

Release Notes

FortiAP-W2 7.0.0



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/support-and-training/training.html>

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



May 4, 2021

FortiAP-W2 7.0.0 Release Notes

40-700-0713598-20210504

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
New features or enhancements	6
Upgrade and downgrade information	7
Upgrading to FortiAP-W2 version 7.0.0	7
Downgrading to previous firmware versions	7
Firmware image checksums	7
Supported upgrade paths	7
Product integration and support	8
Resolved issues	9
Common vulnerabilities and exposures	9
Known issues	10

Change log

Date	Change description
2021-04-27	Initial release.
2021-05-04	Added a CVE section to Resolved issues on page 9

Introduction

This document provides release information for FortiAP-W2 version 7.0.0, build 0008:

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

Supported models

FortiAP-W2 version 7.0.0, build 0008 support 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 7.0.0 new features and enhancements:

Bug ID	Description
621445	FAP-224E/231E: When WAN-LAN mode is set, LAN2 port supports MAC address authentication, RADIUS accounting, and dynamic VLAN assignment.
653113	Adds the following enhancements for "voice-enterprise" SSIDs: <ul style="list-style-type: none">• Supports 802.11k Neighbor Report Dual Band;• Enhances 802.11v BSS Transition Management by adding Disassociation Imminent, Disassociation Timer for low RSSI, and Disassociation Timer for AP load-balancing.
691341	DHCP address enforcement forces connected clients to complete the DHCP process and obtain an IP address, otherwise they are disconnected from the SSID.
695639	FortiAP radio can support the service assurance management (SAM) mode as configured from FortiGate, to operate as a client and perform tests against another AP. Ping tests and iPerf tests can be run on interval, with results captured on WiFi event logs. This allows FortiGate to verify and ensure an existing Wi-Fi network can provide acceptable services.
697970	For RADIUS MAC authentication and Accounting, FortiGate supports pushing MAC Address Delimiter options in VAP configuration.
699401	Bridge captive-portal SSID has a new portal-type option "external-macauth" to support external Cisco ISE authentication.

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.0.0

FortiAP-W2 version 7.0.0 support upgrading from FortiAP-W2 version 6.4.5 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.0.0 support downgrading to FortiAP-W2 version 6.4.5 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 7.0.0:

FortiOS	7.0.0 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 7.0.0. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
684825	Unable to establish MESH between two FortiAP units when DHCP relay is used on FortiGate.
703088	Fix two TARGET ASSERT issues (in <code>_HTCPipeProcessControlMsg</code> and <code>_tx_send_seq_start_sequence</code>); Fix kernel panic "PC is at <code>nss_core_handle_napi</code> ".
710922	FortiAP units cannot stay on the channels assigned by FortiGate DARRP function.

Common vulnerabilities and exposures

FortiAP-W2 version 7.0.0 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) reference:

Bug ID	Description
681061	CVE-2021-26106: FortiAP OS command injection through hidden kdbg CLI command.

For details, visit the [FortiGuard Labs](#) website.

Known issues

The following issues have been identified in FortiAP-W2 version 7.0.0. 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> .



www.fortinet.com

Copyright© 2021 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.