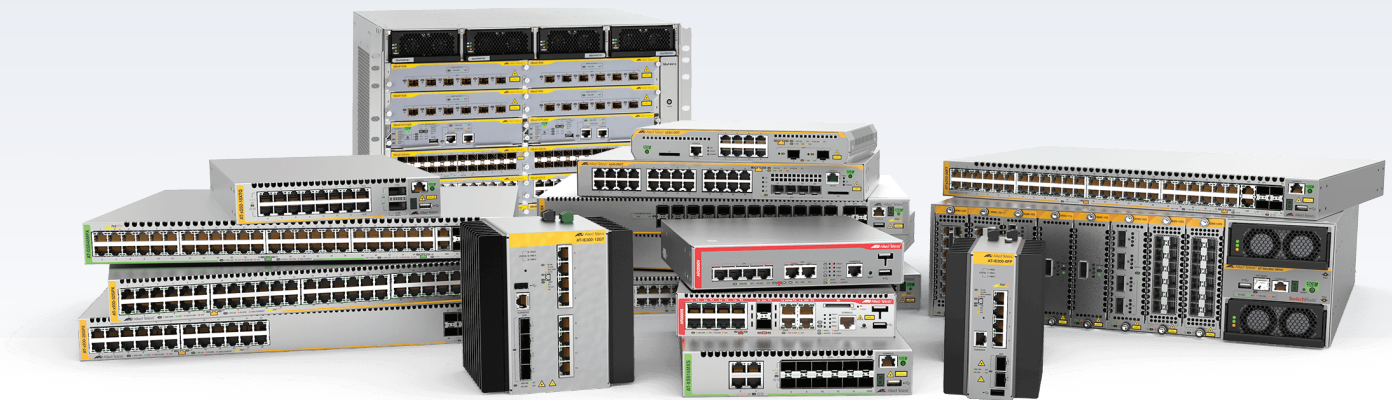


# Release Note for AlliedWare Plus Software Version 5.5.1-0.x



## AlliedWare Plus OPERATING SYSTEM

- » AMF Cloud » SBx8100 Series » SBx908 GEN2 » x950 Series » x930 Series
- » x550 Series » x530 Series » x510 Series » IX5 Series
- » x320 Series » x310 Series » x230 Series » x220 Series
- » IE500 Series » IE340 Series » IE300 Series » IE210L Series » IE200 Series
- » XS900MX Series » GS980MX Series » GS980EM Series » GS980EM Series
- » GS970M Series » GS900MX/MPX Series » FS980M Series
- » AR4050S » AR3050S » AR2050V » AR2010V » AR1050V
  
- » 5.5.1-0.1 » 5.5.1-0.2 » 5.5.1-0.3

## Acknowledgments

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

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

All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see [www.openssl.org/](http://www.openssl.org/)

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

This product includes software licensed under the GNU General Public License available from: [www.gnu.org/licenses/gpl2.html](http://www.gnu.org/licenses/gpl2.html)

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

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

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

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

©2021 Allied Telesis Inc. All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

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

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

## Getting the most from this Release Note

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

---

# Contents

<b>What's New in Version 5.5.1-0.3 .....</b>	<b>2</b>
<b>Introduction.....</b>	<b>2</b>
<b>Issues Resolved in Version 5.5.1-0.3 .....</b>	<b>8</b>
<b>What's New in Version 5.5.1-0.2 .....</b>	<b>17</b>
<b>Introduction.....</b>	<b>17</b>
<b>New Features and Enhancements.....</b>	<b>20</b>
<b>What's New in Version 5.5.1-0.1 .....</b>	<b>22</b>
<b>Introduction.....</b>	<b>22</b>
<b>Recently-Released Products.....</b>	<b>25</b>
<b>New Features and Enhancements.....</b>	<b>25</b>
<b>Important Considerations Before Upgrading .....</b>	<b>34</b>
<b>Obtaining User Documentation .....</b>	<b>41</b>
<b>Verifying the Release File .....</b>	<b>41</b>
<b>Licensing this Version on an SBx908 GEN2 Switch .....</b>	<b>42</b>
<b>Licensing this Version on an SBx8100 Series CFC960 Control Card .....</b>	<b>44</b>
<b>Installing this Software Version .....</b>	<b>46</b>
<b>Accessing the Web-based GUI on Switches .....</b>	<b>48</b>
<b>Accessing the Web-based GUI on AR-Series Devices.....</b>	<b>51</b>

# What's New in Version 5.5.1-0.3

Product families supported by this version:

AMF Cloud	IE510-28GSX
SwitchBlade x8100: SBx81CFC960	IE340 Series
SwitchBlade x908 Generation 2	IE300 Series
x950 Series	IE210L Series
x930 Series	IE200 Series
x550 Series	XS900MX Series
x530 Series	GS980MX/10HSm
x530L Series	GS980EM Series
x510 Series	GS980M Series
x510L Series	GS970M Series
IX5-28GPX	GS900MX/MPX Series
x320 Series	FS980M Series
x310 Series	AR4050S
x230 Series	AR3050S
x230L Series	AR2050V
x220 Series	AR2010V
	AR1050V

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-0.3.

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

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 46](#).

For instructions on how to update the web-based GUI, see [“Accessing the Web-based GUI on Switches” on page 48](#) or [“Accessing the Web-based GUI on AR-Series Devices” on page 51](#). The GUI offers easy visual monitoring and configuration of your device.



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

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

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		07/2021	vaa-5.5.1-0.3.iso (VAA OS) vaa-5.5.1-0.3.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-0.3.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	07/2021	SBx81CFC960-5.5.1-0.3.rel
SBx908 GEN2	SBx908 GEN2	07/2021	SBx908NG-5.5.1-0.3.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	07/2021	x950-5.5.1-0.3.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	07/2021	x930-5.5.1-0.3.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	07/2021	x550-5.5.1-0.3.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530-18GHXm x530-10GHXm x530L-52GTX x530L-52GPX x530L-28GTX x530L-28GPX x530L-10GHXm	x530 and x530L	07/2021	x530-5.5.1-0.3.rel
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 and x510L	07/2021	x510-5.5.1-0.3.rel
IX5-28GPX	IX5	07/2021	IX5-5.5.1-0.3.rel
x320-10GH x320-11GPT	x320	07/2021	x320-5.5.1-0.3.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	07/2021	x310-5.5.1-0.3.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	07/2021	x230-5.5.1-0.3.rel

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

Models	Family	Date	Software File
x220-28GS x220-52GT x220-52GP	x220	07/2021	x220-5.5.1-0.3.rel
IE510-28GSX	IE510-28GSX	07/2021	IE510-5.5.1-0.3.rel
IE340-20GP IE340L-18GP	IE340	07/2021	IE340-5.5.1-0.3.rel
IE300-12GT IE300-12GP	IE300	07/2021	IE300-5.5.1-0.3.rel
IE210L-10GP IE210L-18GP	IE210L	07/2021	IE210-5.5.1-0.3.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	07/2021	IE200-5.5.1-0.3.rel
XS916MXT XS916MXS	XS900MX	07/2021	XS900-5.5.1-0.3.rel
GS980MX/10HSm	GS980MX	07/2021	GS980MX-5.5.1-0.3.rel
GS980EM/10H GS980EM/11PT	GS980EM	07/2021	GS980EM-5.5.1-0.3.rel
GS980M/52 GS980M/52PS	GS980M	07/2021	GS980M-5.5.1-0.3.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	07/2021	GS970-5.5.1-0.3.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	07/2021	GS900-5.5.1-0.3.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	07/2021	FS980-5.5.1-0.3.rel
AR4050S AR3050S	AR-series UTM firewalls	07/2021	AR4050S-5.5.1-0.3.rel AR3050S-5.5.1-0.3.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	07/2021	AR2050V-5.5.1-0.3.rel AR2010V-5.5.1-0.3.rel AR1050V-5.5.1-0.3.rel



**Caution:** Software version 5.5.1-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-0.x. Such switches do not need a new license before upgrading to later versions.

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

- “Licensing this Version on an SBx908 GEN2 Switch” on page 42 and
- “Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 44.

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

The 5.5.1-0.3 software version is ISSU compatible with 5.5.1-0.2.

## New hardware platforms

With this software update:

- There are two new variants of x530 Series switch supported: x530-10GHXm and x530-18GHXm.
- The GS980MX Series has been added for APAC, CSA and NA regions. Please note for EMEA the GS980MX/10HSm only has been posted at this time.

## Enhancements

Software version 5.5.1-0.3 provides the following enhancements:

### Dynamic DNS Client

*Applies to: AR4050S, AR2050V/AR2010V, AR1050V, AR3050S*

From 5.5.1-03 onwards, HTML results contained within responses from a remote Dynamic DNS server are now supported by the Dynamic DNS client. They are no longer treated as failed DynDNS updates.

### AMF working-set

*Applies to: FS980M, GS900MX/MPX, GS70M, GS980EM, GS980M, XS900MX, IE200, IE300, IE340, IE210L, IE510, x220, x230/x230L, x310, IX5, x510/x510L, x530 / x530L, x550, x930, x950, SBx908Gen2, SBx81CFC960, AR4050S, AR2050V/AR2010V, AR1050V, x320, AR3050S*

With this software update, the **atmf working-set** command is now available via the GUI shell. Use this command to execute commands across an individually listed set of AMF nodes or across a named group of nodes.

Note that this command can only be run on a master node.

## Multi-point GRE tunnels behind NAT-T gateways

*Applies to: AR4050S, AR2050V/AR2010V, AR1050V, AR3050S*

Previously, if a remote VPN device was situated behind an external NAT gateway and connected to a local multi-point GRE tunnel, then next-hop resolution of the remote tunnel endpoint did not work correctly. This issue is now resolved.

With this software update, AR routers automatically learn GRE endpoints on dynamic GRE multi-point tunnels when the peer device is behind a NAT gateway.

## Support for Q-in-Q tunneling of DHCP snooped packets

*Applies to: SB8100CFC960*

Previously, the SBx8100, supported Q-in-Q a couple of different configuration methods:

- vlan-based: vlan-stacking vlan 10 outer-vlan 100
- port-based: switchport vlan-stacking provider-port / switchport vlan-stacking customer-edge-port

However, when these were implemented, they supported hardware-forwarding only.

From software version 5.5.1-0.3 onwards, Q-in-Q together with DHCP Snooping is supported on the SBx8100 and includes CPU-forwarded packets. No change is made to older port-based Q-in-Q.

## Enhanced ping polling for web authentication

*Available on all platforms except: AR1050, AR2010, VAA, vFW, AMF container*

With version 5.5.1-0.3 onwards, you can use ARP ping polling to check that a web authenticated supplicant (client device), is still connected.

A new command is available:

```
(no)auth-web-server ping-poll type {arp|ping}
```

Use this command to set the type of polling used to check that a web authenticated supplicant is still connected. The polling can be done using the default ICMP (ping) messages, or ARP messages. ARP polling works when a firewall is present, while ICMP does not. The polling will not start until ping-polling is enabled and the supplicant has been authorized.

For example, to set the polling type to ARP, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
awplus(config)# auth-web-server ping-poll type arp
```



For more information on the web-authentication and ping polling, see the [AAA and Port Authentication Feature Overview and Configuration Guide](#).

## SBx8100 Series switch, support for VLAN-based Q-in-Q

This software version supports VLAN-based Q-in-Q with DHCP snooping on the SBx8100 Series switch.

VLAN-based Q-in-Q is also known as VLAN-based VLAN stacking or VLAN-based double-tagging. When you configure this VLAN stacking for a customer VLAN, it applies an outer-VLAN tag to all traffic from that VLAN as it traverses the service provider's network. The outer tag is removed for traffic from the provider network ingressing via the provider port, which is configured as a member of the outer VLAN.

Based on an inner-VLAN to outer-VLAN mapping, VLAN-based Q-in-Q:

- adds an outer-VLAN tag to traffic incoming on customer ports that belong to one or more inner VLANs
- sends the traffic out with double-tagging on the provider port or ports, which are configured as members of the outer VLAN
- removes the outer-VLAN tag from traffic incoming on the provider port or ports (members of the outer VLAN) before it goes to the customer VLAN.

For more information on the VLAN-based Q-in-Q, see the [VLAN Feature Overview and Configuration Guide](#).

# Issues Resolved in Version 5.5.1-0.3

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

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud
CR-73387	802.1x	Previously, unauthorized supplicants could result in memory exhaustion. 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	Y	Y	-
CR-72418	AMF	With this software update, the speed and duplex setting on a <b>virtual</b> interface is avoided. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR-72964	AMF	Previously, the AMF guest node learning would not update in the event of an IP change. This issue has been resolved. ISSU: Effective when ISSU complete.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	Y	Y	Y	Y	Y
CR-73385	AMF	With this software update, AMF application proxy threat actions are no longer removed after the device lookup function is triggered by AMF Security. ISSU: Effective when CFCs upgraded.	Y	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-	Y	-	Y	Y	Y	Y	-
CR-73392	ARP Neighbor Discovery	Previously, ARPs could get stuck in the probe state if an ARP request with a new source MAC address kept arriving. 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	Y	-
CR-71185	AWC-Lite	Previously, running <b>enable traps</b> in SNMP mode in AWC-Lite could cause memory exhaustion. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73260	AWC-Lite	Previously, the AWC-Lite security settings could cause memory exhaustion. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-73261	AWC-Lite	Previously, the <b>no wireless</b> command could cause memory exhasution. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73263	AWC-Lite	Previously, the <b>auto-config</b> command could cause memory exhaustion. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73264	AWC-Lite	Previously, the <b>show wireless auto-config</b> command would cause memory exhaustion. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73272	AWC-Lite	Previously, the <b>wireless download ap</b> and <b>wireless power-channel ap</b> commands could cause memory exhaustion. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73273	AWC-Lite	Previously, the <b>debug wireless</b> and <b>show debug wireless</b> commands could cause memory exhaustion. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73274	AWC-Lite	With this software update, the following error log messages are added for different types of incorrect AP configuration: " "WDS SSID not found" " " "VAP0 not found" " " "Hwtype does not support CB" " " "CB control VLAN not found" " " "CB key not found" " " "SC SSID not found" " " "SC key not found" " " "SC radio not found" " " "SC channel not found" " " "SC VAP not found" " " "Passpoint security must be WPA Enterprise" " "	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-73275	AWC-Lite	Previously, under rare circumstances, an AWC-Lite capable device could freeze when entering the <b>no wireless</b> command while the log transfer was still active.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73318	AWC-Lite	Previously, incorrect log messages were displayed with the following commands: <ul style="list-style-type: none"> <li>■ wireless power-channel ap"</li> <li>■ wireless ap-configuration apply app"</li> <li>■ wireless reset ap"</li> <li>■ wireless download ap"</li> </ul> This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73319	AWC-Lite	With this software update, the maximum captive portal is set to 12,000 rather than 50,000.  Also, previously, a memory exhaustion could occur when the management address was applied to the AP.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73328	AWC-Lite	Previously, configuring the Channel Blanket eligible channel could cause memory exhaustion.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73419	AWC-Lite	With this software update, AWC-Lite capable devices can now perform configuration update, firmware upgrade and reboot to an AP without issue.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73446	AWC-Lite	Previously, products that support AWC-Lite had an incorrect passpoint value setting.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73577	AWC-Lite	Previously, MAC address filter import could cause the AWC-lite daemon to restart unexpectedly.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-73655	AWC-Lite	Previously, configuring Passpoint could cause memory exhaustion. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	Y	Y	Y	-	-	-	-	Y	-	Y	Y	Y	-
CR-73391	Bootup	Previous, erroneous system debug messages were generated during x510 or IE510 series switches initialization. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-73615	Bootup	Previously, on x510-DP series switches, unexpected errors occurred at startup if the PSU IDs failed to be read before the fan settings were updated. This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-73339	CLI	Previously, the <b>show system fiber-monitoring</b> command required user privilege level 15 to execute. With this software update, it has been reduced to level 7. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	Y	Y	Y	Y	-
CR-73776	Device Security	With this software update, the command: <b>show http</b> will display a summary of the server certificate in use, including the SHA-1 and SHA-256 fingerprints. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	Y	Y	Y	Y	Y	Y	-
CR-54492	DHCP Server	This software update alters the DHCPv4 lease time calculation to avoid roll over errors on 64-bit OS systems when using -1 (infinite) or large values for default DHCP lease time. ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	Y	Y	Y	-	-	-	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	Y	Y	Y	Y	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-68889	DHCP Server	Previously, the commands <b>show ip dhcp binding</b> and <b>show ip dhcp pools</b> were unable to process DHCP bindings that included malformed HW addresses and would display "Malformed statement" instead.  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	Y	Y	-	
CR-72171	DPI	Previously, a resource leak in DPI (with "provider procera") occurred when either: <ul style="list-style-type: none"><li>■ DPI was disabled and then enabled or</li><li>■ when a new DPI resource was installed.</li></ul> The resource leak would start to impact operation after more than 125 iterations. This would require 2 to 3 years at the typical resource release interval.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	
CR-63798	Environmental Monitoring	Previously, the temperature sensor on x950 series and x908 GEN2 could occasionally reported an abnormal condition.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-
CR-73556	Hardware Health Monitoring	Previously, IE510-28GSX fans would run at maximum speed even from power on and stay at maximum speed.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-73364	Multicast Forwarding	Previously, in some multicast configurations, the processing of JOIN/LEAVE could result in memory depletion.  This issue has been resolved.  ISSU: Effective when CFCs upgraded.	Y	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-	Y	-	-	-	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-73456	OpenFlow	Previously, packets encapsulated with an 802.3 header (length instead of type) which were not using SNAP encapsulation could cause hardware flows to be added which would match all Ethernet types, thus adversely affecting OpenFlow switching.  This issue has been resolved.	-	Y	Y	Y	-	-	Y	Y	Y	Y	-	-	Y	Y	Y	Y	-	Y	Y	Y	-	-	-	-	Y	-	-	-	-	-	-
CR-73471	OpenFlow	Previously, in rare circumstances, updating an OpenFlow flow could result in a system reboot.  Also, certain flow actions (involving setting Ethernet source or destination address without a linked VLAN action) could result in the flow being available in software only.  Both issues have been resolved.	-	Y	Y	Y	Y	-	Y	Y	Y	Y	-	-	Y	Y	Y	Y	-	Y	Y	Y	-	-	-	-	Y	-	-	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud			
CR-71115	PoE	<p>Previously, on IE300 and x320 series, some dual-signature PoE power devices would not draw the minimum DC current for a pair-set unless both pair-sets were powered up simultaneously, resulting in disconnection of the power devices.</p> <p>This issue has been resolved with a new parameter in the <u>command</u>:  <b>power-inline disconnect-defer</b>  &lt;disconnect-defer-timeout&gt;</p> <p>This causes the disconnect detection to be enabled 3 seconds after the default pair-set has been powered which gives the power devices enough time to draw power on both pair-sets. The disconnect detection timeout can also be configured longer than 3 seconds if required.</p> <p>The command "(no) <b>power-inline disconnect-defer</b>" defers the DC disconnect detection in hardware. It is disabled by default. Some 60W PDs take longer than the 802.3at standard time for drawing the minimum DC current on an individual pair. By deferring the enabling of the DC disconnect logic it allows both sets of pairs to power up and start drawing current.</p>	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
CR-72497	PoE	<p>With this software update, the auto-negotiation is now enabled at 1G speed on x930 series. Also with this software update, the auto-negotiation was enabled on SFP plus ports for the x310 series.</p>	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-73123	PoE	<p>Previously, the SPF on x930 series switches was not reflecting the speed/duplex/medium-type settings correctly.</p> <p>This issue has been resolved.</p>	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-



CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
CR-72940	PoE	Previously, the <b>power-inline-max</b> command would not apply for PoE ports all the time.  This issue has been resolved.  ISSU: Effective when CFCs upgraded.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-73223	SD WAN	Previously, when Vista Manager was used to configure SD WAN, in certain circumstances (such as tunnels going up and down) the device could consume excess memory, which could eventually cause the device to run out of memory and restart.  This issue has been resolved.	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	Y	-
CR-73207	SNMP	Previously, MIB variable 'dot1xPaePortReauthenticate' was not working 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	Y	Y	-	-	-	-	Y	Y	Y	Y	Y	Y	-
CR-73422	Unicast Routing	Previously, in certain complex routing situations, rebooting one device could cause another device to reboot as part of transient routing changes.  This issue has been resolved.  With this software update, the routing calculation has been improved to prevent this from happening.  ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	Y	Y	Y	Y	-
CR-73020	VCStack	Previously, resiliency link traffic could be dropped when the device CPU was congested.  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	-	-	-	-	-	-

CR	Module	Description	FS980M	GS970M	GS900MX/MPX	XS900MX	GS980M	GS980MX	GS980EM	IE200	IE210L	IE300	IE340	IE510	x220	x230, x230L	x310	x320	x330	IX5	x510, 510L	x530, x530L	x550	x930	x950	SBx8100 CFC960	x908Gen2	AR1050V	AR2010V	AR2050V	AR3050S/AR4050S	AMF Cloud	
			<b>CR-72608</b>	<b>VCStack</b>	Previously, on rare occasions, a stack member might not join the stack correctly on a reboot or power cycle. 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	-	-	-
<b>CR-72961</b>	<b>VCStack</b>	Previously, a stack member might not join the stack during a master failover. This issue has been resolved. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	-	-	Y	Y	Y	-	-	-	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	-	-	-	-	-	-
<b>CR-73650</b>	<b>VCStack</b>	Previously, it was possible for the stacked device to consume memory over a long run. 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	-	-	-	-	-	-
<b>CR-73636</b>	<b>Web Authentication</b>	Previously, the default web-auth-server ping-polling type was displayed in the running configuration. With this software update, it is removed. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	-	Y	Y	Y	Y	-
<b>CR-73652</b>	<b>Web Authentication</b>	With this software update, ARP polling packets for Web-Authentication has been changed from broadcast to unicast since broadcasting ARP polling for Web-Authentication could pose as a small security risk and is likely to have a greater network impact. ISSU: Effective when CFCs upgraded.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	-	Y	Y	-	Y	Y	Y	Y	-

---

# What's New in Version 5.5.1-0.2

Product families supported by this version:

AMF Cloud	IE510-28GSX
SwitchBlade x8100: SBx81CFC960	IE340 Series
SwitchBlade x908 Generation 2	IE300 Series
x950 Series	IE210L Series
x930 Series	IE200 Series
x550 Series	XS900MX Series
x530 Series	GS980MX/10HSm
x530L Series	GS980EM Series
x510 Series	GS980M Series
x510L Series	GS970M Series
IX5-28GPX	GS900MX/MPX Series
x320 Series	FS980M Series
x310 Series	AR4050S
x230 Series	AR3050S
x230L Series	AR2050V
x220 Series	AR2010V
	AR1050V

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-0.2.

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

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 46](#).

For instructions on how to update the web-based GUI, see [“Accessing the Web-based GUI on Switches” on page 48](#) or [“Accessing the Web-based GUI on AR-Series Devices” on page 51](#). The GUI offers easy visual monitoring and configuration of your device.



---

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

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

---

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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud		04/2021	vaa-5.5.1-0.2.iso (VAA OS) vaa-5.5.1-0.2.vhd and upload_vhd.py (for AWS) vaa_azure-5.5.1-0.2.vhd (for Microsoft Azure)
SBx81CFC960	SBx8100	04/2021	SBx81CFC960-5.5.1-0.2.rel
SBx908 GEN2	SBx908 GEN2	04/2021	SBx908NG-5.5.1-0.2.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	04/2021	x950-5.5.1-0.2.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	04/2021	x930-5.5.1-0.2.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2021	x550-5.5.1-0.2.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GTX x530L-52GPX x530L-28GTX x530L-28GPX x530L-10GHXm	x530 and x530L	04/2021	x530-5.5.1-0.2.rel
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 and x510L	04/2021	x510-5.5.1-0.2.rel
IX5-28GPX	IX5	04/2021	IX5-5.5.1-0.2.rel
x320-10GH x320-11GPT	x320	04/2021	x320-5.5.1-0.2.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	04/2021	x310-5.5.1-0.2.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2021	x230-5.5.1-0.2.rel
x220-28GS x220-52GT x220-52GP	x220	04/2021	x220-5.5.1-0.2.rel
IE510-28GSX	IE510-28GSX	04/2021	IE510-5.5.1-0.2.rel

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

Models	Family	Date	Software File
IE340-20GP IE340L-18GP	IE340	04/2021	IE340-5.5.1-0.2.rel
IE300-12GT IE300-12GP	IE300	04/2021	IE300-5.5.1-0.2.rel
IE210L-10GP IE210L-18GP	IE210L	04/2021	IE210-5.5.1-0.2.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	04/2021	IE200-5.5.1-0.2.rel
XS916MXT XS916MXS	XS900MX	04/2021	XS900-5.5.1-0.2.rel
GS980MX/10HSm	GS980MX	04/2021	GS980MX-5.5.1-0.2.rel
GS980EM/10H GS980EM/11PT	GS980EM	04/2021	GS980EM-5.5.1-0.2.rel
GS980M/52 GS980M/52PS	GS980M	04/2021	GS980M-5.5.1-0.2.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2021	GS970-5.5.1-0.2.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	04/2021	GS900-5.5.1-0.2.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	04/2021	FS980-5.5.1-0.2.rel
AR4050S AR3050S	AR-series UTM firewalls	04/2021	AR4050S-5.5.1-0.2.rel AR3050S-5.5.1-0.2.rel
AR2050V AR2010V AR1050V	AR-series VPN routers	04/2021	AR2050V-5.5.1-0.2.rel AR2010V-5.5.1-0.2.rel AR1050V-5.5.1-0.2.rel



**Caution:** Software version 5.5.1-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-0.x. Such switches do not need a new license before upgrading to later versions.

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

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 42 and](#)
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 44.](#)

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

The 5.5.1-0.2 software version is ISSU compatible with 5.5.1-0.1.

## New Features and Enhancements

This section summarizes the new features in 5.5.1-0.2:

- [“Support for AR Series UTM firewalls and VPN routers” on page 20](#)
- [“Support for AMF Cloud” on page 20](#)
- [“Enhancements to AMF Cloud support for AWS” on page 20](#)
- [“Set a minimum TLS version for OpenVPN” on page 21](#)

To see how to find full documentation about all features on your product, see [“Obtaining User Documentation” on page 41.](#)

## Support for AR Series UTM firewalls and VPN routers

From 5.5.1-0.2 onwards, the AlliedWare Plus version 5.5.1 stream supports the AR Series UTM firewalls and VPN routers: AR4050S, AR3050S, AR2050V, AR2010V, and AR1050V.

## Support for AMF Cloud

From 5.5.1-0.2 onwards, the AlliedWare Plus version 5.5.1 stream supports AMF Cloud.

Note that AMF Cloud now supports XenServer 7.1 CU1. From 5.5.1-0.2 onwards, XenServer 6.5 is no longer supported.

## Enhancements to AMF Cloud support for AWS

*Available on AMF Cloud*

From AlliedWare Plus version 5.5.1-0.2 onwards, AMF Cloud on Amazon Elastic Compute Cloud (AWS EC2) now supports the T3, M5, and C5 instance types.

---

## Set a minimum TLS version for OpenVPN

*Available on AR Series UTM firewalls and VPN routers*

From version 5.5.1-0.2 onwards, you can set a minimum TLS (Transport Layer Security) version for authenticating OpenVPN clients.

OpenVPN supports different TLS versions. This can be a security risk as the older TLS versions have known security flaws and were deprecated in 2020.

**New command** `tunnel openvpn tls-version-min {1.1|1.2}`  
`no tunnel openvpn tls-version-min`

Use the **no** variant of this command to revert to the default TLS version (1.0)

For example, to set the minimum TLS version as 1.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)tunnel openvpn tls-version-min 1.1
```

For more information on configuring OpenVPN, see the [OpenVPN Feature Overview and Configuration Guide](#).

# What's New in Version 5.5.1-0.1

Product families supported by this version:

AMF Cloud <sup>1</sup>	IE510-28GSX
SwitchBlade x8100: SBx81CFC960	IE340 Series
SwitchBlade x908 Generation 2	IE300 Series
x950 Series	IE210L Series
x930 Series	IE200 Series
x550 Series	XS900MX Series
x530 Series	GS980MX/10HSm
x530L Series	GS980EM Series
x510 Series	GS980M Series
x510L Series	GS970M Series
IX5-28GPX	GS900MX/MPX Series
x320 Series	FS980M Series
x310 Series	AR4050S <sup>1</sup>
x230 Series	AR3050S <sup>1</sup>
x230L Series	AR2050V <sup>1</sup>
x220 Series	AR2010V <sup>1</sup>
	AR1050V <sup>1</sup>

1. Support for AMF Cloud and AR-series UTM firewalls and VPN routers is in 5.5.1-0.2

## Introduction

This release note describes the new features in AlliedWare Plus software version 5.5.1-0.1.

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

For instructions on how to upgrade to this version, see [“Installing this Software Version” on page 46](#).

For instructions on how to update the web-based GUI, see [“Accessing the Web-based GUI on Switches” on page 48](#) or [“Accessing the Web-based GUI on AR-Series Devices” on page 51](#). The GUI offers easy visual monitoring and configuration of your device.



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

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



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

Table 1: Models and software file names

Models	Family	Date	Software File
AMF Cloud <sup>1</sup>			
SBx81CFC960	SBx8100	04/2021	SBx81CFC960-5.5.1-0.1.rel
SBx908 GEN2	SBx908 GEN2	04/2021	SBx908NG-5.5.1-0.1.rel
x950-28XSQ x950-28XTQm x950-52XSQ	x950	04/2021	x950-5.5.1-0.1.rel
x930-28GTX x930-28GPX x930-52GTX x930-52GPX x930-28GSTX	x930	04/2021	x930-5.5.1-0.1.rel
x550-18SXQ x550-18XTQ x550-18XSPQm	x550	04/2021	x550-5.5.1-0.1.rel
x530-28GTXm x530-28GPXm x530-52GTXm x530-52GPXm x530L-52GTX x530L-52GPX x530L-28GTX x530L-28GPX x530L-10GHXm	x530 and x530L	04/2021	x530-5.5.1-0.1.rel
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 and x510L	04/2021	x510-5.5.1-0.1.rel
IX5-28GPX	IX5	04/2021	IX5-5.5.1-0.1.rel
x320-10GH x320-11GPT	x320	04/2021	x320-5.5.1-0.1.rel
x310-26FT x310-50FT x310-26FP x310-50FP	x310	04/2021	x310-5.5.1-0.1.rel
x230-10GP x230-10GT x230-18GP x230-18GT x230-28GP x230-28GT x230L-17GT x230L-26GT	x230 and x230L	04/2021	x230-5.5.1-0.1.rel
x220-28GS x220-52GT x220-52GP	x220	04/2021	x220-5.5.1-0.1.rel
IE510-28GSX	IE510-28GSX	04/2021	IE510-5.5.1-0.1.rel
IE340-20GP IE340L-18GP	IE340	04/2021	IE340-5.5.1-0.1.rel

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

Models	Family	Date	Software File
IE300-12GT IE300-12GP	IE300	04/2021	IE300-5.5.1-0.1.rel
IE210L-10GP IE210L-18GP	IE210L	04/2021	IE210-5.5.1-0.1.rel
IE200-6FT IE200-6FP IE200-6GT IE200-6GP	IE200	04/2021	IE200-5.5.1-0.1.rel
XS916MXT XS916MXS	XS900MX	04/2021	XS900-5.5.1-0.1.rel
GS980MX/10H5m	GS980MX	04/2021	GS980MX-5.5.1-0.1.rel
GS980EM/10H GS980EM/11PT	GS980EM	04/2021	GS980EM-5.5.1-0.1.rel
GS980M/52 GS980M/52PS	GS980M	04/2021	GS980M-5.5.1-0.1.rel
GS970M/10PS GS970M/10 GS970M/18PS GS970M/18 GS970M/28PS GS970M/28	GS970M	04/2021	GS970-5.5.1-0.1.rel
GS924MX GS924MPX GS948MX GS948MPX	GS900MX/MPX	04/2021	GS900-5.5.1-0.1.rel
FS980M/9 FS980M/9PS FS980M/18 FS980M/18PS FS980M/28 FS980M/28PS FS980M/52 FS980M/52PS FS980M/28DP	FS980M	04/2021	FS980-5.5.1-0.1.rel
AR4050S AR3050S <sup>1</sup>	AR-series UTM firewalls		
AR2050V AR2010V AR1050V <sup>1</sup>	AR-series VPN routers		

1. Support for AMF Cloud and AR-series UTM firewalls and VPN routers is in 5.5.1-0.2



**Caution:** Software version 5.5.1-0.x requires a release license for the SBx908 GEN2 and SBx8100 switches. If you are using either of these switches, make sure that each switch has a 5.5.1 license certificate before you upgrade.

Once an SBx908 GEN2 or SBx8100 switch has a version 5.5.1 license installed, that license also covers all later 5.5.1 versions, including 5.5.1-0.x. Such switches do not need a new license before upgrading to later versions.

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

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 42](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 44.](#)

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

The 5.5.1-0.1 software version is ISSU incompatible with previous software versions.

## Recently-Released Products

The following recent products are supported by version 5.5.1-0.1:

- x530L-10GHXm
- GS980MX/10HSm

## New Features and Enhancements

This section summarizes the new features in 5.5.1-0.1:

- “Autonomous Management Framework (AMF) and Autonomous Wave Control (AWC) License Enhancements” on page 26
- “Multicast Source Discovery Protocol (MSDP)” on page 26
- “VXLAN” on page 27
- “Link Health Monitoring for Switches” on page 28
- “Enable hardware forwarding on the guest VLAN” on page 29
- “Reducing IGMP hardware entries” on page 29
- “Multicast overlapping group handling” on page 29
- “Jumbo frames for Layer 3 switched traffic and control packets” on page 30
- “Improvements to ACL configuration” on page 30
- “Flow Control enhancement” on page 31
- “Port security on aggregators” on page 31
- “Conformation with IPv6 Ready Logo Phase-2” on page 32
- “Improvement to handling of some 60W Powered Devices on IE300 Series switches” on page 33

To see how to find full documentation about all features on your product, see “Obtaining User Documentation” on page 41.

## Autonomous Management Framework (AMF) and Autonomous Wave Control (AWC) License Enhancements

Purchasing of AMF and AWC licenses has been simplified. For the following software products, you now simply buy licenses for sets of 10 nodes or APs (for switches) or 5 nodes or APs (for AR4050S):

- AMF Master
- AMF Controller (per 10 areas, for SwitchBlade products only)
- AWC
- AWC-CB
- AWC-SC

For example, there are now four AMF Master licenses available:

- AT-SW-AM10-1YR: a 1-year license for switches
- AT-SW-AM10-5YR: a 5-year license for switches
- AT-SW-AM5-1YR: a 1-year license for AR4050S
- AT-SW-AM5-5YR: a 5-year license for AR4050S

To manage 38 nodes with an x950 Series switch, you need 4 x AT-SW-AM10-1YR licenses (for a 1-year subscription). If you add another 12 nodes later, you just need to add a fifth AT-SW-AM10-1YR license.

These new licenses are available with 5.4.8-2.x and newer AlliedWare Plus versions, as long as the AlliedWare Plus version supports the license's feature on the relevant device model. For AWC-CB and AWC-SC, this means you will need a more recent release than 5.4.8-2.x.

## Multicast Source Discovery Protocol (MSDP)

*Available on SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, and x320 Series switches*

From version 5.5.1-0.1 onwards, AlliedWare Plus supports Multicast Source Discovery Protocol (MSDP).

MSDP provides a mechanism to allow PIM Sparse-mode (PIM-SM) Rendezvous Points (RP) to exchange multicast source information, either between multicast domains, or within a multicast domain that utilises anycast RP addresses.

A virtual MSDP topology is implemented using TCP connections between MSDP peers. The MSDP topology allows PIM-SM RPs peers to discover active multicast sources from other RPs.

If there are receivers for multicast sources in a domain, the normal source-tree building mechanism in PIM-SM will be used to deliver multicast data over a distribution tree, which may span PIM-SM domains.

When an RP in a PIM-SM domain first learns of a new sender, via PIM register messages, it constructs a "Source-Active" (SA) message and sends it to its MSDP peers. All RPs that intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or via an intermediate MSDP peer. The SA message contains the following fields:

- Source address of the data source.
- Group address the data source sends to.
- IP address of the RP.

MSDP is used in two scenarios:

- An MSDP-speaking router in a PIM-SM domain has a MSDP peering relationship with one or more MSDP-speaking router(s) in another domain(s). One MSDP peer shares information on sources originating in its domain by sending SA (Source-Active) messages to its peer(s).
- Within a PIM domain utilising anycast-RPs [RFC3446] that does not support RFC4610 (PIM register messages between anycast RPs), MSDP may be used to synchronize active sources between the anycast RPs. MSDP peering used in this scenario is based on MSDP mesh groups, where typically two to tens of peers can comprise a given mesh group.

For more information, see the [MSDP Feature Overview and Configuration Guide](#).

## VXLAN

*Available on x530 Series switches*

From version 5.5.1-0.1 onwards, AlliedWare Plus supports static Virtual Extensible LAN (VXLAN) tunnels on the x530 Series.

If your network is growing rapidly, stretching your VLANs could be a solution, as it can help you span your Layer 2 across the physical network. This is where VXLAN could be another solution.

VXLAN is an overlay encapsulation technology. It creates a virtual network overlaid on top of the existing physical network infrastructure. It uses the underlay IP network and builds a flexible Layer 2 overlay logical network on it.

VXLAN enables you to statically configure source and destination virtual tunnel endpoints (VTEPs) for a particular traffic flow. A source VTEP encapsulates and a destination VTEP de-encapsulates Layer 2 packets with a VXLAN header, thereby tunneling the packets through an underlying Layer 3 IP network.

Simple configuration example:

```
awplus# configure terminal
awplus(config)# nvo vxlan
awplus(config-vxlan)# source-interface lo
awplus(config-vxlan)# remote-vtep building2 192.168.5.64
```

```
awplus(config-vxlan) # remote-vtep building3 192.168.5.128
awplus(config-vxlan) # map-access vlan 201 vni 10201
awplus(config-vxlan) # map-access vlan 202 vni 10202
awplus(config-vxlan) # map-access vlan 203 vni 10203
```

For more information, see the [VXLAN Feature Overview and Configuration Guide](#).

## Link Health Monitoring for Switches

*Available on SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, x230, x230L and x220 Series switches*

From version 5.5.1-0.1 onwards, AlliedWare Plus supports link health monitoring for switches.

Link health monitoring is a feature that allows a network manager to continually monitor the health of their network. It does this by gathering health metrics comprising latency, jitter, and probe loss on an on-going basis. The health metrics can optionally be recorded in a history buffer for later review and analysis. Link health monitoring can also be used with the AlliedWare Plus Trigger facility to automatically change device configuration in response to changes in the health of a monitored link.

Link health monitoring on switches can be used to periodically monitor the health of a specific link or specific routing path over time by sending probes at a fixed interval. By recording the jitter and latency experienced by the probe, as well as the rate of probe loss, the health quality of the link can be determined.

Link health monitoring probes can be sent to fixed IPv4 or IPv6 addresses, or a fully-qualified domain name (FQDN) can be specified as the destination which the device will attempt to resolve to an IP address. Link health monitoring can be configured to use either ICMP echo (ping) packets or HTTP GET requests, depending on the type of server the probe is being sent to.

The probe metrics can be recorded into a history buffer at multiple levels of granularity, allowing the network manager to collect performance data about their network that they can analyse to help diagnose network performance issues and outages. Triggers can be associated with link health monitoring probes and set to activate when a link is judged to be good, bad, unreachable, or upon any state change, allowing for device configuration to be dynamically modified in response to changing network conditions.

For more information, see the [Link Health Monitoring for Switches Feature Overview and Configuration Guide](#).

## Enable hardware forwarding on the guest VLAN

Available on all AlliedWare Plus switches. (Previously only available on GS970M, x230, and IE210 Series switches)

From version 5.5.1-0.1 onwards, you can enable hardware forwarding on the guest VLAN. By default all traffic on the VLAN is forwarded by the CPU. To enable this feature, use the following command on the interface associated with the guest VLAN:

```
awplus(config-if)# auth guest-vlan hw-forwarding
```

For more information on guest VLANs, see the [AAA and Port Authentication Feature Overview and Configuration Guide](#).

## Reducing IGMP hardware entries

Available on SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, XS900MX, GS980MX/10HSm, GS980M, GS900MX/MPX and FS980M Series switches

From version 5.5.1-0.1 onwards, a new multicast command is available:

```
ip igmp flood-group
```

This command adds an all sources multicast entry into the switch's multicast hardware table to flood multicast packets to all ports within the VLAN without mirroring the traffic to the CPU. This significantly reduces the number of hardware entries consumed.

For example, to configure an IGMP flooding group to L2 ports only, use the following commands. This will flood any UDP packet to group 239.255.255.250 to all ports in vlan1.

```
awplus(config)#int vlan1
awplus(config-if)#ip igmp flood-group 239.255.255.250
```

For more information on IGMP flooding, see the [IGMP/MLD Feature Overview and Configuration Guide](#).

## Multicast overlapping group handling

Available on SBx81CFC960, x530, x530L, x320, x220, GS980MX/10HSm, GS980EM, and GS980M series switches.

From 5.5.1-0.1 onwards, the command **platform l2mc-overlap** is enabled on these switches by default. This command checks for overlapping (shared) multicast entries, so that shared entries are not deleted if they are still in use.

When the overlap handling is on, group entries will not be deleted if a multicast overlap exists. However, this may have the unexpected behavior of flooding multicast packets to ports which have not joined the group. The workaround is to turn off the command or redesign the network to ensure no multicast groups overlap.

## Jumbo frames for Layer 3 switched traffic and control packets

*Available on SBx908 GEN2 and x950 Series switches*

From version 5.5.1-0.1 onwards, jumbo frames are supported for Layer 3 switching and control packets. Once jumbo frame support is enabled, the maximum packet size can be up to 9216 bytes for devices that support Layer 3 jumbo frames.

Jumbo frames for Layer 3 switching increases performance by reducing the amount of packet overhead relative to the amount of data transmitted. For example, you could use jumbo frames in SAN (Storage Area Networks), which are dedicated networks used by servers to access block-level storage.

To configure jumbo frames for Layer 3 switching and control packets, you need to:

- turn on jumbo frame support, using the **mruf** command for the required switchports, and
- increase the MTU value, using the **mtu** command for the required VLANs.

For more information about how to configure L3 jumbo frames for Layer 3 traffic and control packets, see the [Switching Feature Overview and Configuration Guide](#).

## Improvements to ACL configuration

*Available on all AlliedWare Plus switches.*

From 5.5.1-0.1 onwards, the CLI for ACLs has the following minor improvements:

1. A new command allows you to delete an extended IPv6 software ACL without specifying its filter details:

```
awplus(config)# no ipv6 access-list extended <name>
```

2. A new command option for IPv4 software ACLs allows you to specify an IP address without a mask in the standard numbered IPv4 sub-mode. To do this, use the command option:

```
awplus(config)# access-list {<1-99>|<1300-1999>}  
awplus(config-ip-std-acl)# [<1-65535>] {deny|permit}  
<ip-add>
```

where *<ip-add>* is in dotted decimal format

3. The command that previously set a maximum number of software filters for IPv4 software access-lists has been removed. This command was:

```
awplus(config)# maximum-access-list <1-4294967294>
```

For more information on ACLs, see the [ACL Feature Overview and Configuration Guide](#).



## Flow Control enhancement

Available on x530 and x530L Series switches and GS980MX/10HSm switches.

From version 5.5.1-0.1 onwards, AlliedWare Plus supports **flow-control receive on** for the x530 and x530L Series switches. It was already supported on some other AlliedWare Plus switches.

This enables a port to react to reception of flow control XOFFs without sending any flow control packets itself. This is to prevent the port reacting to oversubscribed ports in the system.

The command is:

```
[no] flowcontrol [send|receive] [off|on]
```

To enable flow control on port1.0.2 (receive only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive on
```

## Port security on aggregators

Available on SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, x230, x230L and x220 Series switches.

From 5.5.1-0.1 onwards, you can use port-security to set the maximum number of MAC addresses that link aggregation groups (LAGs) can learn. Previously, you could only specify this for switch ports.

For example, to enable the port-security feature on the link aggregation group sa2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)# switchport port-security
```

You can then use the commands **switchport port-security maximum** and **switchport port-security violation** to configure port-security.

Note that on SBx81CFC960, port-security can be configured on a maximum of 30 aggregators.

For more information on port-security, see the [Switching Feature Overview and Configuration Guide](#).

## Conformation with IPv6 Ready Logo Phase-2

Available on all AlliedWare Plus devices that support IPv6

From 5.5.0-2.5 and 5.5.1-0.1 onwards, AlliedWare Plus firmware conforms with IPv6 Core Protocols Test Specification (Version 5.0.1) and IPv6 Core Protocols Interoperability Test Scenario (Version 5.0.2).

For more information on IPv6, see the [IPv6 Feature Overview and Configuration Guide](#).

As part of this, the following enhancements have been made:

### Set default router preference value for RAs

The following new command lets you set the default router preference value for Router Advertisements sent on the given IPv6 interface:

```
awplus(config-if)# ipv6 nd router-preference [low|medium|high]
```

where:

- **low** corresponds to a value of 0b11
- **medium** corresponds to a value of 0b00, and is the default
- **high** corresponds to a value of 0b01

To reset the default router preference value, use the command:

```
awplus(config-if)# no ipv6 nd router-preference
```

### Advertise DNS search list option in RAs

The following new command lets you create a DNS Search List (DNSSL) to be included in the Router Advertisement for a given IPv6 interface:

```
awplus(config-if)# ipv6 nd dns search-list <domain-name>
```

where **<domain-name>** is a domain name to be added to the search list, for example example.com.

To delete one or all domain names, use the command:

```
awplus(config-if)# no ipv6 nd dns search-list [<domain-name>]
```

If no domain name is specified, then all domain names previously added will be deleted.

For example, to add the domain 'mybusinessexample.com' to the search list on VLAN1, use the commands:

```
awplus(config)# int vlan1
awplus(config-if)# ipv6 nd dns search-list
mybusinessexample.com
```

### Advertise Route Information Option

The following new commands let you add a Route Information Option for a more specific route to Router Advertisements sent from a specific IPv6 interface:

```
awplus(config-if)# ipv6 nd route-information <prefix>
awplus(config-if)# ipv6 nd route-information <prefix>
{<0-4294967295>|infinity|default} (low|medium|high)
```

where:

- **<prefix>** is the prefix for the more specific route to announce in the RA
- **<0-4294967295>|infinity|default** is the length of time in seconds (relative to the time the packet is sent) for which the prefix is valid for route determination. The **default** lifetime is 3 \* MaxRtrAdvInterval, and the value **infinity** specifies that the route advertise has an infinite lifetime.
- **low|medium|high** is the preference value for the route information.

To delete the route information, use one of the commands:

```
awplus(config-if)# no ipv6 nd route-information X:X::X:X/M
awplus(config-if)# no ipv6 nd route-information all
```

### Improvements to IPv6 fragment handling

IPv6 fragment handling has been improved so that it conforms to RFC-8200, Section 4.5, which says:

“If the first fragment does not include all headers through an Upper-Layer header, then that fragment should be discarded and an ICMP Parameter Problem, Code 3, message should be sent to the source of the fragment, with the Pointer field set to zero.”

## Improvement to handling of some 60W Powered Devices on IE300 Series switches

From 5.5.1-0.1 onwards, handling of some 60W Powered Devices (PDs) on IE300 Series switches has been improved.

Some 60W PoE PDs won't draw the minimum DC current for a pair-set unless both pair-sets are powered up simultaneously. This makes the IE300 Series switch cycle through the phases of detection, classification, power up, and disconnect on pair-sets connected to such PDs, which prevents the switch from powering such PDs.

To resolve this, a new command has been added. This command delays the disconnect detection on the selected port until 1s after the default pair-set has been powered. This gives the PD enough time to draw power on both pair-sets.

The new command is:

```
awplus(config-if)# power-inline disconnect-defer
```

---

# Important Considerations Before Upgrading

Please read this section carefully before upgrading.

This section describes changes that are new in 5.5.1-x.x and may affect your device or network behavior if you upgrade:

- [Upgrade compatibility for SBx908 GEN2 and x950 Series switches](#)
- [Changes that may affect device or network configuration](#)

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

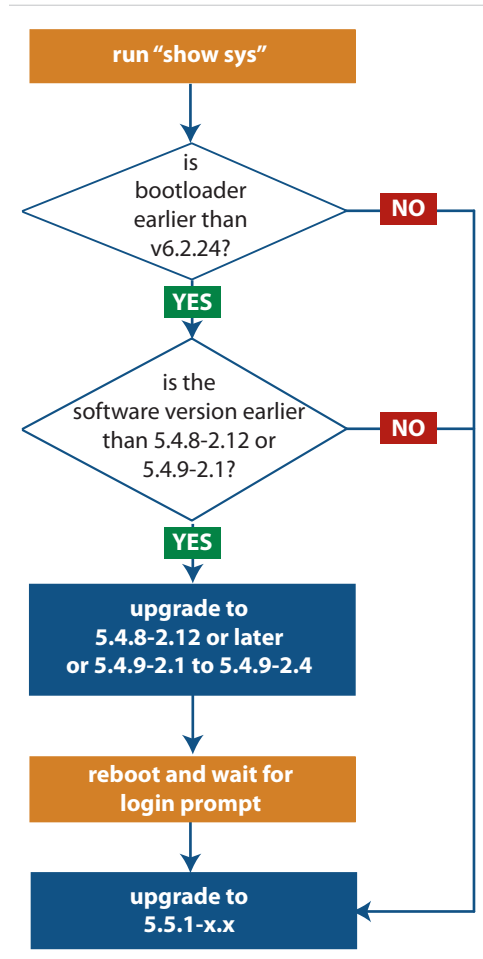
- [Software release licensing](#)
- [Upgrading a VCStack with rolling reboot](#)
- [Forming or extending a VCStack with auto-synchronization](#)
- [AMF software version compatibility](#)
- [Upgrading all devices in an AMF network](#)

If you are upgrading from an earlier version than 5.5.1-x.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.5.0-1.x version, please check the 5.5.0-2.x release note. Release notes are available from our website, including:

- [5.5.0-x.x release notes](#)
- [5.4.9-x.x release notes](#)
- [5.4.8-x.x release notes](#)
- [5.4.7-x.x release notes](#)
- [5.4.6-x.x release notes](#)

## Upgrade compatibility for SBx908 GEN2 and x950 Series switches

On the SBx908 GEN2 and x950 Series switches, please check your bootloader and current software version before you upgrade to AlliedWare Plus version 5.5.1-x.x.



If your bootloader is older than 6.2.24, you can only upgrade to 5.5.1-x.x from the following software versions:

- ▶ 5.4.8-2.12 or a later 5.4.8-2.x version,
- ▶ or 5.4.9-2.1, 5.4.9-2.2, 5.4.9-2.3 or 5.4.9-2.4
- ▶ or any 5.5.0-x.x or 5.5.1-x.x version

If your bootloader is older than 6.2.24, your switch must be running one of the above versions when you upgrade to 5.5.1-x.x.

**If your bootloader is older than 6.2.24, you cannot upgrade to 5.5.1-x.x directly from:**

- ▶ 5.4.9-1.x,
- ▶ 5.4.9-0.x, or
- ▶ any version before 5.4.8-2.12

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

```
awplus# show system
```

If you experience issues when upgrading, please contact your Allied Telesis support team. See our website at [alliedtelesis.com/support](http://alliedtelesis.com/support).

## Changes that may affect device or network configuration

The following changes may require you to modify your device or network configuration when you upgrade to this release.

Summary	Affected devices	Detail
Some commands not available when accessing CLI via Vista Manager	<i>All AlliedWare Plus devices</i>	<p>From 5.5.1-0.1 onwards, users accessing the AlliedWare Plus command line via Vista Manager are unable to use the following CLI commands:</p> <ul style="list-style-type: none"> <li>■ atmf select area</li> <li>■ no atmf select area</li> </ul> <p>Also, for 5.5.1-0.1 and 5.5.1-0.2, users accessing the AlliedWare Plus command line via Vista Manager are unable to use the following CLI commands:</p> <ul style="list-style-type: none"> <li>■ atmf working-set</li> <li>■ no atmf working-set</li> <li>■ atmf remote-login</li> </ul> <p>Use of these commands was re-instated in 5.5.1-0.3.</p>

## Software release licensing

*Applies to SBx908 GEN2 and SBx8100 Series switches*

Please ensure you have a 5.5.1 license on your switch if you are upgrading to 5.5.1-x.x on your SBx908 GEN2 or SBx8100 switch. To obtain a license, contact your authorized Allied Telesis support center. You will need to provide the MAC addresses of the switches you want to license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 42](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 44.](#)

## Upgrading a VCStack with rolling reboot

*Applies to all stackable AlliedWare Plus switches, except SBx8100*

This version supports VCStack “rolling reboot” upgrades. With the **reboot rolling** command, you can reduce downtime when upgrading a VCStack.

### For SBx908 GEN2, x950 and x550 Series switches

You can use rolling reboot to upgrade to 5.5.1-0.x from:

- 5.5.0-x.x

On these switches, you **cannot** use rolling reboot to upgrade to 5.5.1-0.x from any version earlier than 5.5.0-0.x.

### For x530 Series switches using DAC to stack

If you are using DACs (Direct Attach Cables) to connect stack members, you can use rolling reboot to upgrade to 5.5.1-0.x from:

- 5.5.0-x.x
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

### For other switches and for x530 switches using SFP+ to stack

Otherwise, you can use rolling reboot to upgrade to 5.5.1-0.x from:

- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 5.4.4-1.x

### To use rolling reboot

First enter the **boot system** command, which will install the new release file on all stack members. Then enter the **reboot rolling** command.

## Forming or extending a VCStack with auto-synchronization

*Applies to all stackable AlliedWare Plus switches*

If you create a VCStack from switches that are running different software versions, auto-synchronization ensures that all members will run the same software version when they boot up.

If auto-synchronization is not supported between the software versions on the devices in your stack, you need to make sure all devices are running the same version before you connect the stack together.

### For SBx908 GEN2, x950 and x550 Series switches

Auto-synchronization is supported between 5.5.1-0.x and:

- 5.5.0-x.x

On these switches, auto-synchronization is not supported between 5.5.1-0.x and any version earlier than 5.5.0-0.x.

**For CFC960 cards  
on an SBx8100  
system**

If you want to combine CFC960 v2 and earlier CFC960 cards in a chassis or stack, make sure that the earlier cards are running 5.5.0-x.x or later before you combine them. This applies whether you:

- add a CFC960 v2 card to a chassis or stack that contains earlier CFC960 cards, or
- add an earlier CFC960 card to a chassis or stack that contains CFC960 v2 cards.

Auto-synchronization will not update the software on the earlier CFC960 cards.

Note that this situation only applies if your chassis or stack includes CFC960 v2 cards that are labeled "SBx81CFC960 v2" on the front panel of the card. All cards that are labeled "SBx81CFC960" are referred to as earlier cards, even if their documentation refers to them as version 2.

If you do combine cards that are running incompatible software, then remove the CFC960 v2 card or cards, update the software on the other cards, and re-install the CFC960 v2 cards.

**For x530 Series  
switches using  
DAC to stack**

If you are using DACs (Direct Attach Cables) to connect stack members, auto-synchronization is supported between 5.5.1-0.x and:

- 5.5.0-x.x
- 5.4.9-0.x (but not 5.4.9-1.x or 5.4.9-2.x)
- 5.4.8-2.x

**For other switches  
and for x530  
switches using  
SFP+ to stack**

Otherwise, auto-synchronization is supported between 5.5.1-0.x and:

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

It is not supported between 5.5.1-0.x and 5.4.6-1.1 or **any** earlier releases.



## AMF software version compatibility

*Applies to all AlliedWare Plus devices*

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

### If using an AMF controller

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

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

### If using secure mode

If your AMF network is in secure mode, all nodes must run version 5.4.7-0.3 or later. Upgrade all nodes to version 5.4.7-0.3 or later before you enable secure mode.

### If using Vista Manager EX

If you are using Vista Manager EX, then as well as the restrictions above:

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

### If using none of the above

If none of the above apply, then nodes running version 5.5.1-0.x are compatible with nodes running:

- 5.5.0-x.x
- 5.4.9-x.x
- 5.4.8-x.x
- 5.4.7-x.x
- 5.4.6-x.x
- 5.4.5-x.x
- 5.4.4-x.x
- 5.4.3-2.6 or later.

## Upgrading all devices in an AMF network

*Applies to all AlliedWare Plus devices*

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

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

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

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

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

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

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

## Obtaining User Documentation

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

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

## Verifying the Release File

On devices that support crypto secure mode, to ensure that the release file has not been corrupted or interfered with during download, you can verify the release file. To do this, enter Global Configuration mode and use the command:

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

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

This command compares the SHA256 checksum of the release file with the correct checksum for the file. The correct checksum is listed in the release's sha256sum file, which is available from the [Allied Telesis Download Center](#).

### Caution



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

**“% Verification Failed”**

**In the case of verification failure, please delete the release file and contact Allied Telesis support.**

All switch models of a particular series run the same release file and therefore have the same checksum. For example, all x930 Series switches have the same checksum.

If you want the switch to re-verify the file when it boots up, add the “crypto verify” command to the boot configuration file.

# Licensing this Version on an SBx908 GEN2 Switch

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

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

## 1. Obtain the MAC address for a switch

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

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

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

## 2. Obtain a release license for a switch

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

## 3. Apply a release license on a switch

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

## 4. Confirm release license application

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

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

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

```
awplus#show license

Board region: Global

Index          : 1
License name   : Base License
Customer name  : Base License
Type of license : Full
License issue date : 20-Mar-2021
Features included : AMF-APP-PROXY, AMF-GUEST, AMF-Starter, BGP-64,
                   EPSR-MASTER, IPv6Basic, L3-FORWARDING,
                   L3-MC-ROUTE, LAG-FULL, MLDSnoop, OSPF-64,
                   RADIUS-100, RIP, VCStack, VRRP

Index          : 2
License name   : 5.5.0
Customer name  : ABC Consulting
Quantity of licenses : 1
Type of license : Full
License issue date : 20-Mar-2021
License expiry date : N/A
Release       : 5.5.0
```

# Licensing this Version on an SBx8100 Series CFC960 Control Card

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

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

If your CFC960 control card is in a stacked chassis, you do not need to perform these steps on each chassis in the stack, only on the stack master.

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

## 1. Obtain the MAC address for a control card

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

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

```
awplus#show system mac license
MAC address for licensing:

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

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

## 2. Obtain a release license for a control card

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

## 3. Apply a release license on a control card

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

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

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

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

Stack member 1 installed 1 license

1 license installed.
```

#### 4. Confirm release license application

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

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

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

```
awplus#show license
OEM Territory : ATI USA
Software Licenses
-----
Index                : 1
License name         : Base License
Customer name       : ABC Consulting
Quantity of licenses : 1
Type of license      : Full
License issue date   : 20-Mar-2021
License expiry date  : N/A
Features included    : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100
                    : Virtual-MAC, VRRP

Index                : 2
License name         : 5.5.0
Customer name       : ABC Consulting
Quantity of licenses : -
Type of license      : Full
License issue date   : 20-Mar-2021
License expiry date  : N/A
Release              : 5.5.0
```

# Installing this Software Version



**Caution:** This software version requires a release license for the SBx908 GEN2 and SBx8100 switches. Contact your authorized Allied Telesis support center to obtain a license. For details, see:

- [“Licensing this Version on an SBx908 GEN2 Switch” on page 42](#) and
- [“Licensing this Version on an SBx8100 Series CFC960 Control Card” on page 44.](#)

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

1. Copy the software version file (.rel) onto your TFTP server.
2. If necessary, delete or move files to create space in the switch’s Flash memory for the new file. To see the memory usage, use the command:

```
awplus# show file systems
```

To list files, use the command:

```
awplus# dir
```

To delete files, use the command:

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

You cannot delete the current boot file.

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

```
awplus# copy tftp flash
```

Follow the onscreen prompts to specify the server and file.

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

```
awplus# configure terminal
```

Then set the switch to reboot with the new software version:

Product	Command
SBx8100 with CFC960	<code>awplus (config) # boot system SBx8100-5.5.1-0.3.rel</code>
SBx908 GEN2	<code>awplus (config) # boot system SBx908NG-5.5.1-0.3.rel</code>
x950 series	<code>awplus (config) # boot system x950-5.5.1-0.3.rel</code>
x930 series	<code>awplus (config) # boot system x930-5.5.1-0.3.rel</code>
x550 series	<code>awplus (config) # boot system x550-5.5.1-0.3.rel</code>
x530 series	<code>awplus (config) # boot system x530-5.5.1-0.3.rel</code>
x510 series	<code>awplus (config) # boot system x510-5.5.1-0.3.rel</code>
IX5-28GPX	<code>awplus (config) # boot system IX5-5.5.1-0.3.rel</code>
x320 series	<code>awplus (config) # boot system x320-5.5.1-0.3.rel</code>
x310 series	<code>awplus (config) # boot system x310-5.5.1-0.3.rel</code>
x230 series	<code>awplus (config) # boot system x230-5.5.1-0.3.rel</code>
x220 series	<code>awplus (config) # boot system x220-5.5.1-0.3.rel</code>
IE510-28GSX	<code>awplus (config) # boot system IE510-5.5.1-0.3.rel</code>



Product	Command
IE340 series	<code>awplus (config)# boot system IE340-5.5.1-0.3.rel</code>
IE300 series	<code>awplus (config)# boot system IE300-5.5.1-0.3.rel</code>
IE210L series	<code>awplus (config)# boot system IE210-5.5.1-0.3.rel</code>
IE200 series	<code>awplus (config)# boot system IE200-5.5.1-0.3.rel</code>
XS900MX series	<code>awplus (config)# boot system XS900-5.5.1-0.3.rel</code>
GS980M series	<code>awplus (config)# boot system GS980M-5.5.1-0.3.rel</code>
GS980EM series	<code>awplus (config)# boot system GS980EM-5.5.1-0.3.rel</code>
GS980MX/10HSm	<code>awplus (config)# boot system GS980MX-5.5.1-0.3.rel</code>
GS970M series	<code>awplus (config)# boot system GS970-5.5.1-0.3.rel</code>
GS900MX/MPX series	<code>awplus (config)# boot system GS900-5.5.1-0.3.rel</code>
FS980M series	<code>awplus (config)# boot system FS980-5.5.1-0.3.rel</code>
AR4050S	<code>awplus (config)# boot system AR4050S-5.5.1-0.3.rel</code>
AR3050S	<code>awplus (config)# boot system AR3050S-5.5.1-0.3.rel</code>
AR2050V	<code>awplus (config)# boot system AR2050V-5.5.1-0.3.rel</code>
AR2010V	<code>awplus (config)# boot system AR2010V-5.5.1-0.3.rel</code>
AR1050V	<code>awplus (config)# boot system AR1050V-5.5.1-0.3.rel</code>

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

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

- Reboot using the new software version.

```
awplus# reload
```

# Accessing the Web-based GUI on Switches

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

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

On SBx908 GEN2 switches, x950 Series, x930 Series, x550 Series and x530 Series, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

## Browse to the GUI

Perform the following steps to browse to the GUI.

1. If you haven't already, add an IP address to an interface. For example:

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

Alternatively, you can use the default address on unconfigured devices, which is 169.254.42.42.

2. Open a web browser and browse to the IP address from step 1.
3. The GUI starts up and displays a login screen. Log in with your username and password. The default username is *manager* and the default password is *friend*.

## Check the GUI version

To see which version you have, open the About page in the GUI and check the field called **GUI version**. The version to use with 5.5.1-0.3 is 2.8.0.

If you have an earlier version, update it as described in ["Update the GUI version" on page 49](#).

## Update the GUI version

Perform the following steps through the Device GUI and command-line interface if you have been running an earlier version of the GUI and need to update it.

1. Obtain the GUI file from our Software Download center. The filename for v2.8.0 of the GUI is awplus-gui\_551\_23.gui.

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

2. Log into the GUI:

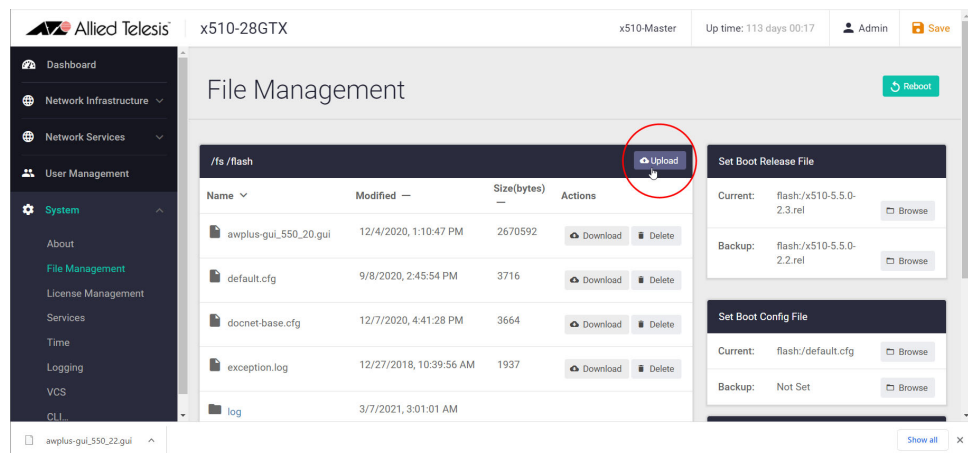
Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

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

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

3. Go to **System > File Management**

4. Click **Upload**.



5. Locate and select the GUI file you downloaded from our Software Download center. The new GUI file is added to the **File Management** window.

6. Use a Serial console connection, or Telnet or SSH to access the CLI, then use the following commands to stop and restart the HTTP service:

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

7. In the Device GUI, go to **System > About** to check that the latest file has been successfully added to the device. Look for the GUI Version and GUI Build entries. The first part of the GUI Build entry is the GUI build date.

System Information	
Name:	x510-Master
Model:	x510-28GTX
MAC Address:	00-10-00-00-00-04
Serial Number:	012345678
Environment:	<span style="color: orange;">▲</span> Status: Fault - PSU Power Output <input type="button" value="v"/>
Current Software:	x510-5.5.1-0.2.rel
Software Version:	5.5.1-0.2
Bootloader:	2.0.9-devel
GUI Version:	2.8.0
GUI Build:	20210423_1329

The device GUI service expects a GUI resource file with a .gui extension. If there is more than one .gui file then it will pick up the one with the highest number in its name.

For example, if the following two files are present:

- awplus-gui\_550\_22.gui
- awplus-gui\_551\_23.gui

The GUI service will use the .gui file with the 23 in its name, as this is the highest number.

# Accessing the Web-based GUI on AR-Series Devices

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

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

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

On AR4050S, AR3050S, AR2050V and AR2010V devices, you can also optimize the performance of your Allied Telesis APs through the Autonomous Wave Control wireless manager.

## Browse to the GUI

Perform the following steps to browse to the GUI.

**Prerequisite:** If the firewall is enabled, you need to create a firewall rule to permit traffic generated by the device that is destined for external services. See the "Configuring a Firewall Rule for Required External Services" section in the [Firewall and Network Address Translation \(NAT\) Feature Overview and Configuration Guide](#).

1. If you haven't already, add an IP address to an interface. For example:

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

Alternatively, you can use the default address on unconfigured devices, which is 192.168.1.1.

2. Open a web browser and browse to the IP address from step 1.
3. The GUI starts up and displays a login screen. Log in with your username and password. The default username is *manager* and the default password is *friend*.

## Check the GUI version

To see which version you have, open the About page in the GUI and check the field called **GUI version**. The version to use with 5.5.1-0.3 is 2.8.0. If you have an earlier version, update it as described in ["Update the GUI version" on page 49](#).

