuration automatically to a Traffic Control configuration.

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

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

Applies to SBx8100 switches

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

Using the switch GUI with TACACS+ command authorization

Applies to AlliedWare Plus switches

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

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

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

Changes to NTP configuration in AMF networks

Applies to all AlliedWare Plus devices

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

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

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

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

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

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

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

DC2552XS/L3 reboot history now stored in NVS

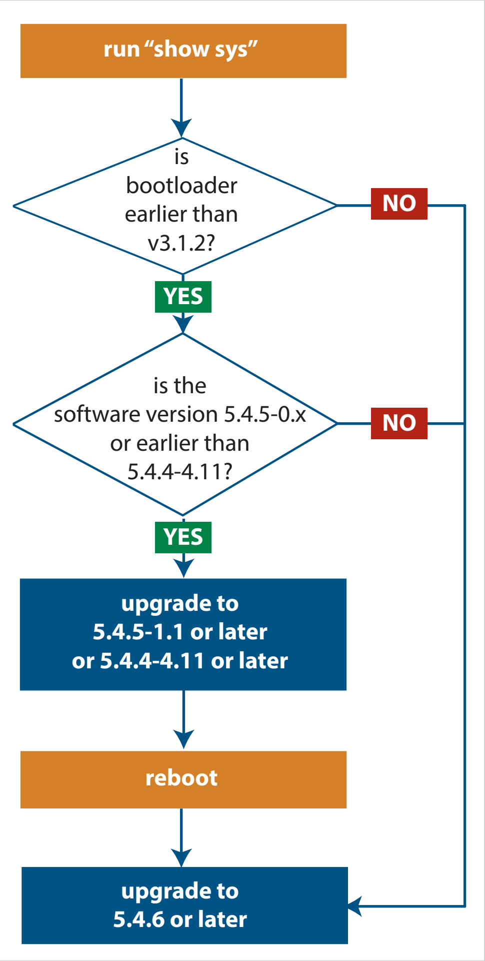
Applies to DC2552XS/L3 switches

When you upgrade a DC2552XS/L3 switch from 5.4.5-x.x or earlier to 5.4.7-0.x or 5.4.6-x.x, the switch's reboot history is reset. The ongoing reboot history will be stored in NVS. If you need to view the previous reboot history, see the file reboot.log in the Flash file system.

Bootloader compatibility for SBx81CFC960

Applies to SBx8100 Series switches

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


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

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

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

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

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

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

```
awplus# show system
```

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

Licensing

Applies to SBx908 and SBx8100 Series switches

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

If you are upgrading to 5.4.7-0.x on your SBx908 or SBx8100 switch, please ensure you have a 5.4.7 license on your switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

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

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

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

You cannot use ISSU to upgrade to 5.4.7-0.1 or 5.4.7-0.2 from any previous software version.

Upgrading a VCStack with reboot rolling

Applies to all stackable AlliedWare Plus switches

This version supports VCStack "reboot rolling" upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack. You can use the **reboot rolling** command to upgrade to 5.4.7-0.x from:

- 5.4.6-0.x, or
- 5.4.6-1.x, or
- 5.4.6-2.x, or
- 5.4.5-x.x, or
- 5.4.4-1.x or later.

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

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

Forming or extending a VCStack with auto-synchronization

Applies to all stackable AlliedWare Plus switches

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up. Auto-synchronization is supported between 5.4.7-0.x and:

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

It is not supported between 5.4.7-0.1 and 5.4.6-1.1 or **any** earlier releases.

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

On VCStacks

If you are working with a VCStack:

- If you want to upgrade an existing VCStack to 5.4.7-0.x, this should not cause any problems. The **boot system** command will automatically copy the new software release to all stack members. Do not reboot any individual stack members after installing the new release - instead reboot the stack as a whole.

  If you encounter any errors from the **boot system** command, then check that the release file was copied to all stack members before rebooting. If it was not, then address any problems reported, such as freeing up space in Flash for the new release file, and then repeat the **boot system** command again.
- If a stack is running v5.4.7-0.x, and you connect a switch running 5.4.6-1.1 or earlier to the stack, then the v5.4.7-0.x software will not be automatically copied over to the newly-added stack member, even if **stack software-auto-synchronize** has been enabled on the stack. Instead, upgrade the switch that is to be added to the stack to v5.4.7-0.x before you add it to the stack.
- If a stack is running 5.4.6-1.1 or earlier, and you connect a switch running v5.4.7-0.x to the stack, then the older software cannot be automatically copied over to the newly-added stack member, even if **stack software-auto-synchronize** has been enabled on the stack. Instead, downgrade the switch that is to be added to the stack to the older release before you add it to the stack.
- If you do boot up a stack with a switch running an incompatible version, the incompatible switch will boot up as a standalone unit. To recover, simply leave the incompatible switch cabled into the stack, log into it, upgrade or downgrade it to the desired release, and reboot the switch.

On a VCStack Plus Pair of SBx8100 chassis

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

- If you want to upgrade an existing SBx8100 VCStack Plus system to v5.4.7-0.x, this should not cause any problems. The **boot system** command will automatically copy the new software release to all stack members. Do not reboot any individual CFCs or stack members after installing the new release - instead reboot the stack as a whole.

  If you encounter any errors from the **boot system** command, then check that the release file was copied to all CFCs. If it was not, then address any problems reported, such as freeing up space in Flash for the new release file, and then repeat the **boot system** command again.
- If you want to insert a new dual CFC into a chassis that is part of an existing VCStack Plus system, refer to "Upgrading an SBx8100 chassis or adding a CFC to an SBx8100 chassis" below.
- If you want to insert a new SBx8100 chassis into a VCStack Plus system, refer to "On VCStacks" on page 46 above.

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

If you want to upgrade an existing SBx8100 that has two CFCs installed to v5.4.7-0.x, this should not cause any problems. The **boot system** command will automatically copy the new software release to both CFCs. Do not reboot any individual CFCs after installing the new release - instead reboot the chassis as a whole.

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

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

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

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

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

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

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

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

Upgrading/ downgrading a CFC

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

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

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

AMF software version compatibility

Applies to all AlliedWare Plus devices

We strongly recommend that all nodes in an AMF network run the same software release. If this is not possible, compatibility depends on whether your AMF network is in secure mode or not.

If it is **in secure mode**, all nodes must run version 5.4.7-0.3 or later. (Upgrade all nodes to run version 5.4.7-0.3 or later before you enable secure mode.)

If it is **not in secure mode**, nodes running version 5.4.7-0.x are compatible with nodes running:

- 5.4.6-2.x
- 5.4.6-1.x
- 5.4.6-0.x
- 5.4.5-x.x
- 5.4.4-x.x, and
- 5.4.3-2.6 or later.

If you are using Vista Manager, all nodes must run version 5.4.7-0.1 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 of these methods to upgrade to this software version. You can use these methods to upgrade to this version from 5.4.3-2.6 and later.

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

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

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

Obtaining User Documentation

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

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

Verifying the Release File for x930 Series Switches

On x930 Series switches, to ensure that the release file has not been corrupted or interfered with during download, you can verify the release file. To do this, enter Global Configuration mode and enter the following command to verify the SHA256 checksum of the file:

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

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

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

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

The following command contains the hash for 5.4.7-0.4, so you can simply copy and paste that command into the CLI if you wish to verify the file x930-5.4.7-0.4.rel:

```
crypto verify x930-5.4.7-0.4.rel 6bb740bee6b1a2d0aed6a21087dbf2c22ce7dcf85d816da0bdd57dfc9dfa11c8
```

The following command contains the hash for 5.4.7-0.3, so you can simply copy and paste that command into the CLI if you wish to verify the file x930-5.4.7-0.3.rel:

```
crypto verify x930-5.4.7-0.3.rel c817360a1cea4eabd5159c138be028afff0dbac6d2f0b3d802eb3cb5f5af0b53
```

The following command contains the hash for 5.4.7-0.2, so you can simply copy and paste that command into the CLI if you wish to verify the file x930-5.4.7-0.2.rel:

```
crypto verify x930-5.4.7-0.2.rel 4cfbcc96b672699df8e05b43e6685f5f3edd3c866f01cd6ef9e51fe5b3a5d931
```

The following command contains the hash for 5.4.7-0.1, so you can simply copy and paste that command into the CLI if you wish to verify the file x930-5.4.7-0.1.rel:

```
crypto verify x930-5.4.7-0.1.rel e878c83bd4220ca1fde7f9a8f1a3046735fae6a2c40559586527e649929f81e3
```

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

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

Verifying the release on subsequent boot-ups

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

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

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

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

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

Licensing this Software Version on an SBx908 Switch

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

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

1. Obtain the MAC address for a switch

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

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

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

2. Obtain a release license for a switch

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

3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus switches:

```
awplus#show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                         : 1
License name                  : Base License
Customer name                 : ABC Consulting
Quantity of licenses          : 1
Type of license               : Full
License issue date            : 20-Mar-2017
License expiry date           : N/A
Features included             : EPSR-MASTER, IPv6Basic, MLDSnoop, OSPF-64,
                                RADIUS-100, RIP, VRRP

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

Licensing this Software Version on an SBx8100 Series Switch Control Card

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

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

If your control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

If your license certificate contains release licenses for each control card present in a stacked chassis, entering the **license certificate** command on the stack master will automatically apply the release licenses to all the control cards within the stack.

1. Obtain the MAC address for a control card

A release license is tied to the control card MAC address in a chassis.

Chassis may have several MAC addresses. Use the **show system mac license** command to show the control card MAC address for release licensing. Note the MAC addresses for each control card in the chassis. The chassis MAC address is not used for release licensing. Use the card MAC address for release licensing.

```
awplus#show system mac license

MAC address for licensing:

Card                 MAC Address
------------------------------------
1.5                  eccd.6d9e.3312
1.6                  eccd.6db3.58e7

Chassis MAC Address eccd.6d7b.3bc2
```

2. Obtain a release license for a control card

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

3. Apply a release license on a control card

Use the **license certificate** command to apply a release license to each control card installed in your chassis or stack.

Note the license certificate file can be stored on internal flash memory, a USB drive, or on a server accessible by the TFTP, SCP or HTTP protocols.

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

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

Stack member 1 installed 1 license

1 license installed.
```

4. Confirm release license application

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

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

The **show license** command displays the base feature license and any other feature and release licenses installed on AlliedWare Plus chassis:

```
awplus#show license
OEM Territory : ATI USA
Software Licenses
------------------------------------------------------------------------
Index                         : 1
License name                  : Base License
Customer name                 : ABC Consulting
Quantity of licenses          : 1
Type of license               : Full
License issue date            : 20-Mar-2017
License expiry date           : N/A
Features included             : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                                Virtual-MAC, VRRP

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

Installing this Software Version

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

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

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

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

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

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

   ```
   awplus# copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

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

   ```
   awplus# configure terminal
   ```

   Then set the switch to reboot with the new software version. For example, for 5.4.7-0.3, use one of the following commands:

Product	Command
FS980M series	`awplus(config)# boot system FS980-5.4.7-0.3.rel`
GS900MX/ MPX series	`awplus(config)# boot system GS900-5.4.7-0.3.rel`
GS970M series	`awplus(config)# boot system GS970-5.4.7-0.3.rel`
XS900MX series	`awplus(config)# boot system XS900-5.4.7-0.3.rel`
x210 series	`awplus(config)# boot system x210-5.4.7-0.3.rel`
x230 series	`awplus(config)# boot system x230-5.4.7-0.3.rel`
IE200 series	`awplus(config)# boot system IE200-5.4.7-0.3.rel`
x310 series	`awplus(config)# boot system x310-5.4.7-0.3.rel`
IE300 series	`awplus(config)# boot system IE300-5.4.7-0.3.rel`
IX5-28GPX	`awplus(config)# boot system IX5-5.4.7-0.3.rel`

Product	Command
x510 series	`awplus(config)# boot system x510-5.4.7-0.3.rel`
IE510-28GSX	`awplus(config)# boot system IE510-5.4.7-0.3.rel`
x610 series	`awplus(config)# boot system x610-5.4.7-0.3.rel`
SBx908	`awplus(config)# boot system SBx908-5.4.7-0.3.rel`
x930 series	`awplus(config)# boot system SBx930-5.4.7-0.3.rel`
DC2552XS/L3	`awplus(config)# boot system DC2500-5.4.7-0.3.rel`
SBx8100 with CFC400	`awplus(config)# boot system SBx81CFC400-5.4.7-0.3.rel`
SBx8100 with CFC960	`awplus(config)# boot system SBx81CFC960-5.4.7-0.3.rel`
AR2010V	`awplus(config)# boot system AR2010V-5.4.7-0.3.rel`
AR2050V	`awplus(config)# boot system AR2050V-5.4.7-0.3.rel`
AR3050S	`awplus(config)# boot system AR3050S-5.4.7-0.3.rel`
AR4050S	`awplus(config)# boot system AR4050S-5.4.7-0.3.rel`

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

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

6. Reboot using the new software version.

```
awplus# reload
```

Accessing the AR-Series Firewall GUI

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

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

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

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

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

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

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

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

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

```
awplus# update webgui now
```

4. Enable the HTTP service:

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

5. Log into the GUI.

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

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

Installing the Switch GUI

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

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

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

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

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

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

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

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To list files, use the command:

   ```
   awplus# dir
   ```

   To delete files, use the command:

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

   You cannot delete the current boot file.

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

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

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

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

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

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

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

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

   TFTP server: Use the command:

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

   SD card: use the command:

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

   USB storage device: use the command:

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

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

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

   ```
   awplus# configure terminal
   ```

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

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

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

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

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

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

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

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

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

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

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

11. Log into the GUI.