Software Maintenance Release Note

AlliedWare Plus™ Software Version 5.4.6-1.3

For SwitchBlade x8100, SwitchBlade x908, DC2552XS/L3, x930, x610, x510, IE200, IE300, IE500 Series Switches, IX5, x310, x230, x210, 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 5.4.6-1.3.

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
GS900MX/MPX	GS900	GS900-5.4.6-1.3.rel	Sept 2016	GS900-gui_546_11.jar
XS900MX	XS900	XS900-5.4.6-1.3.rel	Sept 2016	XS900-gui_546_11.jar
x210-9GT x210-16GT x210-24GT	x210	x210-5.4.6-1.3.rel	Sept 2016	x210-gui_546_11.jar
x230-10GP x230-18GP x230-28GP	x230	x230-5.4.6-1.3.rel	Sept 2016	x230-gui_546_11.jar
x310-26FT x310-50FT x310-26FP x310-50FP	x310	x310-5.4.6-1.3.rel	Sept 2016	x310-gui_546_11.jar
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	IE200-5.4.6-1.3.rel	Sept 2016	ie200-gui_546_11.jar
IE300-12GP IE300-12GT	IE300	IE300-5.4.6-1.3.rel	Sept 2016	n/a
IX5-28GPX		IX5-5.4.6-1.3.rel	Sept 2016	IX5-gui_546_11.jar
x510-28GTX x510-52GTX x510-28GPX x510-52GPX x510-28GSX x510-28GSX-80 x510DP-28GTX x510DP-52GTX x510L-28GT x510L-28GP x510L-52GT x510L-52GP	x510	x510-5.4.6-1.3.rel	Sept 2016	x510-gui_546_11.jar
IE510-28GSX-80	IE500	IE510-5.4.6-1.3.rel	Sept 2016	IE510-gui_546_04.jar
x610-24Ts x610-24Ts-POE+ x610-24Ts/X x610-24Ts/X-POE+ x610-24SPs/X x610-48Ts x610-48Ts-POE+ x610-48Ts/X x610-48Ts/X-POE+	x610	x610-5.4.6-1.3.rel	Sept 2016	x610-gui_546_11.jar

Table 1: Supported switch models and software file names

Models	Series	Release File	Date	GUI file
SwitchBlade x908*	SBx908	SBx908-5.4.6-1.3.rel	Sept 2016	SBx908-gui_546_11.jar
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	x930-5.4.6-1.3.rel	Sept 2016	x930-gui_546_11.jar
DC2552XS/L3		dc2500-5.4.6-1.3.rel	Sept 2016	dc2500-gui_546_11.jar
SBx81CFC400 SBx81CFC960	SBx8100	SBx81CFC400-5.4.6-1.3.rel SBx81CFC960-5.4.6-1.3.rel	Sept 2016	SBx81CFC400_gui_546_11.jar SBx81CFC960_gui_546_11.jar
AR2010V AR2050V	VPN Firewalls	AR2010V-5.4.6-1.3.rel AR2050V-5.4.6-1.3.rel	Sept 2016	n/a
AR3050S AR4050S	NGFW	AR3050S-5.4.6-1.3.rel AR4050S-5.4.6-1.3.rel	Sept 2016	n/a
VAA (Virtual AMF Appliance)		vaa-5.4.6-1.3.iso	Sept 2016	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.

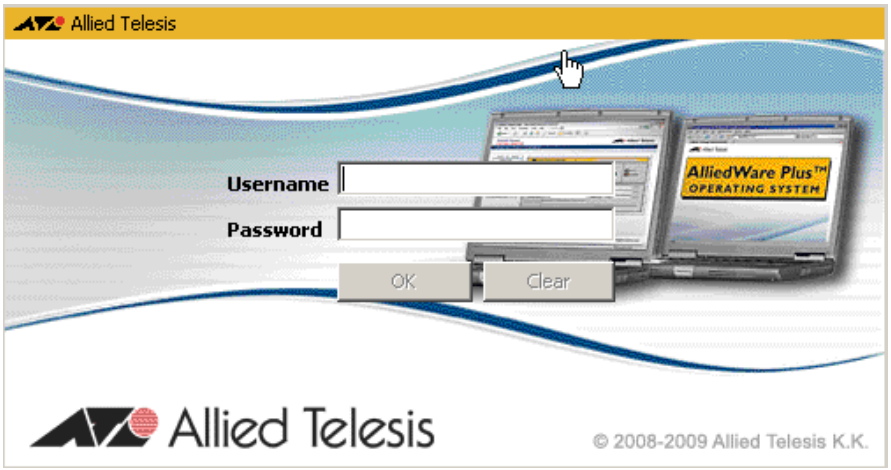
8. **Enter the URL in the Java Control Panel Exception Site List.**

   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 x210-5.4.6-1.3.rel
   ```

   On the x230 Series switches, use the command:

   ```
   awplus(config)#boot system x230-5.4.6-1.3.rel
   ```

   On the x310 Series switches, use the command:

   ```
   awplus(config)#boot system x310-5.4.6-1.3.rel
   ```

   On the x510 Series switches, use the command:

   ```
   awplus(config)#boot system x510-5.4.6-1.3.rel
   ```

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

   ```
   awplus(config)#boot system ix5-5.4.6-1.3.rel
   ```

   On the x610 Series switches, use the command:

   ```
   awplus(config)#boot system x610-5.4.6-1.3.rel
   ```

   On the SwitchBlade x908, use the command:

   ```
   awplus(config)#boot system SBx908-5.4.6-1.3.rel
   ```

   On the x930 Series switches, use the command:

   ```
   awplus(config)#boot system x930-5.4.6-1.3.rel
   ```

   On the DC2552XS/L3 switch, use the command:

   ```
   awplus(config)#boot system dc2500-5.4.6-1.3.rel
   ```

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

```
awplus(config)#boot system SBx81CFC400-5.4.6-1.3.rel
```

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

```
awplus(config)#boot system SBx81CFC960-5.4.6-1.3.rel
```

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

```
awplus(config)#boot system AR2010v-5.4.6-1.3.rel
awplus(config)#boot system AR2050v-5.4.6-1.3.rel
awplus(config)#boot system AR3050S-5.4.6-1.3.rel
awplus(config)#boot system AR4050S-5.4.6-1.3.rel
```

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

```
awplus#show boot
```

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

```
awplus(config)#boot system GS900-5.4.6-1.3.rel
```

On the XS900MX Series switches, use the command:

```
awplus(config)#boot system XS900-5.4.6-1.3.rel
```

On the IE200 Series switches, use the command:

```
awplus(config)#boot system IE200-5.4.6-1.3.rel
```

On the IE300 Series switches, use the command:

```
awplus(config)#boot system IE300-5.4.6-1.3.rel
```

On the IE500 Series switches, use the command:

```
awplus(config)#boot system IE500-5.4.6-1.3.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-5.4.6-1.3.iso, and copy it onto the VAA.
2. Run the command **software-upgrade vaa-5.4.6-1.3.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 13.

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 11.
3. If you want to insert a new SBx8100 chassis into a VCStack Plus system, refer to “Consequences for VCStacks” on page 11.

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.

This maintenance release cannot be upgraded from any previous release using ISSU.

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.

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

		TO						
FROM	RELEASE	5.4.6-0.1	5.4.6-0.2	5.4.6-0.3	5.4.6-0.4	5.4.6-1.1	5.4.6-1.2	5.4.6-1.3
	5.4.6-0.1		C	I	I	I	I	I
	5.4.6-0.2			C	I	I	I	I
	5.4.6-0.3				C	I	I	I
	5.4.6-0.4					I	I	I
	5.4.6-1.1						I	I
	5.4.6-1.2							C
	5.4.6-1.3							

Additional information

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

ISSU is not supported on other platforms.

You may also find the following How To Note useful:

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

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 5.4.6-1.3

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

CR number format: A new issue tracking system is being introduced. The CRs in the new system use a new format (CR-5xxxx). The previous system used the format: CR000xxxx.

For the next while, both systems will be used and both formats may appear in these tables. When referring to CRs, use the full CR format, e.g. CR-5xxxx.

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	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-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-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	–