

Release Notes

FortiAP 7.4.2



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>

FORTINET TRAINING 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



Dec 28, 2023

FortiAP 7.4.2 Release Notes

20-742-983876-20231228

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	6
Upgrade and downgrade information	8
Upgrading to FortiAP version 7.4.2	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
2023-12-28	Initial release.

Introduction

This document provides release information for FortiAP version 7.4.2, build 0634.

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

Supported models

FortiAP version 7.4.2, build 0634 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-433G

New features or enhancements

The following table includes FortiAP version 7.4.2 new features and enhancements:

Bug ID	Description
904048	SAM test can support more security modes: OWE, WPA3-SAE, and WPA2/WPA3-Enterprise.
932066	WPA3-SAE SSID can support "Hunting-and-Pecking (HnP) only" setting as configured from the FortiGate.
942942	Third-party external antenna gain can be configured from the FortiGate. Supported FortiAP models are FAP-432F, FAP-432FR, FAP-433F, FAP-233G, and FAP-433G.
963865	Improve CAPWAP connectivity over a NAT device by sending keep-alive messages at the configured time interval in "nat-session-keep-alive" from the FortiGate.
967338	Support automated reboot functionality when stuck in a discovery loop.
967547	Support simplified Bonjour profile provisioning and failover mechanism.
970729	Support individual control of IEEE 802.11k and 802.11v protocols in SSID configuration.
973755	Support new model FAP-234G.

Region/country code update and DFS certification

Bug ID	Description
950124	Support 6GHz channels in Brazil, Colombia, Costa Rica, Dominican Republic, Guatemala, Honduras, Peru, and Saudi Arabia.
950206	Support 6GHz channels in Argentina, and El Salvador.
951886	Enable DFS channels for FAP-431G and FAP-433G with region code "T".
974085	Enable DFS channels for FAP-431G and FAP-433G with region code "J".

Changes in CLI

Bug ID	Description
960062	Add a command to help generate private key for WPA3-SAE SSID with Public Key authentication enabled. FortiAP CLI:

Bug ID	Description
	cw_diag sae-pk-gen ssid [curve:prime256v1 secp384r1 secp521r1]

Upgrade and downgrade information

Upgrading to FortiAP version 7.4.2

FortiAP 7.4.2 supports upgrading from FortiAP version 7.2.2 and later.

Downgrading to previous firmware versions

FortiAP 7.4.2 supports downgrading to FortiAP version 7.2.2 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 7.4.2:

FortiOS	FortiOS 7.4.2 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 7.4.2. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
761298	FAP-234F Bluetooth Low Energy (BLE) function could not work.
915600	FAP-431G/433G could not auto negotiate 802.3bt power level from a capable switch.
964007	Wi-Fi clients encounter a login prompt again when roaming over external-portal SSID in bridging mode.
981265	Local-standalone SSID with RADIUS authentication could not apply the customized port number to accounting packets.

Known issues

The following issues have been identified in FortiAP version 7.4.2. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
692160	Wireless packets captured by FortiAP radio in Sniffer mode are corrupted.
928135	FAP-231G/233G 2.4GHz radio sometimes would stop beaconing multiple SSIDs.
981982	FAP-234G as mesh leaf cannot create a connection with mesh root FAP. Workaround: On the FortiGate, edit the <code>wtp-profile</code> of FAP-234G, and set <code>indoor-outdoor-deployment</code> to <code>indoor</code> .



www.fortinet.com

Copyright© 2023 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 General Counsel, 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.