



Release Notes

FortiAP 7.6.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



Oct 23, 2025

FortiAP 7.6.3 Release Notes

20-763-1209900-20251023

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
New features or enhancements	6
Region/country code update and DFS certification	6
Changes in CLI	7
Upgrade and downgrade information	8
Upgrading to FortiAP version 7.6.3	8
Downgrading to previous firmware versions	8
Firmware image checksums	8
Supported upgrade paths	8
Product integration support	9
Resolved issues	10
Known issues	11

Change log

Date	Change description
2025-10-23	Initial release.

Introduction

This document provides release information for FortiAP version 7.6.3, build 1032.

For more information about your FortiAP device, see the [FortiWiFi and FortiAP Configuration Guide](#).

Supported models

FortiAP version 7.6.3, build 1032 supports the following models:

Wi-Fi 6 Models

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

Wi-Fi 6E Models

FAP-231G, FAP-233G, FAP-234G,
FAP-431G, FAP-432G, FAP-433G

Wi-Fi 7 Models

FAP-231K, FAP-23JK,
FAP-241K, FAP-243K,
FAP-441K, FAP-443K

New features or enhancements

The following table includes FortiAP version 7.6.3 new features and enhancements:

Bug ID	Description
0839368	Support Zero-Wait Dynamic Frequency Selection (DFS).
0951642	FAP-234G, 432G, 441K, and 443K support Automated Frequency Coordination (AFC).
1087811	FortiAP Wi-Fi 7 models support Multi-Link Operation (MLO) and Preamble Puncturing.
1107131	Support Zero-Touch Provisioning (ZTP) in mesh configuration.
1151548	Support bypassing the default Captive Network Assistant (CNA).
1164271	Improve stability of CAPWAP connections between FortiAP and FortiEdge Cloud.
1187579	Improve the foreground scan and dedicated scan radio functions on FortiAP Wi-Fi 6E and 7 models.

Region/country code update and DFS certification

Bug ID	Description
1137875	Enable 6GHz channels 1 ~ 93 for Indonesia (ID), excluding FAP-234G, 432G, 243K, and 443K.
1146051	Enable DFS channels for FAP-241K and FAP-243K with region code "N" (Brazil) and region code "J".
1151022	Enable DFS channels for FAP-234G with region code "U" (Ukraine).
1153860	Enable DFS channels for FAP-441K and FAP-443K with region code "K".
1160566	Enable DFS channels for FAP-231K with region code "A" and "T".
1154577	Enable DFS channels for FAP-23JK with region code "H".
1155395	Enable DFS channels for FAP-23JK with region code "P".
1158383	Enable DFS channels for FAP-432G with region code "J".
1160626	Enable 6GHz channels 1 ~ 93 for Egypt (EG).
1174024	Enable DFS channels for FAP-231K and FAP-443K with region code "D".
1183521	Enable DFS channels for FAP-23JK with region code "J".
1184533	Enable DFS channels for FAP-432G with region code "K".

Bug ID	Description
1184975	Disable 6GHz channels for Oman (OM).
1187727	Enable DFS channels for FAP-231K with region code "K".
1188974	Enable DFS channels for FAP-231K with region code "J".
1203318	Disable 6GHz channels for Vietnam (VN).

Changes in CLI

Bug ID	Description
1107131	The factory default value of MESH_AP_TYPE is changed to 2 (Ethernet with mesh backup support). The factory default value of MESH_AP_SECURITY is changed to 1 (WPA/WPA2-Personal or WPA3-SAE).
1145886	Add 240MHz and 320MHz as site-survey channel bandwidth options for FortiAP Wi-Fi 7 models. SURVEY_CW_50: Select a 5G channel bandwidth used for site survey SSID (default=0): • 0(20MHz) • 1(40MHz) • 2(80MHz) • 3(160MHz) • 4(240MHz). SURVEY_CW_60: Select a 6G channel bandwidth used for site survey SSID (default=0): • 0(20MHz) • 1(40MHz) • 2(80MHz) • 3(160MHz) • 4(320MHz)

Upgrade and downgrade information

Upgrading to FortiAP version 7.6.3

FortiAP 7.6.3 supports upgrading from FortiAP version 7.4.3 and later.

Downgrading to previous firmware versions

FortiAP 7.6.3 supports downgrading to FortiAP version 7.4.3 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 *Support > Firmware Image Checksum*.
4. Enter the image file name, including the extension. For example, FAP_231F-v7-build0365-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 7.6.3:

FortiOS	FortiOS 7.6.4 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 7.6.3. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
0966608	Fixed a crash issue in FortiAP Wi-Fi 6 models (Target Assert at ar_wal_tqm.c:408).
1001394	FortiAP antenna gains have been adjusted to be up-to-date.
1094307	FortiAP intermittently disconnected from FortiGate HA setup when the MPSK VAP was configured.
1145853	FortiAP underwent an unnecessary reboot during the FortiOS upgrade in HA FortiGate units.
1152942	FortiAP should disable lightweight requests to FortiEdge Cloud on UDP port 53 as it is obsolete.
1158407	Fixed a packet drop issue in FortiAP Wi-Fi 6E and Wi-Fi 7 models.
1159906	The USB port of FAP-241K/243K should be enabled when the power mode is high (802.3at PoE).
1183316	FAP-243K and FAP-443K should support optional antenna "FANT-04BEAX-0606-PR".
1201399	Fixed a crash issue in FortiAP (at ieee80211_recv_action).
1213894	FortiAP Wi-Fi 6 models should enable 802.11ax when country code is Ukraine (UA).

Known issues

The following issues have been identified in FortiAP version 7.6.3. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
980717	FAP-234G/432G outdoor mode cannot work on the 6GHz radio band.
981982	FAP-234G/432G as mesh leaf cannot create a connection with mesh root FAP. Workaround: On the FortiGate, edit the wtp-profile of FAP-234G/432G, and set indoor-outdoor-deployment to indoor.
1217849	FortiAP cannot respond to the command <code>diagnose wireless-controller wlap wtpcmd</code> sent by FortiGate.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.