

IQ Engine 10.5r2

Release Notes

September 2022



Copyright © 2022 Extreme Networks, Inc. All rights reserved.

Legal Notice

, 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 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

and the logo are trademarks or registered trademarks of , 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 trademarks, see:

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..... | 4 |
| Release Date..... | 4 |
| Hardware platforms supported..... | 4 |
| Management platforms supported..... | 4 |
| New Features..... | 5 |
| Known Issues..... | 6 |
| Addressed Issues..... | 7 |



General Release Information

Release Date

September 2022

Hardware platforms supported

- AP122
- AP230
- AP1130
- AP150W
- AP550
- AP30
- AP305C/CX
- AP305C-1
- AP302W
- AP510C/CX
- AP410C
- AP410C-1
- AP4000
- AP4000-1
- AP5010
- AC, WiFi6, and WiFi6E models

Management platforms supported

ExtremeCloud IQ 22.4.0.1 and later



New Features

The release introduces the following features:

(Security Enhancement) Unauthenticated File Read - .conf:

Use the follow command to stop the web server on the AP for advanced security.

No `system web-server hive-UI enable`

Disabling the web server will remove functionality for the following:

- PPSK self on boarding
- Local Captive Portal
- Maintenance Mode SSID (will normally broadcast and provide web access if AP is not connected to the cloud). SSH still accessible.
- Local AP management web server. SSH only.
- Client mode provisioning screens. SSH only.

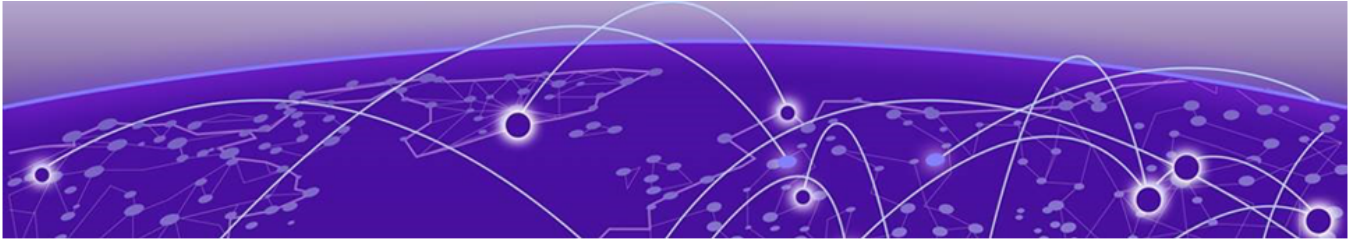
(Security Enhancement) Service accounts removed by default. New CLI Commands for Service Account Creation added: To use the WebUI image upgrade, use the following new CLI commands to add the WebUI service account and the CAPWAP service account to enable distributed image upgrades from the AP:

- `[no] webui exec scp-user`
- `[no] capwap exec scp-user`

(Security Enhancement) Admin Shell Backdoor Disabled: This has been disabled in production images.

(Security Enhancement) Bootloader Access Disabled: Bootloader access is now disabled to prevent hacker access.

Link Aggregation Support enabled with AD Essentials: AD Essentials and Link Aggregation now work simultaneously.



Known Issues

| Issue ID | Description |
|-----------|---|
| HOS-17683 | Some WPA3 clients cannot associate to the AP4000 properly when band steering is enabled. Workaround: Disable band steering. |



Addressed Issues

| Issue ID | Description |
|---------------------------|---|
| HOS-18459 | AP fails to power up completely when connected to ETH1 of a 5010 powered by a 3BT power source. |