Software Maintenance Release Note

AlliedWare Plus™ Software Version 5.4.6-2.12

For SwitchBlade x8100, SwitchBlade x908, DC2552XS/L3, x930, x610, x510, IE200, IE300, IE500 Series Switches, IX5, x310, x230, x210, FS980M, GS900, and XS900 Series Switches, AR2010V, AR2050V VPN Firewalls, AR3050S and AR4050S NGFWs, and VAA.

Introduction

This document lists the issues addressed in AlliedWare Plus™ software maintenance version 5.4.6-2.12. Read this maintenance release note in conjunction with the:

- *New and Enhanced Features in AlliedWare Plus 5.4.6 Major and Minor Versions*, which describes new and enhanced features in AlliedWare Plus software version 5.4.6-0.x.
- For more information, see the Command Reference for your switch or AR-Series firewall.

Contents

Supported Models and Software File Names

Table 1: Supported switch models and software file names

Models	Series	Release File	Date	GUI file
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS	FS980M	FS980-5.4.6-2.12 rel	September/ 2018	FS980-gui_546_20.jar
AT-GS924MX AT-GS924MPX AT-GS948MX AT-GS948MPX	GS900	GS900-5.4.6-2.12.rel	September/ 2018	GS900-gui_546_04.jar
AT-XS916MXT AT-XS916MXS	XS900	XS900-5.4.6-2.12.rel	September/ 2018	XS900-gui_546_11.jar
AT-x210-9GT AT-x210-16GT AT-x210-24GT	x210	x210-5.4.6-2.12.rel	September/ 2018	x210-gui_546_11.jar
AT-x230-10GP AT-x230-18GP AT-x230-18GT AT-x230-28GP AT-x230-28GT	x230	x230-5.4.6-2.12.rel	September/ 2018	x230-gui_546_20.jar
AT-x310-26FT AT-x310-50FT AT-x310-26FP AT-x310-50FP	x310	x310-5.4.6-2.12.rel	September/ 2018	x310-gui_546_11.jar
AT-IE200-6FT AT-IE200-6FP AT-IE200-6GT AT-IE200-6GP	IE200	IE200-5.4.6-2.12.rel	September/ 2018	ie200-gui_546_11.jar
AT-IE300-12GT AT-IE300-12GP	IE300	IE300-5.4.6-2.12.rel	September/ 2018	n/a
AT-IE510-28GSX-80	IE510	IE510-5.4.6-1.4.rel	September/ 2018	ie510-gui_546_04.jar
AT-IX5-28GPX		IX5-5.4.6-2.12.rel	September/ 2018	IX5-gui_546_11.jar

Table 1: Supported switch models and software file names

Models	Series	Release File	Date	GUI file
AT-x510-28GTX AT-x510-52GTX AT-x510-28GPX AT-x510-52GPX AT-x510-28GSX AT-x510-28GSX-80 AT-x510DP-28GTX AT-x510DP-52GTX AT-x510L-28GT AT-x510L-28GP AT-x510L-52GT AT-x510L-52GP	x510	x510-5.4.6-2.12.rel	September/ 2018	x510-gui_546_11.jar
IE510-28GSX-80	IE500	IE510-5.4.6-2.12.rel	September/ 2018	IE510-gui_546_04.jar
AT-x610-24Ts AT-x610-24Ts-PoE+ AT-x610-24Ts/X AT-x610-24Ts/X-PoE+ AT-x610-24SPs/X AT-x610-48Ts AT-x610-48Ts-PoE+ AT-x610-48Ts/X AT-x610-48Ts/X-PoE+	x610	x610-5.4.6-2.12.rel	September/ 2018	x610-gui_546_11.jar
SwitchBlade x908*	SBx908	SBx908-5.4.6-2.12.rel	September/ 2018	SBx908-gui_546_11.jar
AT-x930-28GTX AT-x930-28GPX AT-x930-52GTX AT-x930-52GPX AT-x930-28GSTX	x930	x930-5.4.6-2.12.rel	September/ 2018	x930-gui_546_11.jar
AT-DC2552XS/L3		dc2500-5.4.6-2.12.rel	September/ 2018	dc2500-gui_546_11.jar
AT-SBx81CFC400 AT-SBx81CFC960	SBx8100	SBx81CFC400-5.4.6-2.12.rel SBx81CFC960-5.4.6-2.12.rel	September/ 2018	SBx81CFC400_gui_546_20.jar SBx81CFC960_gui_546_20.jar
AT-AR2010V AT-AR2050V	VPN Firewalls	AR2010V-5.4.6-2.12.rel AR2050V-5.4.6-2.12.rel	September/ 2018	n/a
AT-AR3050S AT-AR4050S	NGFW	AR3050S-5.4.6-2.12.rel AR4050S-5.4.6-2.12.rel	September/ 2018	n/a
AMF Cloud		vaa-5.4.6-2.12.iso	September/ 2018	n/a

*Under version 5.4.6, not all models of XEM are supported in the SwitchBlade x908. The following table lists which XEMs are and are not supported under version 5.4.6.

Table 2: Support of XEM modules for the SwitchBlade x908 in version 5.4.6-x.x

Product	Supported in version 5.4.6-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 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.

Installing the GUI to your Switch using an SD Card or USB Device

1. **Download a GUI Java applet.**

   The GUI Java applet file is available in a compressed (zip) file with the AlliedWare Plus Operating System software from the Software Download area of the Allied Telesis Website: http://www.alliedtelesis.com/support/software/restricted. Log in using your assigned Email Address and Password. Download the Java applet file. This file will have a `.zip` file name extension. You need to extract the Java `.jar` file from the compressed `.zip` file. The version number of the software applet file (`.jar`) gives the earliest version of the software file (`.rel`) that the GUI can operate with.

2. **Copy the GUI Java applet .jar file to an SD card or USB storage device.**

   Insert the SD card in the SD slot on the front of your switch or the USB device into the USB port on the switch. Connect to the management port, then login to the switch.

   Copy the GUI Java applet to your switch, using the below commands:

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

   or

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

   Where `<filename.jar>` is the GUI Java applet file you downloaded in Step 1.

Note: Where the GUI file is not in the root directory of the USB flash drive, you must enter the full path to the GUI file. For example, where the GUI file resided in the folder gui_files, you would enter the command: copy usb:/gui_files/filename.jar flash:/

3. **Assign IP addresses.**

   Use the following commands to assign the IP addresses for connecting to the Java applet.

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

4. **Configure the gateway.**

   Configure your switch with a default gateway, if necessary, using these commands:

   ```
   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. Note that you do not need to define a default gateway if you browse to the switch from within its own subnet.

5. **Create a user account.**

   In order to log into the GUI, you must first create a user account. Use these commands to setup a user account:

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

   Note that you can create multiple users to log into the GUI. See the AlliedWare Plus Software Reference for information about the **username** command.

6. **Ensure HTTP service is enabled.**

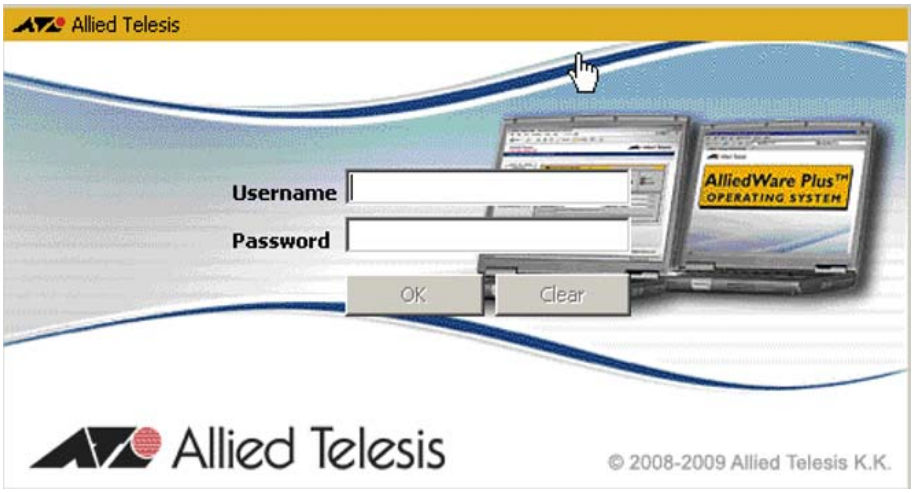
   The HTTP service needs to be enabled on the switch before it accepts connections from a web browser. The HTTP service is enabled by default. However, if the HTTP service has been disabled, you must enable the HTTP service again. If the HTTP service is disabled, use the following command to enable it:

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

   See the *AlliedWare Plus Software Reference* for information about the **service http** command.

7. **Log into the GUI.**

   Start a browser and enter the IP address you configured in Step 3 as the URL. You will be presented with a login screen after the GUI Java applet has started. Log in with the username and password that you defined in the earlier step, named **Create a user account.**



Note: Any configuration changes should be saved to ensure the device settings are retained.

Installing the GUI to your Switch via TFTP Server

1. **Download a GUI Java applet file from the support site.**

   The GUI Java applet file is available in a compressed (.zip) file with the AlliedWare Plus Operating System software. You can download the applet from the Allied Telesis Download Center by logging into your account.

   You need to extract the Java .jar file from the compressed .zip file. The version number of the software applet file (.jar) gives the earliest version of the software file (.rel) that the GUI can operate with.

2. **Copy the GUI applet.**

   Copy the GUI applet .jar file onto a TFTP server. Ensure this TFTP server is enabled and ready for the switch. Connect to the management port of the switch, then login to the switch. Do not connect to the management port of the TFTP server

3. **Assign the IP addresses.**

   Use the following commands to configure your switch with an appropriate IP address:

   ```
   awplus# configure terminal
   awplus(config)# interface vlan1
   awplus(config-if)# ip address 192.168.2.6/24
   ```

   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`, and a subnet mask of `255.255.255.0`, use the following command:

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

   Use the following commands to configure your switch with a default gateway:

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

4. **Configure the default gateway.**

   In necessary, use the following commands to configure the default gateway.

   ```
   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. Note that you do not need to define a default gateway if you browse to the switch from within its own subnet.

5. **Copy the GUI Java applet to your switch.**

   Use the following commands to copy the GUI Java applet to your switch:

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

   Where *<server-address>* is the IP address for the TFTP server, and where *<filename.jar>* is the GUI Java applet file you downloaded in Step 1.

6. **Create a user account.**

   In order to log into the GUI, you must first create a user account. Use the following commands to setup a user account.

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

   Note that you can create multiple users to log into the GUI. See the AlliedWare Plus Software Reference for information about the `username` command.

7. **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.

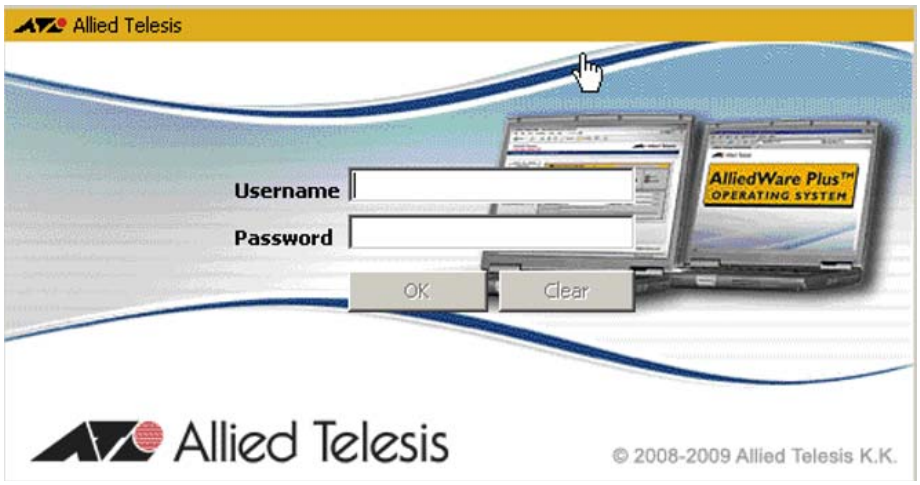
8. **Enter the URL in the Java Control Panel Exception Site List.**

   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.

9. **Log into the GUI.**

   Start a browser then enter the IP address you configured in Step 3 as the URL. You will then be presented with a login screen after the GUI Java applet has started. You can then Log in with the username and password that you defined previously in Step 6.



Note: Any configuration changes should be saved to ensure the device settings are retained.

For more information please refer to the 5.4.6 Command Reference for your product available from the Support area of the Allied Telesis Website.

Installing and Enabling this Version

To use this version, your switch must already be running AlliedWare Plus. Contact your distributor or reseller for more information.

To install this version:

1. Put the version file onto your TFTP server.
2. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   Note that you cannot delete the current boot file.

   To list files, use the command:

   ```
   awplus# dir
   ```

   To see the memory usage, use the command:

   ```
   awplus# show file systems
   ```

   To delete files, use the command:

   ```
   awplus#del <filename>
   ```
3. Copy the new release from your TFTP server onto the switch.

   To do this, enter Privileged Exec mode and use the command:

   ```
   awplus#copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.
4. Set the switch to boot from the new release.

   Enter Global Configuration mode.

   On the x210 Series switches, use the command:

   ```
   awplus(config)#boot system x210-5.4.6-2.12.rel
   ```

   On the x230 Series switches, use the command:

   ```
   awplus(config)#boot system x230-5.4.6-2.12.rel
   ```

   On the x310 Series switches, use the command:

   ```
   awplus(config)#boot system x310-5.4.6-2.12.rel
   ```

   On the x510 Series switches, use the command:

   ```
   awplus(config)#boot system x510-5.4.6-2.12.rel
   ```

   On the IX5-28GPX switch, use the command:

   ```
   awplus(config)#boot system ix5-5.4.6-2.12.rel
   ```

   On the x610 Series switches, use the command:

   ```
   awplus(config)#boot system x610-5.4.6-2.12.rel
   ```

   On the SwitchBlade x908, use the command:

   ```
   awplus(config)#boot system SBx908-5.4.6-2.12.rel
   ```

   On the x930 Series switches, use the command:

   ```
   awplus(config)#boot system x930-5.4.6-2.12.rel
   ```

   On the DC2552XS/L3 switch, use the command:

   ```
   awplus(config)#boot system dc2500-5.4.6-2.12.rel
   ```

On the SwitchBlade x8100 Series switches with a SBxCFC400 controller card installed, use the command:

```
awplus(config)#boot system SBx81CFC400-5.4.6-2.12.rel
```

On the SwitchBlade x8100 Series switches with a SBxCFC960 controller card installed, use the command:

```
awplus(config)#boot system SBx81CFC960-5.4.6-2.12.rel
```

On the ARxx series (NGFW) security appliances, use the commands for each product as follows:

```
awplus(config)#boot system AR2010v-5.4.6-2.12.rel
awplus(config)#boot system AR2050v-5.4.6-2.12.rel
awplus(config)#boot system AR3050S-5.4.6-2.12.rel
awplus(config)#boot system AR4050S-5.4.6-2.12.rel
```

If desired, check the boot settings by entering Privileged Exec mode and using the following command:

```
awplus#show boot
```

On the FS980M Series switches, use the command:

```
awplus(config)#boot system FS980-5.4.6-2.12.rel
```

On the GS900MX/MPX Series switches, use the command:

```
awplus(config)#boot system GS900-5.4.6-2.12.rel
```

On the XS900MX Series switches, use the command:

```
awplus(config)#boot system XS900-5.4.6-2.12.rel
```

On the IE200 Series switches, use the command:

```
awplus(config)#boot system IE200-5.4.6-2.12.rel
```

On the IE300 Series switches, use the command:

```
awplus(config)#boot system IE300-5.4.6-2.12.rel
```

On the IE500 Series switches, use the command:

```
awplus(config)#boot system IE500-5.4.6-2.12.rel
```

5. Reboot.

   To do this, enter Privileged Exec mode and use the command:

   ```
   awplus#reload
   ```

Upgrading the Software of a VAA

VAA does not need to be the same release as the products it is managing, however, as VAA is intended to be used as an AMF Master or Controller, it is recommended it be on the latest release. Before you begin, you will first need to upload a VAA ISO image to a data store on your ESXi server. For the complete set of instructions on uploading a VAA ISO image, please refer to the VMware vSphere 6.0 Documentation Centre. To upgrade or downgrade the current installed image, you will need to change the current.iso software image in the virtual-machine configuration, then reboot the virtual-machine.

To change the current .iso software image:

- Power off the virtual-machine you wish to upgrade/downgrade.
- Edit the settings of the virtual-machine.
- Select CD/DVD Drive 1 item
- Ensure that **Connect at power on** check-box is ticked.
- Select the **Datastore ISO File** radio button.
- **Browse** for the desired VAA iso image.

Start the virtual machine, during boot you will see a menu that looks like this:

```
Alliedware+
Boot from CD
```

- Select the **Boot from CD** option.

You will only have 5 seconds to select "Boot from CD" before the boot continues with the previously installed release.

This will boot using the new .iso software image, and next time you login using the console you will be presented with the "*Install this release to disk? (y/n)*" option.

Upgrading a VAA running under Amazon Web Services (AWS)

To update an existing VAA running under AWS, follow these steps:

1. Download the file, for example: vaa-5.4.6-2.12.iso, and copy it onto the VAA.
2. Run the command **software-upgrade vaa-5.4.6-2.12.iso**

Important Information about Compatibility with Earlier Software Versions

Loss of auto-synchronization compatibility on VCS and on dual-CFC SBx8100 chassis

Auto-synchronization compatibility has not been maintained for VCStack or dual-CFC SBx8100 chassis between AlliedWare Plus version 5.4.6-1.2 and any previous software version (including v5.4.6-1.1).

This affects VCStack, standalone dual-CFC SBx8100 switches, and VCStack Plus.

Consequences for VCStacks

On VCStacks, the loss of auto-synchronization means:

1. If you want to upgrade an existing VCStack to 5.4.6-1.2, 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.

2. If a stack is running v5.4.6-1.2, and you connect a switch running an older release to the stack, then the v5.4.6-1.2 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 v5.4.6-1.2 before you add it to the stack.

3. If a stack is running an older release, and you connect a switch running v5.4.6-1.2 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.

4. 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.

Consequences for a single SBx8100

If you want to insert a new CFC into a chassis, the loss of auto-synchronization means:

1. If you want to upgrade an existing SBx8100 that has two CFCs installed to 5.4.6-1.2, 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.

2. If a standalone SBx8100 has a CFC installed that is running an older release, and you add a CFC running v5.4.6-1.2 to the chassis, then the older software cannot be automatically copied over to the newly-added CFC.
3. If a standalone SBx8100 has a CFC installed that is running v5.4.6-1.2, and you add a CFC running an older release to the chassis, then the v5.4.6-1.2 software cannot be automatically copied over to the newly-added CFC.
4. 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 5.4.6-1.2 and another CFC joins with 5.4.6-0.x, the error you get is:

```
======
cfc960 login: manager
Password:
Last login: Thu Aug 18 02:15:21 UTC 2016 on ttyS0
All 1 lines for VR:PVR are busy. Try again later
======
```

To recover from this situation, see "Upgrading/downgrading a CFC" on page 14.

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) v5.4.6
Current release filename: SBx81CFC400-5.4.6-1.2.rel
```

Consequences for a VCStack Plus Pair of SBx8100 chassis

If you are dealing with VCStack Plus, the effect of the loss of auto-synchronization depends on whether you are installing a new CFC or a whole new chassis:

1. If you want to upgrade an existing SBx8100 VCStack Plus system to 5.4.6-1.2, 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.
2. If you want to insert a new dual CFC into a chassis that is part of an existing VCStack Plus system, refer to "Consequences for a single SBx8100" on page 12.

3. If you want to insert a new SBx8100 chassis into a VCStack Plus system, refer to “Consequences for VCStacks” on page 12.

Upgrading/downgrading a CFC

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

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.
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.

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.

Additional information

		To Release										
FROM	Release	5.4.6-2.2	5.4.6-2.3	5.4.6-2.4	5.4.6-2.5	5.4.6-2.6	5.4.6-2.7	5.4.6-2.8	5.4.6-2.9	5.4.6-2.10	5.4.6-2.11	5.4.6-2.12
	5.4.6-2.1	C	I	I	I	I	I	I				
	5.4.6-2.2		C	I	I	I	I	I				
	5.4.6-2.3			C	I	I	I	I				
	5.4.6-2.4				C	I	I	I				
	5.4.6-2.5					C	I	I				
	5.4.6-2.6						C	I				
	5.4.6-2.7							I				
	5.4.6-2.8								C			
	5.4.6-2.9									C		
	5.4.6-2.10										C	
	5.4.6-2.11											C

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

Enhancements in 5.4.6-2.10

CR	Module	Description
ER-1483	**Security**	For: GS900, FS980, GS970, XS900, IE300, IE500, x230, x310, Ix5, x510, SBx908, x930, DC2552, SBx81CFC400, SBx81CFC960, AR4050S, AR3050S, AR2050V, AR2010V With this Software update, the Subject Alternative Name field in an X.509 certificate with RadSecProxy and Syslog is supported. ISSU: Effective when CFCs upgraded

Enhancements in 5.4.6-2.9

CR	Module	Description
ER-1507	**PoE**	With this software update, the PoE firmware on FS980 series switches has been updated.
ER-1508	**PoE**	With this software update, the PoE dynamic mode is now supported on FS980 series switches.

Enhancements in 5.4.6-2.8

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. With this command enabled, once you set the password you 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-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-1483	Security	For: x930 With this software update, RadSecProxy and Syslog now support Subject Alternative Name as part of the Common Criteria requirements.
ER-1489	IGMP	For: IE300, IE510, x310, IX5, x510, x610, x930, DC2500, SBx908, SBx81CFC400, SBx81CFC960, AR2050V, AR3050S, AR4050S, VAA. With this software update, it is now possible to have an address-less interface to operate as an IGMP mroute proxy interface. Note that for such interface to be able to send queries to hosts directly attached to the interface, it is necessary to enable IGMP snooping querier on the interface.

Enhancements in 5.4.6-2.7

CR	Module	Description

ER-1131	**TCP**	For x930 Series
		Enhancement: With this software updated, a new command is added to configure the number of SYN ACK retries the system kernel will attempt before discarding half open TCP connections.
		To configure the number of SYN ACK retries the kernel will attempt before discarding half open TCP connections, use the following command:
		`ip tcp synack-retries <0-255>`
		where `<0-255>` Sets how many times to retry sending a SYN ACK for a half open TCP connection before abandoning it.
		
		To set the number of SYN ACK retries back to the default of 5, use the following command:
		`no ip tcp synack-retries`
		
		The behaviour of the kernel results in the following approximate relations between retries and half open connection timeouts:
		0 retries ~ 1 second
		1 retry ~ 3 seconds
		2 retries ~ 7 seconds
		3 retries ~ 15 seconds
		4 retries ~ 31 seconds
		5 retries ~ 63 seconds
		These are approximate and represent lower bounds for the timeout rather than upper limits.
		ISSU: Effective when CFCs upgraded

Enhancements in 5.4.6-2.6

CR	Module	Description
ER-92	**Stacking**	For FS980M, XS900MX, IE510, x310, IX5, x510, x510L, x610, x930, DC2552XS/L3, SBx908, SB8100CFC400, SB8100CFC960: With this software update, a new command has been added to allow the removal of a file across all stack members. To delete a file across all stack members use the command: **delete stack-wide force [recursive] FILENAME** Note that the explicit **force** option will make this a non-interactive command with any file specified being removed without question if the file exists from all stack members. This command can be used within ATMF working sets.
ER-1103	**Firewall**	For AR3050S, AR4050S: With this software update, Firewall rules now have an "no-state-enforcement" option. This option should only be used when asymmetric routing is causing the firewall to block required traffic and there is no way to resolve the routing issues.
ER-1159	**Unicast Routing**	With this software update, the x310 variant switches are now capable of performing hardware switching to more remote destinations using routes that are not added to the hardware routing table. A new function has been added to allow remote hosts that are routed by the software to appear in the hardware IP host table, therefore enabling hardware switching to the remote hosts. This new feature can be enabled and disabled with the command **{{(no) fib cache-remote-host}}**

Enhancements in 5.4.6-2.3

CR	Module	Description
ER-1146	**PKI**	With this software update, the certificate-using processes like HTTPS connections to Webauth, HTTPS browsing to the switch, RestFUL API calls, etc., can now be pointed at a configured trustpoint, in the same way that SYLog-over-TLS and RADIUS-over-TLS can. The commands **auth-web-server trustpoint NAME** and **http trustpoint NAME** are added to link a certificate created in the specified trustpoint. The commands **no auth-web-server trustpoint NAME** and **no http trustpoint NAME** are added to remove the association with the trustpoint.
ER-147	**EPSR**	LACP links can now be configured as part of an EPSR ring. Please note that this enhancement applies **ONLY** to the following devices: SBx908, SBx81CFC400, SBx81CFC960, FS980M Series. EPSR is supported unchanged over LACP on all other devices.

Enhancements in 5.4.6-1.5

CR	Module	Description
ER-783	**Pluggable transceivers**	Previously there were some differences between switch devices with regard to which pluggable modules and cables could be used for stacking. With this software update, there is now no differing requirements between switches with regard to which pluggable modules and cables could be used for stacking.There is now a single definition for all switches that use stacking ports of the type that accept insertion of pluggable modules.

Enhancements in 5.4.6-1.2

CR	Module	Description
ER-1089	**SNMP**	IE200, IE300, IE510, x210, x230, x310, x510, x610, x930, IX5, DC2552XS/L3, x900, SBx908, SBx8100 CFC400, SBx8100 CFC960, AR2050, AR3050, AR4050, VAA With this software update, it is now possible to generate an SNMP trap when the *syslog-ng* process fails.

Enhancements in 5.4.6-0.3

CR	Module	Description

ER-809	**VLAN Classifier**	IE200, IE300, IE510, x210, x230, x310, x510, x610, x930, IX5, DC2552XS/L3, x900, SBx908, SBx8100 CFC400, SBx8100 CFC960, AR2050, AR3050, AR4050, VAA
		With this software update, it is now possible to configure VLAN classifiers directly on an aggregator interface (not on their member ports) using the command **vlan classifier activate**.
		Use this command in Interface Configuration mode to associate a VLAN classifier group with the switch port.
		Use the **no** variant of this command to remove the VLAN classifier group from the switch port.
		Syntax:
		`vlan classifier activate <vlan-class-group-id>`
		`no vlan classifier activate <vlan-class-group-id>`
		You cannot enter this command on a link aggregator. Enter it on the aggregator's switch ports instead.
		Example:
		To associate VLAN classifier group 3 with switch port1.0.3, enter the following commands:
		`awplus# configure terminal`
		`awplus(config)# interface port1.0.3`
		`awplus(config-if)# vlan classifier activate 3`
		To remove VLAN classifier group 3 from switch port1.0.3, enter the following commands:
		`awplus# configure terminal`
		`awplus(config)# interface port1.0.3`
		`awplus(config-if)# no vlan classifier activate 3`

ER-891	**Healthcheck**	Previously, on a stack of x310, IX5, x510, x610, x903 or DC2552 switches, under an extremely rare condition, a resiliency-link healthcheck packet would be corrupted during transmission and this corrupted packet would loop continuously around the resiliency-link VLAN, causing higher CPU utilisation than normal. With this software update, extra diagnostic logging has been added to detect a corrupted healthcheck packet. Also, additional internal software checks have been put in place to prevent a corrupted packet loop occurring.

ER-958	**VRRP**	x210, x230, x310, IX5, x510, x610, SBx908, x930, DC2552, SBx81CFC400, SBx81CFC960, AR3050S, AR4050S, AR2050V, IE200, IE300, IE510
		Previously, only one circuit-failover interface would be allowed per VRRP instance, so configuring a new circuit-failover interface would replace the existing one. With this software update, up to 32 circuit-failover interfaces can be configured and monitored per VRRP instance. The VRRP priority is cumulatively decremented/incremented when a circuit-failover interface goes down and up.
		This command adds a new circuit failover interface instead of overwriting existing one.
		`circuit-failover <interface> <1-253>`
		This command removes the circuit failover interface with the specified interface name.
		`no circuit-failover [<interface> <1-253>]`
		This command removes all circuit failover interfaces on a VRRP instance.
		`no circuit-failover`
		Example
		To configure circuit failover on an IPv4 VRRP instance, so that if interface VLAN3 goes down, then the priority of VRRP instance 1 is reduced by 30, use the commands:
		`awplus# configure terminal`
		`awplus(config)# router vrrp 1 vlan2`
		`awplus(config-router)# circuit-failover vlan3 30`

Issues Resolved in 5.4.6-2.12

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59919	**IGMP**	Previously, an IGMP snooping device might fail to respond to a Group Specific Query. This could lead to multicast data failing to forward downstream of that device until the next General Query was received by the device. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

Issues Resolved in 5.4.6-2.11

This AlliedWare Plus maintenance version includes the resolved issue described in the following table:

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-59557	**Firewall** **GUI**	Previously, it was possible to bypass user authentication and gain unauthorized access to an AR series device running AlliedWare Plus software version 5.4.5 or later. This issue was due to a vulnerability in a third-party package used by Allied Telesis AR series devices running AlliedWare Plus that provided HTTP and HTTPS access to the firewall GUI. Allied Telesis switches running AlliedWare Plus are not vulnerable. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

Issues Resolved in 5.4.6-2.10

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	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58838	**AMF**	Previously, the automated AMF backup process would be carried out on all stack members while it should be carried out on stack master. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	Y	–	Y	–	Y	Y	–	–	–	–
CR-58793	**API**	Previously, high rates of MAC address movement (for example, MAC thrashing) would cause unnecessary memory consumption. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–
CR-58981	**ARP**	Previously, packets ingressing on a NLB VLAN with a Microsoft NLB MAC address could be incorrectly routed. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–
CR-58562	**ARP** **Neighbor Discovery** **VRF-lite**	Previously, when using the flooding nexthop functionality (for example to facilitate Microsoft NLB) on a device, packets were not being inter-VRF routed correctly between VRF interfaces. This issue did not occur for intra-VRF routed packets. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	Y	–	–	–	–

CR-58756	**ARP Neighbor Discovery**	Previously, Microsoft NLB heartbeat packets could potentially reflect back out the ingress port of the switch and the same packets could potentially fail to egress out ports on other stack members. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–
CR-58437	**CLI**	Previously, changing console window size while **tech-support** was running in the background could induce a system reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded ISSU complete.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–
CR-58984	**Firewall**	Previously, removing an application that the firewall installed would cause unnecessary delay to the firewall configuration update. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-58729	**Health Check**	Previously, an x510 or x310 variant switch could sometimes fail to generate a core dump file if an operating system process failed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	y	–	–	–	–	–	–	–	–	–	–	–
CR-58664	**IGMP**	Previously, an interface running an IGMP proxy service could intermittently fail to send membership joins in response to a specific query sent by the querier, even though one or more mroute-proxy interfaces were members of the group specified within the query. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–

CR00057886	**L2TP**	Temporary communication disruption via L2TP could occur under some circumstances. Background: Communication via an L2TP site-to-site VPN (such as a L2TPv3 mode VTI terminating an Ethernet pseudo-wire) requires that each end of the VPN is assigned a MAC address and that the MAC address information is propagated to the peer via a mechanism, such as Gratuitous ARP (G-ARP) or ND protocol. Previously, a random MAC address was allocated to L2TP interface on startup. However, if one end of the L2TP VPN was unexpectedly terminated and re-established (such as shut/no shut on the VTI), then this could result in temporary communication disruption. This was because the peer was not aware of the new randomly allocated MAC address until it aged out its old peer MAC entry allowing the new MAC address to be learned. With this software update, the communication disruption is avoided. The L2TP VTI interface now uses a deterministic MAC address. The static MAC address of a physical interface that has the lowest ifindex is now allocated for use by the L2TP VPN instead of being randomly selected.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-58991	**PoE**	Previously, it was possible for the PoE LED to display incorrectly after a device reboot. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–

CR-57950	**RADIUS**	With this software update, RADIUS is upgraded to address the following vulnerabilities: CVE-2017-10978 An FR-GV-201 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows ""Read / write overflow in make_secret()"" and a denial of service. CVE-2017-10980 An FR-GV-203 issue in FreeRADIUS 2.x before 2.2.10 allows ""DHCP - Memory leak in decode_tlv()"" and a denial of service. CVE-2017-10981 An FR-GV-204 issue in FreeRADIUS 2.x before 2.2.10 allows ""DHCP - Memory leak in fr_dhcp_decode()"" and a denial of service. CVE-2017-10982 An FR-GV-205 issue in FreeRADIUS 2.x before 2.2.10 allows ""DHCP - Buffer over-read in fr_dhcp_decode_options()"" and a denial of service. CVE-2017-10983 An FR-GV-206 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows ""DHCP - Read overflow when decoding option 63"" and a denial of service." ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–
CR-58889	**SSH**	Previously, the number of failed logins since the last VTY login, was not printed when secure bootloader L3 was enabled. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	–	Y	Y	Y	–	Y	–	Y	Y	–	–	Y	Y	Y	–
CR--58935	**System**	Previously, if a device was writing a configuration to Flash and then the device was quickly powered off, it was possible that the configuration would not be saved. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–

CR-58064	**System**	Previously, a on rare occasions the device may have failed to boot up correctly if there was an I2C bus lockup. This issue has been resolved. SSU: Effective when CFCs upgraded	–	–	Y	–	–	–	–	–	–	Y	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–

Issues Resolved in 5.4.6-2.9

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	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-58042	**AMF**	With this software update, the stability of an AMF network on x930 and x510 variant switches with nodes that have more than 20 AMF links has been improved. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-58260	**AMF**	Previously, if there were more than 40 AMF links within an AMF network, the AMF network could become unstable if all the links came up simultaneously. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	Y
CR-57943	**AMF** **SNMP**	Previously, on a SBx81CFC400 controller, AMF SNMP traps for node or link status changes could cause excessive CPU load. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-58442	**ARP** **Neighbor Discovery** **VRF-lite**	Previously, when NLB was used in conjunction with VRF-Lite, any traffic forwarded outside of the default VRF based on static ARP entries could fail. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	–	–	Y	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57396	**System**	Previously, on devices using Bootloader version 5.1.6, the following erroneous startup log message could be displayed: "*an unsupported bootloader version*". This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-58019	**GUI**	Previously, when the firewall on a router was enabled, communication to the GUI could fail. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-57887	**IPv4 Unicast Routing**	Previously, a connected route was incorrectly removed from the FDB whilst associated port configuration changes were occurring, resulting in link flaps. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–
CR-58035	**LACP**	Previously, when using a static ARP with a multicast MAC address that used a LACP based aggregator as the nexthop port, the ports used to egress the frames would not be updated as ports were dynamically added or removed from the aggregator by LACP. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	–	–	Y	–	–	–	–	–	–	–
CR-58462	**Monitoring**	Previously, the fiber monitoring **shutdown** action would not take a port down after a link fail event. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57978	**OpenFlow**	Previously, there was a high latency between an OpenFlow client and an upstream host in establishing communication. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	Y	–	Y	–	Y	–	–	–	–	–	–	–	–	–
CR--57278	**PKI**	This software update will allow logging of all PKI related failures as part of the Common Criteria requirements.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-57282	**PoE**	Previously, a PoE device would not be detected correctly on FS980 series switches. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-57956	**PoE**	Previously, on FS908 variant switches, the output of the commands: **`show platform power-inline`** and **`show power-inline`** displayed PoE setting as "dynamic mode" even when the static mode was configured. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-58144	**Port Configuration**	Previously, on x930 variant switches, if the **wrr-queue disable** command was configured on a port, it was possible that the port would no longer correctly respond to link-down events, leaving the port showing as running. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-58082	**Port Configuration**	Previously, the device Ethernet port would not link up when it was configured with 10M full duplex mode. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57755	**Static Aggregation**	Previously, when using either of the **`arp mac-disparity`** or **`arp A.B.C.D <MULTICAST-MAC>`** commands on device, it was possible for traffic not to egress correctly. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y
CR-57665	**Switching**	Previously, a "soft" parity error within x930 series switches could result in a continuous output of parity error correction log displayed, and could eventually cause an internal process to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-57032	**VCStack**	Previously, x930 variant switches could restart unexpectedly when running the command **`show tech support`** soon after a failover. This issues has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-57920	**VCStack Hot-swap PBR**	Previously, failing over a stack member with policy-based-routing (PBR) configured and forwarding traffic that was targeting the PBR nexthop could increase the time the failover member took to join the stack. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	–	–	Y	–	–	–	Y	Y	Y	–	Y	–	Y	Y	Y	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57311	**VLAN**	Previously, when a port was configured to be a private-vlan with a trunk, and then the configuration was removed, the port would incorrectly remain configured as a private vlan port, so would not be able to operate as a regular trunk or access port. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–

Issues Resolved in 5.4.6-2.8

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	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56607	ACL	Previously, entering the **`no access-group`** command while in "config-ip-hw-acl" mode could result in an error. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–
CR-57188	AMF	Previously, enabling AMF on an IE200 variant switch could cause the switch to lock-up. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-57327	AMF	With this software update, the AMF time-out values have been increased on the SBx81CFC400 controller to avoid time-out of AMF members that are rejoining. In addition, the ATMF background scripts will now execute sequentially rather than in parallel.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-57349	AMF	Previously, an unexpected termination of background AMF processes could occur on a large AMF network with a VAA master. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y
CR-57789	AMF	Previously, after the command **`atmf cleanup`** was issued to reset a x230 variant switch to factory default, the autoboot feature would fail to work. This issue has been resolved.	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
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.	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.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-57053	ARP Neighbor Discovery	Previously, a switch could fail to register Multicast ARP on a channel-group. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-56873	EPSR VCStack	Previously, when adding a data VLAN to a blocked EPSR port in a stacked environment, it was possible that the data VLAN would not be blocked. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–
CR-57450	File System	Previously, there was a rare chance for a system lockup to occur while writing a file to a Flash device. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–
CR-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	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	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-57763	**IGMP MLD**	Previously, the switch could restart unexpectedly when disabling IGMP or MLD after learning many *,G entries for each of the respective protocols. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–
CR-57600	**IP Reputation NAT**	Previously, if flows in Suricata were in asynchronous mode, the flow would only close after a 5 minute time out. This is because Suricata would not be able to see the TCP FIN from the server. When a new flow was created, it was blocked as a TCP retransmission because the old flow was still open. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56817	**LACP Aggregation**	Previously, if a port was configured as a static aggregator and received an LACP BPDU, then an error message such as the following would be logged: ***"Failed learning dynamic channel-group: % The port port1.0.4 is already configured for static aggregation".*** When this log was produced, the device would permanently consume some memory, the amount which depended on the total number of interfaces (vlans, ports, any tunnels, etc.) available on the device. If the configuration was not changed to avoid the statically aggregated ports receiving the LACP BPDUs, then progressively more memory would be permanently and unnecessarily consumed over a long period of time. Eventually the device would run out of free memory and restart. This issue has been resolved, the error logs will still be produced in this case, but no memory will be consumed.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–
CR-57413	**Licensing**	Previously, when a stack master failover occurred and a stack member had an expired subscription license, it could result in other members to restart. This could occur when the last subscription license for a given feature on the member had expired after the member was last restarted and no other members had a non-expired subscription license for the same feature. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57038	**Logging**	Previously, you could enter a log configuration command to filter by program, for example: **`log (console|buffered|permanent) program...`** with **invalid** parameters. This issue has been resolved and an invalid program parameter is now rejected at the CLI. When running the fixed AlliedWare Plus version for the first time, an error might be logged at startup and the invalid config line will not show up in the running-configuration. After the first successful restart, you should save the running-configuration to the startup-configuration.	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y
CR-56963	**OSPFv2**	Previously, during a master failover, OSPF, BGP and IPv6 based 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	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57251	OSPFv2	Previously, when the **maximum paths** command was used to limit the number of ECMP nexthops for routes, after certain routing operations such as OSPF graceful restart, the output of **show ip route database** might have incorrectly marked more next-hops than the configured maximum paths as being installed into the FIB for some routes. The output of **show hsl fib** would indicate that these nexthops were not actually installed into the FIB. This issue has been resolved, the FIB status of nexthops displayed in **show ip route database** is now correct and in sync with the command **show hsl fib** output.	–	–	–	–	–	Y	Y	–	–	–	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	–
CR-57278	PKI	This software update will allow logging of all PKI related failures as part of the Common Criteria requirements.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-57287	PKI	This software update will prevent authenticating CA certificates when the basicConstraints extension is not set.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–
CR-56841	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	–	–	–	–
CR-57767	RESTful API	Previously, an internal RESTful API process could fail and low memory was reported on a device when there was a large number of neighbours being learnt or timing out. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y
CR-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.	Y	–	Y	Y	–	–	Y	–	–	–	Y	Y	Y	–	–	–	Y	Y	Y	Y	–	–	–	–

CR	Module	Description	FS980M	GS970M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56647	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	–	–	–	–
CR-55047	Switching	Previously, when a large number of multicast groups were present on a switch, it could cause the switch to process a port down event slower than it should have been. As a result, the switch could restart unnecessarily. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	–	–	–	–	–	–	–
CR-57460	System	Previously, on rare occasions when a software lockup was detected on a switch, a switch could restart without a generating core dump file. This issue has been resolved. The switch now generates a kernel core dump if there is a software lockup.	–	–	–	–	Y	–	–	Y	–	Y	Y	–	Y	–	–	–	–	–	–	–	–	–	–	–
CR-57093	TACACS+	Previously, for TACACS+ login authentication, the login start packet contained the user password. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	–
CR-56962	VCStack	Previously, if a switch had EAP forwarding enabled and a resiliency link configured, then a storm of EAP packets could be created. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–
CR-57026	VLAN	Previously, if a switch was configured as a RADIUS server, then dynamic VLAN assignment would not work by VLAN name. This issue has been resolved.	–	–	–	–	–	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	x220	x230	x310	IX5	x510, 510L	x610	x930	x950	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-57121	**VRF-lite**	Previously on a SBx908 switch, dynamically removing an interface's VRF association and adding it to a different one was not possible. 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.	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	Y

Issues Resolved in 5.4.6-2.7

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

CR	Module	Description	FS980M	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-56703	**AMF, NTP**	Previously, AMF members would incorrectly form NTP peer relationships with all directly connected nodes. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR--56956	**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. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-56911	**ARP Neighbor Discovery**	Previously, when DHCP snooping and ARP security were enabled, incoming ARP requests were reflected back out the ingress port. This issue has been resolved. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56682	**Bootup**	Previously, on IE300 variant switches, the **alarm facility** command was not being executed from the configuration file at boot up. This issue has been resolved.	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-57070	**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	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-56415	**Firewall**	With this software update, custom applications of protocol ICMPv6 will now use the **icmp-type** and **icmp-code** options.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	FS980M	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-56937	**Firewall**	With this software update, entities will now update more accurately when multiple subnets are dynamically configured. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-56625	**IGMP**	Previously, IGMP-Proxy service might send group reports in reply to group (source-group) specific query sent by an upstream IGMP router even though all IGMP-proxy downstream members of the groups had already left. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–
CR-56654	**IGMP**	Previously, changing IGMP parameters on an upstream IGMP proxy interface could cause all proxy downstream interfaces to incorrectly inherit the IGMP parameters used on the upstream interface, potentially causing proxy operation to fail. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–
CR-56486	**IGMP**	Previously, an unexpected error would occur when handling an IGMPv3 for the member which was already removed. 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-56812	**IPv6**	Previously, setting MTU on a VLAN interface would not take effect until the interface was shut down and brought up again. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	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-56939	**IPv6**	Previously, the XS900 variant switches would fail to send ICMP redirect in response to receiving Layer 3 packets switched in and out the same VLAN, despite being configured to do so. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-56498	**Logging**	With this software update, the following additional log messages have been added in order to meet the Common Criteria Requirement: 1. Error message for all failed commands are logged. These include execution of: - incomplete or ambiguous commands - misspelled or non available commands - commands in wrong configuration modes i.e. User Exec mode, Privileged Exec mode, Global Configuration mode etc. - privileged commands by non-privileged user 2. An additional message "% Verification Successful" is displayed and logged when verification of a build is successful.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56507	**Logging PKI**	With this software update, TLS is now able to log all critical failures along with the reason for the failure as part of the common criteria requirements.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56328	**Malware Protection**	Previously, on a NGFW router, the Suricata process could restart unexpectedly when the Malware protection feature was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	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-56789	**Malware Protection**	Previously, simultaneously enabling all stream-based UTM features (IP Reputation, IPS, Malware Protection, URL Filtering, DPI) might eventually cause the router to restart unexpectedly if it is subjected to sustained high load over many days. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56863	**NTP** **AMF**	Previously, in some cases AMF masters could configure themselves as an NTP peer. This was undesirable. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	Y	–	–	Y	Y
CR-56714	**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. ISSU: Effective when CFCs upgraded	–	–	–	–	Y	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56485	**PKI**	With this software update, the PKI certificates with OCSP URL are now checked for revocation status upon import using OCSP. Import will fail if the OCSP server responds and indicates that the certificate has been revoked.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56057	**PoE**	Previously, PoE ports were showing incorrect powered status. This issue has been resolved. ISSU: Effective when ISSU completed	Y	Y	Y	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	Y	Y	–	–	–	–

CR	Module	Description	FS980M	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-56991	**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. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-56439	**Security**	Previously, on x930 variant switches, verification of a release file against its hash value (used for release file validity checking) could fail during startup after a reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56815	**Switching**	Previously, the output of the **show platform swtable SiliconResourcesUtilization** command showed an incorrect number of lpmIpv4UcPrefixes on the SBx81XLEM following a card reboot. This issue has been resolved. ISSU: Effective when CFCs upgraded	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-56071	**System**	Previously, there was a small chance that the SBx81LIFv1 variant line cards would not be initialized correctly. This issue has been resolved. ISSU: Effective when ISSU completed	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-56801	**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. ISSU: Effective when CFCs upgraded	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR-53470	**VCStack**	Previously, on rare occasions, an unexpected restart of some processes could occur on a switch. This issue has been resolved.	–	–	–	–	–	–	Y	–	Y	–	Y	–	–	–	–	–	–	–	–	–	–

Issues Resolved in 5.4.6-2.6

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

CR	Module	Description	FS980M	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-56293	802.1x	Previously, in a port configuration with **auth dynamic-vlan-creation type multi** configured, hitting the limit of the number of times of authorisation and un-authorisation would stop packets being forwarded on x930 variant switches. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56394	Anti-virus Nat Web Control	Previously, packets that were either "port forwarded" or "destination subnet translated" would not be processed by either Antivirus or Web Control. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56292	ARP / Neighbor Discovery, Multicast Forwarding - HW	Previously, if a SBx8100 chassis was running silicon-profile 3 host mode, the output of **show platform table ip** command would display incorrect information. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-55365	BGP	Previously, using the command **clear BGP*** on a remote device would clear BGP sessions. However, the local BGP peer would not send out the default route even if "default-originate" was enabled for a re-established session. This issue has been resolved. ISSU: Effective when ISSU complete.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–

CR	Module	Description	FS980M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR30505/AR40505	AMF Cloud
CR--56100	**CLI**	Previously, the output of the command **show platform table MAC** was inconsistent across the stacked FS980 variant switches. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-56201	**CPU**	Previously, the average CPU utilisation output of the **show CPU** command would display abnormally high values if the device was running for a prolong period of time. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56294	**Environmental Monitoring**	Previously, upon boot up, the initial fan speed was below the minimum documented fan speed of 4700 RPM. With this software update, the initial fan speed is now set to 5500 RPM, which is a higher value than the minimum documented speed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56300	**EPSR**	Previously, when adding a data VLAN to an EPSR domain on a stacked switch, the VLAN would fail to be blocked. This issue has been resolved.	–	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-54640	**Flow Control**	Previously, back pressure and flow control on x510 variant switches did not work. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-56134	**GUI**	Previously, login to the GUI could take longer than expected. 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	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-56365	**IGMP**	Previously, the device was unable to handle a Type 6 IGMPv3 Leave query because the snooping querier was not included in the **Group-and-Source-Specific Query**. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56486	**IGMP**	Previously, an unexpected error would occur when handling an IGMPv3 for the member which was already removed. 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-56496	**IGMP**	Previously, IGMP fast-leave was not working for IGMPv3 Type 6 Leaves (Block old sources). 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-55820	**Logging**	Previously, parity error messages were being logged every 5 minutes. However, this was not affecting the functionality and performance of the switch. This issue has been resolved.	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–

CR	Module	Description	FS980M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR30505/AR40505	AMF Cloud
CR-56498	**Logging**	With this software update, the following additional log messages have been added in order to meet the Common Criteria Requirement: 1. Error message for all failed commands are logged. These include execution of: • incomplete or ambiguous command • misspelled or non available command • commands in wrong configuration modes i.e. User Exec mode, Privileged Exec mode, Global Configuration command mode etc. • privileged command by non-privileged user 2. An additional message "% Verification Successful" is displayed and logged when verification of a build is successful. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56232	**Malware Protection**	Previously, with Malware protection enabled, the Suricata process could restart unexpectedly, irrespective of the traffic rate. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56230	**OpenFlow**	Previously, an OpenFlow capable switch would sometimes fail to forward DHCP packets from a DHCP server. This issue has been resolved.	–	Y	Y	–	–	–	–	Y	Y	Y	Y	–	Y	Y	–	–	–	–	–	–	–
CR-56391	**OpenFlow**	Previously, an OpenFlow switch was unable to forward multicast/broadcast traffic under certain situations. Also, ACL entries would remain in the field processor after an OpenFlow switch restarted unexpectedly These issues have been resolved.	–	Y	Y	–	–	–	–	Y	Y	Y	Y	–	Y	–	–	–	–	–	–	–	–

CR	Module	Description	FS980M	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-56493	**PKI**	Previously, RadSecProxy was not handling Subject Alternative Name as per RFC 6125, as required by Common Criteria. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56299	**PoE**	Previously, PoE devices would sometimes be disconnected by an unexpected PoE hardware restart. This issue has been resolved.	–	Y	Y	–	Y	Y	–	–	–	Y	Y	Y	Y	Y	–	–	–	–	–	–	–
CR-56197	**Port Authentication**	Previously, customising the Web Authentication page using the style.css and logo did not work correctly. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-56006	**Port Configuration**	Previously, manual 10M speed and full duplex would not be accepted in x930 variant switches if the SFP and copper ports were not populated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56434	**Stacking Security**	Previously, in Secure Mode (Common Criteria), port number 111 used by the port-mapper program was not blocked as it should be. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56327	**System**	Previously, a parity error on the register table used for multicast would not be automatically corrected on x510 variant switches. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–
CR-56251	**Traffic Control**	Previously, the default application for traffic-control of the type "any" was not visible via the WebAPI. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	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-56393	**Triggers**	Previously, a protocol module disconnection could result in a failure of a link-down trigger to activate. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56494	**Unicast Routing**	Previously, the static route configuration between stack members might not match after adding static routes with VLAN interfaces specified as the nexthop. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-56332	**URL Filtering** **Malware Protection** **Update Manager**	Previously, when any of the UTM stream features (IP Reputation, IPS, or URL Filter) had its resource update interval set to "never", after the router was booted up with a software release version different to the one running when the resource was last updated, "show ip-reputation" would incorrectly show the status as "Enabled (loading)" while it should have shown as "Enabled (inactive)" until the resource was next updated. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56344	**VRF-lite** **VRRP**	Previously, when both VRRP and VRF were configured on an interface, the interface would fail to resolve the ARP gateway information across VRF. This resulted in a lack of response to ARP requests received via an interface that was a member of a non-default VRF instance. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	–	Y	Y	–

CR	Module	Description	FS980M	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-56395	**VRRP**	Previously, when running silicon-profile 3 and fd-l3-hosts mode on a SBx8100 chassis with VRRP (master or backup) configured, it might not be capable of L3 routing to hosts at full line rate if the VRRP virtual MAC had been learnt dynamically prior to the unit taking VRRP mastership. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–
CR-56224	**VRRP** **Web Control**	Previously, when Web-control was enabled and clients were routing via an interface configured with VRRP, Web-control would fail to match rules specified to match that VRRP interface. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56636	**Web Control**	Previously, deleting web control custom categories would cause a NGFW router to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56296	**xSTP**	Previously, adding a VLAN into an existing MST instance could result in a broadcast storm. 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 5.4.6-2.4

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

CR	Module	Description	FS980M	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-56148	**NTP**	Previously, NTP would fail to synchronize the time.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56219	**IDS/IPS** **IP Reputation** **Malware Protection** **URL Filtering**	Previously, the Suricata process would look like it was using 100% of the CPU even when there was no load. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56272	**Firewall** **NAT**	Previously, when using the WebAPI to configure a Firewall NAT rule, it was possible to create a **portfwd rule** in the running config that was invalid. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

Issues Resolved in 5.4.6-2.3

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

CR	Module	Description	FS980M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56049	**ACL** **DHCP Snooping**	Previously, the DHCP Snooping database would not be correctly written to non volatile memory on x210 and x230 variant switches. This issue has been resolved.	–	–	–	–	–	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-56053	**AMF**	Previously, a software initialization issue would incorrectly set the internal AMF backup state and prevented the backups from being triggered. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	Y	–	–	Y	Y
CR-56054	**Antivirus** **Webcontrol**	Previously, if two AlliedWare Plus routers had the proxy-based features Web-control or Antivirus enabled, the second device could falsely detect a forwarding loop and block the HTTP traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56062	**ARP** **Neighbor Discovery**	Previously, IPv4 ARP and IPV6 ND entries that used port-groups or flood to a VLAN would not be correctly synchronized across stack members during a stack failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	–	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–

CR	Module	Description	FS980M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56168	**BGP**	Previously, when BGP password authentication was configured on an AR-Series Firewall, the BGP session with its peer would not be successfully established. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-55910	**CLI**	Previously, entering the command: **copy <file> startup-config** could cause a system reboot if the operation was invalid. This issue has been resolved.	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–
CR-56131	**DPI** **Malware Protection** **URL Filtering**	Previously, if two feature resource updates occurred at a similar time, it was possible for the stream engine to be restarted. As a result, a leak of queued hardware buffers could occur. In the worst case, it could reduced the hardware buffer pool to a level where no packets could then be transmitted or received. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-55406	**Firewall**	Previously, changing the configuration of an entity used in a firewall rule would not trigger an update of the rule. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56147	**Firewall**	Previously, if a zone was used in a Firewall rule, a traffic-shaping rule, or NAT rule and that zone had two networks with the same IP subnet range, then an error would be produced and the rule would never become active. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

CR	Module	Description	FS980M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR--56008	**Firewall VRF-lite**	Previously, a host attached to a VLAN on an AR-series firewall could not ping an interface in a VRF instance when the firewall module was enabled. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-55249	**IPv4**	Previously, the dot1q ETH sub-interfaces could occasionally fail to forward traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-55901	**IPv4**	Previously, when a VLAN was configured to be 'shutdown' and after the first port in that VLAN was linked up, the switch would incorrectly add an interface route to the hardware table, resulting in high CPU load. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
CR-56037	**IPv6**	Previously, if a prefix was explicitly specified to be advertised in an IPv6 router advertisement, the prefix would be advertised twice in the same RA packet with conflicting life times. This resulted in confusion in hosts processing the router advertisement. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–	Y	Y	Y	–	–	Y	–
CR-56098	**NTP**	This software update addresses multiple NTP denial of service vulnerabilities that is stated under "Vulnerability Note VU#633847". ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–
CR-56140	**NTP**	Previously, the hardware clock would not be synchronised correctly with NTP time. This issue has been resolved.	–	–	–	–	–	–	Y	–	Y	–	Y	–	–	–	–	–	Y	Y	Y	–

CR	Module	Description	FS980M	GS900MX	XS900MX	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-56112	**RMON**	Previously, the AlarmValue and AlarmThreshold were incorrectly displayed as "0" in the SNMP trap. This issue has been resolved.	Y	–	Y	–	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–
CR-55913	**Stacking**	Previously, if a member of an x930 stack was restarted from the CLI, there was a chance that one of the stack ports would fail to re-join the stack. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-51836	**Stacking**	Previously, rebooting a LIF card or a stack member on a SBx8100 with CFC960 could result in a memory leak. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-55821	**System**	Previously, an uncorrected "L3 Parity Error" would result in the "parity log" error to be displayed continuously, unnecessarily filling up the log table. This type of parity error can be automatically corrected and the issue has been resolved without flooding the log table. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–	–

Issues Resolved in 5.4.6-2.2

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

CR	Module	Description	FS980M	IE200	IE300	IE510	x210	x230	x310	x350	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-55910	**CLI**	Previously, entering the command: **copy <file> startup-config** could cause a system reboot if the operation was invalid. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–
CR-55913	**Stacking**	Previously, if a member of an x930 stack was restarted from the CLI, there was a chance that one of the stack ports would fail to re-join the stack. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-56037	**IPv6**	Previously, if a prefix was explicitly specified to be advertised in an IPv6 router advertisement, the prefix would be advertised twice in the same RA packet with conflicting life times. This resulted in confusion in hosts processing the router advertisement. This issue has been resolved.	–	–	–	–	–	–	Y	–	Y	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	–
CR-56054	**Antivirus Webcontrol**	Previously, if two devices had the proxy-based features Web-control or Antivirus enabled, the second device could falsely detect a forwarding loop and block the HTTP traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-56055	**Antivirus**	Previously, Antivirus on the device would not handle HTTP responses, for example, the "302 redirect," correctly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

Issues Resolved in 5.4.6-1.5

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

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	x350	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-55337	**802.1x** **Malware Protection** **PPPoE**	Previously, the 802.1q tagged packets that contained PPPoE session headers would not be processed by the Malware Protection engine. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-55328	**AMF**	Previously, the AMF auto-recovery would occasionally fail to work. This issue has been resolved.	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	–	–	–	Y
CR-54815	**Energy Efficient Ethernet**	With this software update, the supported port speed on the SBx81XLEM/XT4 expansion module for the SBx81XLEM is limited to 10G only when EEE is enabled. In other words, the port will only go into EEE mode when it is running at 10G speed. If the port is running at 1G, it will not be able to go into EEE mode.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-55372	**HTTP Service**	Previously, it was possible to access the HTTP SSL certificates and HTTP server configuration over HTTPs without authentication if a GUI was not installed. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	–	–	Y	–
CR-55034	**Logging** **Switching**	Previously, there was an unnecessary amount of logging of the Layer 2 switching processes to the tech-support. With this software update, this logging has been reduced to a more useful amount.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-55246	**SSH**	With this software update, as required by Common Criteria, the ECDSA host and user key generation for SSH is now supported in secure mode.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	x350	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-55423	**SSH**	Previously, SSH did not work with Digital Signature Algorithm (DSA). This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	Y	Y	Y	–	–	Y	–
CR-55472	**SSH**	Previously, in the crypto secure mode, it was possible to select DSA and RSA1 public key-chain to known hosts. This should not be allowed under Common Criteria secure mode. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-55592	**SSH**	With this software update, the DSA with diffie-hellman group1 key exchange algorithm is re-enabled for SSH server.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-55292	**Stacking**	Previously, on a SBx8100 stack, a backup member rejoining the stack could fail to rejoin due to software lock-up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–
CR-55311	**System**	Previously, on an AR-Series router, the firewall TCP connection timeout would reset to the default value of 300 seconds, even if it was configured to a different timeout value. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–
CR-55342	**Triggers**	Previously, there was a delay before linkdown triggers would execute their associated script(s). This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-55605	**VRRP**	SH310, IE200, IE300, x230, x310, IX5, x510, x610, SBx908, x930, DC2552, SBx81CFC400, SBx81CFC960, AR4050S, AR3050S, AR2050V Previously, a VRRP role change from backup to master would occasionally cause packets to be routed via the CPU rather than in hardware, and hence severely impacted the performance of the switch. This issue has been resolved.	–	–	–	–	Y	Y	–	Y	–	Y	Y	Y	Y	Y	Y	–	Y	Y	Y

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	x350	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-55451	**Web Control**	With this software update, Web Control now consumes less system resources whilst blocking an HTTP POST.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–

Issues Resolved in 5.4.6-1.4

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S	AR4050S	VAA
CR-55440	**Stacking**	Previously, on certain x510, x610, and DC2500 variant switches, when stacking was disabled, pluggable modules could fail to be detected by the switch in combo ports, SFP+ ports or QSFP ports and would not be shown in the command **show system pluggable**. This issue has been resolved.	–	–	–	–	–	–	–	Y	Y	–	Y	–	–	–	–	–	–	–	–

Issues Resolved in 5.4.6-1.3

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

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S	AR4050S	VAA
CR-55297	**Malware Protection**	Previously, IDS could restart unnecessarily after a Malware protection resource file update occurred. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-55327	**802.1x**	Previously, a supplicant that was connected to a switch via MAC-based authentication would only be successfully authenticated once. If the MAC authentication failed, then the supplicant could fail to be re-authenticated unless the **clear mac** or **dot1x init** command was issued. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y	Y	–	–	–	–	–

Issues Resolved in 5.4.6-1.2

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

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S	AR4050S	VAA
CR-55203	**AMF**	Previously, a switch configured as an AMF controller would reboot unexpectedly due to unnecessary memory consumption. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-55191	**Antivirus**	Previously, HTTP traffic may have been improperly blocked when Antivirus protection was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–
CR-55278	**DPI Firewall**	Previously, if an AR Series Firewall was already running under high load, DNS changes on the unit could cause Antivirus or Web Control to block all HTTP traffic. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-55217	**Environmental Monitoring**	Previously, the speed of the fan on a DC2500 Series switch would not return to normal speed after restart. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-55295	**Environmental Monitoring**	Previously, entering the **show system** command on a CFC400 would not display the DC power supply unit. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–
CR-55051	**GUI** **SNMP**	Previously, the SBx8100 series switches used incorrect indexing for the resource MIB. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S	AR4050S	VAA
CR-54655	**Hardware Health Monitoring**	Previously, on extremely rarely occasions, the backplane ports of a VCS plus switch might not link up after a system reboot. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-54971	**Hot Swap**	Previously, rebooting a line card would sometimes cause a CFC960 to restart unexpectedly. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–
CR-55066	**IDS, IPS**	Previously, FTP throughput on AR-series firewalls was less than expected when the intrusion detection feature was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	Y	–
CR-55157	**Pluggable Transceivers**	Previously, the "Methode Elec 40G DAC" cable with part number "S1348" was not recognised on the SBx81XLEM. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–	–	–	–	–
CR-55200	**Pluggable Transceivers**	Previously, the ports on the SBx81GS24a line card would display "down" in the output of the command **show interface** even when they were linked up. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-55323	**PPP** **Malware Protection**	Previously, packets received on an Ethernet interface that had PPPoE session headers, were not being scanned by some Malware detection processes, even when the Malware protection was enabled. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	Y	–
CR-55250	**System Bootup**	Previously, it was possible for continuous reboot prevention to fail to detect process failures. This issue has been resolved.	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–	–	–	–

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, 510L	x610	x930	DC2552XS/L3	SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2010V	AR2050V	AR3050S	AR4050S	VAA
CR-55321	**System Bootup**	With this software update, it is now possible to configure the **atmf controller** command even if the device does not have an AMF controller license installed on it. However, the controller feature will not actually function until a valid AMF controller license is added. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-55109	**VCStack Trigger**	Previously, when triggers were used to change configuration on a stack, it was possible for part of the configuration to be lost in an failover event. Any OSPF, RIP and BGP configuration would be affected. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR-55096	**VRF-lite**	Previously, if a switch was configured with a VRF interface, the following error message would appears in log after reboot: *"[DECODE] Open: Invalid Router ID"* This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–

Issues Resolved in 5.4.6-0.3

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

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR2010	AR3050	AR4050	VAA
CR-53339	**AMF**	Previously, when an AMF node was replaced and automatically recovered, it occasionally failed to communicate with the adjoining AMF node for recovery file retrieval, causing the recovery to fail. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR-54357	**AMF**	Previously, the "no valid release license" error message would be displayed at login on an AMF Cloud Master or Controller even though there was a proper license installed. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
CR-54391	**AMF**	Previously, the AMF Link Information Database was not updating correctly when a transition event occurred. For example, when a 'master' transitioned to a 'member' and vice versa, the event was not reflected on the Link Information Database. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
CR-54108	**CLI**	Previously, the ***alarm relay*** output from the command **show system environment** on a stacked IE510 switch, was inconsistent across stack members. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR2010	AR3050	AR4050	VAA
CR-54389	**IGMP**	Previously, repeated IGMP group Join and Leave events could cause a slow memory leak. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–
CR-54488	**IGMP, Multicast Routing**	Previously, a switch could unnecessarily log info-level messages like 'Stopping STAT timer' and 'Starting STAT timer with 210 seconds' when static IGMP groups were configured. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–
CR-53205	**LACP**	Previously, configuring static or dynamic link aggregation on an IE200 switch was not working as expected. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-53705	**OSPFv3**	Previously, adding an IPSec authentication on a VLAN interface with already established OSPFv3 neighbours would cause a "*Failed to write IPSec interface configuration*" error message being logged, although the IPSec configuration had been successfully implemented. The error message was spurious. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	–	–	–	–	–	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR2010	AR3050	AR4050	VAA
CR-52980	**OSPFv3, IPv6, Stacking**	Previously, there was a small chance that IPv6 routes leant by OSPFv3 could be installed without the link-local nexthop address set. This affected the traffic forwarding for all intra-area and AS external prefixes associated with that missing nexthop. This issue has been resolved. ISSU: Effective when CFCs upgraded.	–	–	Y	–	–	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y	–
CR-51527	**PoE**	Previously, on an IE200 switch, if the "*power-inline usage-threshold*" was reached and then set to a higher value, no SNMP trap would be sent after a PoE-device was disabled or unplugged. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-54432	**PoE**	Previously, the PoE Firmware Updater on the SBx81GP24 Line card might fail to run a firmware update. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-54224	**Policy-based Routing**	Previously, policy-based routing would still route packets as per the configured rule even if the destination network was unavailable. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	Y	Y	–
CR-54326	**QoS Hardware**	Previously, attaching a policy-map on a port would cause an IE200 switch to reboot unexpectedly. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

CR	Module	Description	IE200	IE300	IE510	x210	x230	x310	IX5	x510, x510L	x610	x930	DC2552XS/L3	x900 / SBx908	SBx8100 CFC400	SBx8100 CFC960	AR2050	AR2010	AR3050	AR4050	VAA
CR-54312	**QoS hardware**	Previously, on a IE200 switch, some traffic such as STP and LLPD was being incorrectly allocated to a lower priority queue on the link between the switch chip and the CPU. This could result in these packets being lost if a high rate of less important data was being sent to the CPU. This issue has been resolved.	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-54213	**System**	Previously, the error message: "ECO *button could not be found"* was displayed at bootup, even though the IE300 switch does not have an ECO button. This issue has been resolved.	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
CR-54382	**System**	Previously, the SBx81XLEM linecard could restart unexpectedly. This issue has been resolved. ISSU: Effective when ISSU complete.	–	–	–	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–
CR-54407	**System**	Previously, the device would send packets from the CPU via an incorrect CPU priority queue. This issue has been resolved.	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–	–
CR-54535	**Unicast Routing**	Previously, equal-cost multi-path routing was not working properly. 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	–