



Release Notes

FortiAP-W2 7.2.5



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



Mar 18, 2025

FortiAP-W2 7.2.5 Release Notes

40-725-1135233-20250318

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
New features or enhancements	6
Region/country code update and DFS certification	6
Special notices	7
Upgrade and downgrade information	8
Upgrading to FortiAP-W2 version 7.2.5	8
Downgrading to previous firmware versions	8
Firmware image checksums	8
Supported upgrade paths	8
Product integration and support	9
Resolved issues	10
Known issues	11

Change log

Date	Change description
2025-03-18	Initial release.

Introduction

This document provides release information for FortiAP-W2 version 7.2.5, build 0386:

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

Supported models

FortiAP-W2 version 7.2.5, build 0386 supports the following models:

Models
FAP-221E, FAP-222E, FAP-223E, FAP-224E, FAP-231E



FortiAP-W2 models do not have the unified threat management (UTM) functionality.

New features or enhancements

FortiAP-W2 version 7.2.5 contains bug fixes and stability improvements.

Region/country code update and DFS certification

Bug ID	Description
0911455	Add Nigeria (NG) to region code "I". Add Djibouti (DJ), Gabon (GA), Gambia (GM), Liberia (LR), Somalia (SO), and Swaziland (SZ) to region code "E".
1030697	Enable DFS channels for FAP-221E Gen3 with region code "U" (Ukraine).
1061658	Change Uzbekistan to region code "P".

Special notices

In order to protect the wireless calibration data, FortiAP-W2 version 7.2.5 and version 7.4.4 have revised the file system partitions.

FortiAP-W2 models running firmware version 7.2.5

- **cannot** be downgraded to version 7.2.4 and earlier versions;
- **cannot** be upgraded to version 7.4.0, 7.4.1, 7.4.2 and 7.4.3;
- can be upgraded to version 7.4.4 (and later versions).

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.2.5

FortiAP-W2 version 7.2.5 supports upgrading from FortiAP-W2 version 7.0.3 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.2.5 does **not** support downgrading to FortiAP-W2 version 7.2.4 and earlier. For more information, see [Special notices on page 7](#).

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_221E-v700-build0337-FORTINET.out.
5. Click **Get Checksum Code**.

Supported upgrade paths

To view all previous FortiAP-W2 versions, build numbers, and their supported upgrade paths, see the [Fortinet Documentation](#) website.

Product integration and support

The following table lists product integration and support information for FortiAP-W2 version 7.2.5:

FortiOS	7.2.9 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-W2 version 7.2.5. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
0692160	Wireless packets captured by the FortiAP radio in Sniffer mode were corrupted.
0815950	HTTPS access to the FortiAP web UI would randomly become inaccessible.
0899796	FortiAP couldn't handle fragmented packets randomly.
0931520, 1027267	FortiAP could not properly scan wireless stations with new MAC addresses.
1011732	FortiAP could not reconnect to FortiLAN Cloud after the network recovered from power outages.
1017829	FortiAP failed to report its LLDP neighbors to the new primary FortiGate after HA failover.
1042993	FortiAP added extra padding in the Circuit ID field of DHCP option 82.

Known issues

The following issues have been identified in FortiAP-W2 version 7.2.5. For inquiries about a particular bug or to report a bug, visit the [Fortinet Support](#) website.

Bug ID	Description
537931	FAP-222E doesn't support the FortiAP Configuration mode. Push and hold the RESET button on the POE adapter for more than 5 seconds to reset FAP-222E to the factory default.
655887	FAP-221E/223E gets low throughput on tunnel SSID when its <code>wtp-profile</code> has set <code>dtls-policy ipsec-vpn</code> .



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.