FortiAP - Release Notes

Version 6.4.7

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

Sep 7, 2021
FortiAP 6.4.7 Release Notes
20-647-743780-20210907

TABLE OF CONTENTS

Change log

Date	Change description
2021-09-07	Initial release.

Introduction

This document provides the following information for FortiAP version 6.4.7, build 0185:

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

Supported models

FortiAP version 6.4.7, build 0185 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 6.4.7

The following list includes FortiAP version 6.4.7 new features:

- Reports more information (SGI, bandwidth, max rate, PHY mode) of rogue APs to the FortiGate WiFi controller.
  Note: FortiGate needs to run FortiOS 7.0.2 and later.
- Support DFS channels on FAP-231F with region code K, N and S.
- Support DFS channels on FAP-234F with region code T.
- Support DFS channels on FAP-23JF with region code A, J and T.
- Support DFS channels on FAP-431F/433F with region code S.
- Support DFS channels on FAP-432F with region code A and T.

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 6.4.7

FortiAP 6.4.7 supports upgrading from FortiAP version 6.4.3 and later.

Downgrading to previous firmware versions

FortiAP 6.4.7 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 6.4.7:

FortiOS	6.4.7 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 6.4.7. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
708954	A batch of FAP-231F units lost connection intermittently due to CRC errors in received and transmitted packets.
709421	FortiCloud SSID would deny station connections after running for one or two days due to an issue in the station counter.
719640	WiFi clients cannot connect bridge-mode SSID when NP7 FGT has capwap-offload enabled.
722948	Mesh fast roaming didn't work in 802.11ax FAP models.
733260	Draeger Delta devices suffered from multicast packets loss for a long period of time.
738596	FAP SSH server limited the credentialed scan performed with Nessus Scanner.

Common vulnerabilities and exposures

FortiAP 6.4.7 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) references:

Bug ID	Description
719016	FRAG attack: • CVE-2020-24586 • CVE-2020-24587 • CVE-2020-24588

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

Known issues

The following issues have been identified in FortiAP version 6.4.7. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
645121	FAP should report detected station information from radio1 and radio2 when FortiPresence is enabled.