FORTINET

Release Notes

FortiAP 6.4.8

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

Mar 21, 2023
FortiAP 6.4.8 Release Notes
20-648-805206-20230321

TABLE OF CONTENTS

Change log

Date	Change description
2022-05-12	Initial release.
2022-05-25	Removed Common vulnerabilities and exposures from Resolved issues on page 9.
2023-03-21	Added Common vulnerabilities and exposures to Resolved issues on page 9.

Introduction

This document provides the following information for FortiAP version 6.4.8, build 0197:

For more information about your FortiAP device, see the *FortiWiFi and FortiAP Configuration Guide*.

Supported models

FortiAP version 6.4.8, build 0197 supports the following models:

Models
FAP-231F, FAP-234F, FAP-23JF
FAP-431F, FAP-432F, FAP-433F
FAP-831F

What's new in FortiAP version 6.4.8

The following list includes FortiAP version 6.4.8 new features:

- FortiAP accepts hexadecimal values of EddyStone namespace ID and instance ID in Bluetooth low energy (BLE) profiles.
- A new command is added for FortiAP to upload Target Assert logs to a specified TFTP server.

  CLI: `cw_diag wlanfw-dump <TFTP server IP>`.
- Region/country code updates and DFS certification:
  - Supports DFS channels on FAP-231F with region code N (including Brazil), P, and U.
  - Supports DFS channels on FAP-234F with region code J, N (including Brazil) and P.
  - Supports DFS channels on FAP-23JF with region code K, N (including Brazil), P and S.
  - Supports DFS channels on FAP-431F with region code N (including Brazil), P and U.
  - Supports DFS channels on FAP-432F with region code J, N (including Brazil) and P.
  - Supports DFS channels on FAP-433F with region code N (including Brazil) and P.
  - Supports DFS channels on FAP-831F with region code A, D, E, I, N (including Brazil), P, S, T, V and Y.
  - The region code of Israel and Qatar is changed from "I" to "E".
  - The default country of region "I" is set as Morocco.

Special notices

New Wi-Fi 6/802.11ax models FAP-431F, FAP-433F and FAP-231F initially supported in the FortiAP-W2 6.4.0 release have been moved to FortiAP 6.4.3 and later for continuing support.

Upgrade and downgrade information

Upgrading to FortiAP version 6.4.8

FortiAP 6.4.8 supports upgrading from FortiAP version 6.4.3 and later.

Downgrading to previous firmware versions

FortiAP 6.4.8 supports downgrading to FortiAP version 6.4.3 and later.

Firmware image checksums

To get the MD5 checksum code for a Fortinet firmware image, perform the following steps:

1. Go to the Fortinet Support website.
2. Log in to your account. If you do not have an account, create one and then log in.
3. From the top banner, select **Download > Firmware Image Checksums**.
4. Enter the image file name, including the extension. For example, FAP_221C-v6-build0030-FORTINET.out.
5. Click **Get Checksum Code**.

Supported upgrade paths

To view all previous FortiAP versions, build numbers, and their supported upgrade paths, see the Fortinet Documentation website.

Product integration support

The following table lists product integration and support information for FortiAP version 6.4.8:

FortiOS	6.4.9 and later
Web browsers	Microsoft Edge version 41 and later
	Mozilla Firefox version 59 and later
	Google Chrome version 65 and later
	Apple Safari version 9.1 and later (for Mac OS X)
	Other web browsers may work correctly, but Fortinet does not support them.

We recommend that the FortiAP firmware version be matched with the respective FortiOS version, when available. Other variations of FortiOS and FortiAP versions may technically work for the lowest common feature set. However, if problems arise, Fortinet Support will ask that the versions be matched, as recommended, before troubleshooting.

Resolved issues

The following issues have been resolved in FortiAP version 6.4.8. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
421233	FortiAP failed to disable wireless multimedia (WMM) settings in the QoS profile.
606388	Sometimes, FortiGate would report SSID's from authorized FortiAP devices as "fake-ap-on-air".
651452	The console port of FAP-231F, 234F and 23JF would occasionally lock-up.
716641	On local-standalone SSID, RADIUS authentication requests were not sent to the secondary RADIUS server when the first one was unreachable.
719386	Synchronize FortiPresence data reporting based on the system time of the WiFi Controller.
724927	FortiAP would take a long time to connect back to the WiFi Controller after implementing reboot from FortiAP CLI.
733260	Draeger Delta devices suffered from multicast packets loss for a long period of time.
746769	Fixed a Target Assert issue: `ar_wal_peer.c:4578 Assertion 0 failedparam0 :zero, param1 :zero, param2 :zero.`
754299	FortiAP devices previously connected to FortiLAN Cloud could not reconnect after some time.
754327	Fixed a dynamic VLAN assignment issue when RADIUS-MAC authentication was delayed.
754775	FortiAP might send corrupted IPv6 client information to FortiGate when reconnected.
767608	802.11n and 802.11ac clients could not connect with local-standalone SSID.
767941	802.11ax clients got low throughput when connected to an SSID with PMF set to optional.
774055	Captive-portal SSID with VLAN ID could not work as the DNS IP was blocked.
776707	Sometimes, FortiAP didn't report LLDP info to the WiFi Controller.
779712	FortiAP would stop responding to SNMP queries sometimes.

Common vulnerabilities and exposures

FortiAP 6.4.8 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) references:

Bug ID	Description
786638	CVE-2022-29058 (Command injection in CLI).

Visit https://fortiguard.com for more information.

Known issues

The following issues have been identified in FortiAP version 6.4.8. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
645121	FortiAP should report detected station information from radio1 and radio2 when FortiPresence is enabled.
692160	Wireless packets captured by FortiAP radio in Sniffer mode are corrupted.
761298	FAP-234F Bluetooth Low Energy (BLE) function cannot work.
767916	When wireless clients are connected to different radios of the same tunnel-mode SSID with static or dynamic VLAN, they cannot ping each other.
795661	Wireless clients cannot communicate with wired clients behind a switch connected to mesh-Ethernet bridge.

www.fortinet.com