

Release Notes

FortiAP-W2 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



Jan 4, 2024

FortiAP-W2 7.4.2 Release Notes

40-742-985802-20240104

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
New features or enhancements	6
Changes in CLI	6
Upgrade and downgrade information	7
Upgrading to FortiAP-W2 version 7.4.2	7
Downgrading to previous firmware versions	7
Firmware image checksums	7
Supported upgrade paths	7
Product integration and support	8
Resolved issues	9
Known issues	10

Change log

Date	Change description
2024-01-04	Initial release.

Introduction

This document provides release information for FortiAP-W2 version 7.4.2, build 0596:

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

Supported models

FortiAP-W2 version 7.4.2, build 0596 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

The following table includes FortiAP-W2 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.
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.

Changes in CLI

Bug ID	Description
960062	Add a command to help generate a private key for WPA3-SAE SSID with Public Key authentication enabled. FortiAP CLI: <code>cw_diag sae-pk-gen ssid [curve:prime256v1 secp384r1 secp521r1]</code>

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.4.2

FortiAP-W2 version 7.4.2 supports upgrading from FortiAP-W2 version 7.2.2 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.4.2 supports downgrading to FortiAP-W2 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_S221E-v600-build0233-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 7.4.2:

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-W2 version 7.4.2. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
923193	5GHz band background scan would be stuck on DFS channels.
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-W2 version 7.4.2. 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 wtp-profile has set <code>dtls-policy ipsec-vpn</code> .
692160	Wireless packets captured by FortiAP radio in Sniffer mode are corrupted.



www.fortinet.com

Copyright© 2024 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.