IQ Engine Release Notes

Version 10.6.1a

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Table of Contents

General Release Information

Release 10.6.1a

December 2023

There are no feature updates for this release.

For information about security updates and addressed issues, see Addressed Issues on page 6.

New Hardware

There is no new hardware supported with this release.

Updated Hardware

The following models are updated for this release:

- AP30
- AP122
- AP122X
- AP130
- AP150W
- AP230
- AP245X
- AP250
- AP550
- AP1130

Management Platforms Supported

ExtremeCloud IQ 23.3.0 and later

Virtual Appliance 21.1.23.4

New Features

There are no feature updates for Release 10.6.1a.

Table 1: Release 10.6.1

Feature ID	New Feature	Description
HOS-17250	AP5050U and AP5050D	AP5050 now supports Client Mode.
HOS-18811	AP5050U and AP5050D	AP5050 now supports Honduras
HOS-18988	AP5050U and AP5050D	AP5050 now supports Japan, No 6E

Addressed Issues

Table 2: Release 10.6.1a

Issue ID	Description
CFD-8010	Resolved an issue with wireless clients losing connectivity on 0.0.0.0, when the DHCP Server/NAT AP is rebooted.
CFD-8240	Resolved an issue with Zebra MC9300 handhelds showing incorrect errors in the Client Trail.
CFD-8965	Resolved an issue with Cloud PPSK users randomly being assigned the default user profile.
CFD-9022	Resolved an issue with Framed-IP-Address AVP appearing twice in Accounting-Request packets.
CFD-9270	Resolved an issue with the continuous deauthentication of wired clients on Eth ports for AP302W models in router mode.
CFD-9684	Resolved an issue with high CPU usage on AP550 models when nearby robots are on the same 2.4 GHz channel, caused by continuous "Wireless Event (cmd=0x8C02) too big (1519)" error prints to the log.
HOS-18796	Resolved HiveOS/IQ Engine Vulnerabilities through CAPWAP.
HOS-18962	Resolved CVE-2022-0778.
HOS-19119	Resolved an issue with WPA3 intermittently not working on AP250 models.
HOS-19168	Security Enhancement: Unauthenticated buffer-overflow fixed.
HOS-19235	Security Enhancement: Cacheable Server Responses Containing PPSKs
HOS-19394	Resolved an issue with 802.1X authentication failures on the wired interface.
HOS-19469	Security Enhancement: TCP Port 5918 is closed by default.

Table 3: Release 10.6.1

Issue ID	Description
CFD-8860 (02705921, 02739394)	Resolved an issue where APs were showing high CPU utilization when they were running 10.5.3 or above. Affected AP122/AP150W/AP302W/AP460C.
CFD-8854 (02718195)	Resolved an issue with some APs requiring a reboot to connect to SSIDs broadcast on wifi1/5GHz.

Table 3: Release 10.6.1 (continued)

Issue ID	Description
CFD-8669 (02652714)	Resolved an issue where on the AP130, WiFi1 stopped transmitting intermittently.
CFD-8188 (02623237, 02635389, 02710327)	Resolved an issue where the AP650X failed to update when **Location Essentials** was enabled.
HOS-18800	Resolved an issue where Function Test roam failed with the target AP sending a `deauth` reason of `unspecified failure on receiving reassoc req from sta`.
HOS-18796	Resolved an issue that involved HiveOS/IQ Engine Vulnerabilities through CAPWAP.

Known Issues

Table 4: Known issues for 10.6.0 and later releases

Issue ID	Description
HOS-17683	Some WPA3 clients cannot associate to the AP4000 properly when band steering is enabled. **Workaround**: Disable band steering.
CFD-7445	802.11ax client, such as iPhone 12/13, experiences difficulties when receiving 11ac frames if the MCS rate >5 on a Wave1 chip platform, such as AP230, AP122, and AP130. **Workaround**: Use 11AC with lower MCS rates (from 0-3), or use 11N.