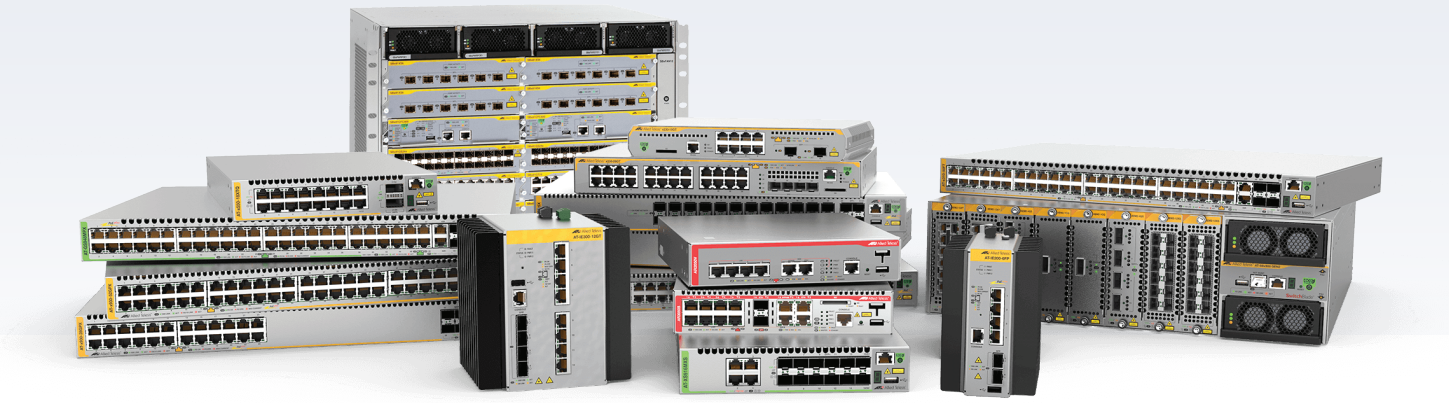
Release Note for AlliedWare Plus Software Version 5.5.1APCERT-0.3



AlliedWare Plus
OPERATING SYSTEM

» x950 Series » x320 Series » x220 Series

Acknowledgments

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/**

Contents

What's New in Version 5.5.1.APCERT-0.3

Product families supported by this version:

x950 Series
x320 Series
x220 Series

Introduction

This release note covers the differences between 5.5.1-0.3 and 5.5.1.APCERT-0.3

Software file details for this version are listed in Table 1. 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 8.

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
x950-52XSQ x950-52XTQm	x950	09/2022	x950-5.5.1.APCERT-0.3.rel
x320-10GH x320-11GPT	x320	09/2022	x320-5.5.1.APCERT-0.3.rel
x220-28GS x220-52GT x220-52GP	x220	09/2022	x220-5.5.1.APCERT-0.3.rel

Enhancements

This section summarizes the enhancements in software version: 5.5.1. APCERT-0.3.

To see how to find full documentation about all features on your product, see "Obtaining User Documentation" on page 7.

Spanning tree loop guard

Available on all AlliedWare Plus devices.

From version 5.5.1.APCERT-0.3 onwards, AlliedWare Plus switches support STP loop guard, which helps prevent spanning-tree loops. Such loops can occur because of a unidirectional link failure on a point-to-point link, or software failures on switches with ports acting as designated ports in a spanning-tree.

Loop guard checks to make sure that root ports and alternate/backup ports keep receiving BPDUs from their designated port on the link. If a port stops receiving BPDUs from its designated port, it transitions to a state called 'loop-inconsistent' and discards packets. The port recovers from this loop-inconsistent state state as soon as it receives a BPDU again from the designated port.

New command You can enable loop guard on a per-port basis, using the new command:

(no) spanning-tree guard loop

Note that spanning-tree loop guard cannot be used with spanning-tree root guard. Only one of these may be configured on an interface.

Example To enable STP loop guard on port1.0.1, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# spanning-tree guard loop
awplus(config-if)# exit
```

To show the spanning-tree status of port1.0.1, use the command:

```
awplus# show spanning-tree interface port1.0.1
```

Unknown unicast flood blocking (UUFB)

Available on all AlliedWare Plus devices.

From version 5.5.1.APCERT-0.3 onwards, you can use UUFB to prevent unknown unicast traffic being flooded to all Layer 2 ports in a VLAN. The UUFB feature blocks unknown unicast traffic flooding and only permits egress traffic with MAC addresses that are known to exit on a specific egreess port.

New command

Use the following new command to activate the UUFB feature:

(no) switchport block unicast-flooding

Example

To enable UUFB on port1.0.13, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.13
awplus(config-if)# switchport block unicast-flooding
```

To show the UUFB status of port1.0.13, use the commands:

```
awplus# show interface port1.0.13
awplus# show running-config interface port1.0.13
```

```
awplus#show interface port1.0.13
Interface port1.0.13
Scope: both
Link is UP, administrative state is UP
Thrash-limiting
Status Not Detected, Action learn-disable, Timeout 1(s)
Hardware is Ethernet, address is eccd.6dc4.24f5
index 5013 metric 1 mru 1500
current duplex full, current speed 1000, current polarity mdix
configured duplex auto, configured speed auto, configured
polarity auto
<UP,BROADCAST,RUNNING,MULTICAST>
SNMP link-status traps: Disabled
input packets 0, bytes 0, dropped 0, multicast packets 0
output packets 0, bytes 0, multicast packets 0, broadcast
packets 0
input average rate : 30 seconds 0 bps, 5 minutes 0 bps
output average rate: 30 seconds 0 bps, 5 minutes 0 bps
Time since last state change: 0 days 00:00:35
Unknown unicast flooding blocking is enabled
```

```
awplus#show running-config interface port1.0.13
! interface port1.0.13
switchport
switchport mode access
switchport block unicast-flooding
!
```

Additional small enhancements

There are a number of additional smaller enhancements available with version 5.5.1.APCERT-0.3 onwards, they are as follows:

- Upgraded hardware entropy generation software.
- The issue with IPSEC starting up erroneously in secure mode is resolved.
- QoS tuning and functions are enhanced.
- SHA-3 details are now visible in the output of the **show post** command. This command provides results of the file integrity check, filesystem tests, and FIPS post including cryptographic function tests.
- Internal support for NIST ACVP test framework is added.

Resolved issues

This section summarizes the resolved issues in software version 5.5.1.APCERT-0.3.

CR-75344 Previously, when using the **wrr-queue queue-limit** command, the applied limits could have been incorrectly calculated.

This issue has been resolved.

The **wrr-queue queue-limi**t command has been ammended to allow more flexibility in such a way that:

- if the sum of ratios < 90, the per-queue allocation will be relative to the sum of the ratios (ratio / sum of ratios)
- if the sum or ratios >= 90, the per-queue allocation will be relative to 100% (ratio / 100). This is because assumes it was an attempt to fully consume the port bandwidth.

CR-74612 Previously, SSH service in crypto-secure mode allowed CBC mode ciphers. This was potentially a security vulnerability.

This issue has been resolved with a new command to optionally disable CBC mode ciphers for SSH server in cypto secure mode.

New command The new command is:
(no) ssh server disallow-cbc-ciphers

With this command, the SSH server will only offer aes128-ctr, aes192-ctr, and aes256-ctr cipher algorithms.

Example To disallow CBC mode ciphers for the SSH server in crypto secure-mode, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server disallow-cbc-cipher
```

Important Considerations Before Upgrading

Please read this section carefully before upgrading.

If you are upgrading from an earlier version than 5.5.1-0.x, please check previous release notes for other important considerations. For example, if you are upgrading from a 5.4.9-1.x version, please check the 5.4.9-2.x release note. Release notes are available from our website, including:

- 5.5.1-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

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 x950 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.

Installing this Software Version

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
x950 series	`awplus(config)# boot system x950-5.5.1.APCERT-0.3.rel`
x320 series	`awplus(config)# boot system x320-5.5.1.APCERT-0.3.rel`
x220 series	`awplus(config)# boot system x220-5.5.1.APCERT-0.3.rel`

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

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

6. Reboot using the new software version.

   ```
   awplus# reload
   ```