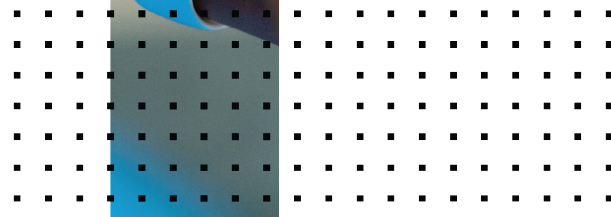


Release Notes

FortiAP-W2 7.0.3



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



Feb 22, 2022

FortiAP-W2 7.0.3 Release Notes

40-703-0783684-20220222

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	7
Upgrading to FortiAP-W2 version 7.0.3	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
2022-02-22	Initial release.

Introduction

This document provides release information for FortiAP-W2 version 7.0.3, build 0060:

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

Supported models

FortiAP-W2 version 7.0.3, build 0060 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 7.0.3 new features and enhancements:

Bug ID	Description
745957	Supports dynamic VLAN assignment by Name Tag. A "vlan-name" table can be configured per VAP/SSID. When the attribute "Tunnel-Private-Group-Id" in the RADIUS Access-Accept message can match any "vlan-name" entry, the corresponding "vlan-id" value will be assigned to the client.
752876	Supports 802.11r roaming on local-standalone SSID. Note: FortiGate needs to run FortiOS version 7.0.6, 7.2.0 and later.
755766	FortiAP local WAN port authentication (802.1x supplicant settings) can be configured via FortiAP web UI.

Region/country code update and DFS certification.

Bug ID	Description
758997	Supports DFS Channels on FAP-221E, FAP-222E, FAP-223E, FAP-224E and FAP-231E with region code "P" (Russia).
760881	Supports DFS Channels on FAP-221E with region code "U" (Ukraine).

Changes in CLI

Bug ID	Description
755438	Added a new <code>fap-tech</code> command for debugging customer issues.

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.0.3

FortiAP-W2 version 7.0.3 support upgrading from FortiAP-W2 version 6.4.5 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.0.3 support downgrading to FortiAP-W2 version 6.4.5 and later.



FAP-221E Gen3 and FAP-223E Gen3 cannot be downgraded to firmware 7.0.0 and earlier versions.

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 7.0.3:

FortiOS	7.0.4, 7.0.5 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 7.0.3. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
719386	Synchronize FortiPresence data reporting based on the system time of WiFi Controller.
754299	FortiAP devices previously connected to FortiLAN Cloud could not reconnect after some time.
754327	Fixed a dynamic VLAN assignment issue when RADIUS-MAC authentication was delayed.
767608	802.11n and 802.11ac clients could not connect with local-standalone SSID.
770624	Report FAP LAN port(s) <code>link_speed</code> , <code>carrier</code> and <code>duplex</code> info to FortiGate (for the REST API support).
771012	FortiAP couldn't report Hostname and Device OS of clients to FortiLANCloud if they were detected before FortiAP joins FortiLANCloud.
774055	Captive-portal SSID with VLAN ID could not work as the DNS IP was blocked.
776707	Sometimes, FortiAP didn't report LLDP info to WiFi Controller.

Known issues

The following issues have been identified in FortiAP-W2 version 7.0.3. 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© 2022 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.