

Release Notes

FortiAP-W2 7.0.1



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



Aug 3, 2021

FortiAP-W2 7.0.1 Release Notes

40-701-0735511-20210803

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 7.0.1	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
2021-08-03	Initial release.

Introduction

This document provides release information for FortiAP-W2 version 7.0.1, build 0033:

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

Supported models

FortiAP-W2 version 7.0.1, build 0033 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 7.0.1 new features and enhancements:

Bug ID	Description
642963	<p>After being authenticated on a bridge-mode external captive-portal SSID, the client can log out via an HTTP or HTTPS URL:</p> <ul style="list-style-type: none"> • <code>http://[FAP IP]:5000/logout</code> • <code>https://[FAP IP]:5001/logout</code> <p>The REST API to log out a client by MAC address:</p> <ul style="list-style-type: none"> • URL: <code>https://[FAP IP]/cp-logout</code> • Method: POST • Data: <code>macaddr=[client MAC address]</code>
705046	Supports VLAN ID assignment according to RADIUS attribute "Tunnel-Private-Group-Id" when it is a text string, and matches one interface name of sub-VLAN interfaces of VAP.
706967	Local-standalone NAT-mode SSID can configure optional DNS servers to assign out to wireless clients through DHCP.
709872	Supports "SKIP CAPWAP Offload" flag in CAPWAP header of certain packets as required by new FortiGate models with NP7 acceleration module.
719445	Console port on applicable FAP models can be enabled or disabled by <code>wtp-profile > console-login</code> setting from FortiGate.
726569	Supports FAP-221E Gen3 and FAP-223E Gen3.
730228	Supports captive-portal authentication in Service Assurance Manager (SAM) mode.

Changes in CLI

Bug ID	Description
700986	<p>For site-survey mode SSID, allow to set different transmit power levels for 2.4 and 5 GHz respectively.</p> <ul style="list-style-type: none"> • The previous "SURVEY_TX_POWER" has been replaced with "SURVEY_TX_POWER_24" and "SURVEY_TX_POWER_50"; • Value range: [1, 33] dBm; default=30.

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.0.1

FortiAP-W2 version 7.0.1 support upgrading from FortiAP-W2 version 6.4.5 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.0.1 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 7.0.1:

FortiOS	7.0.1 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 7.0.1. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
680436	FAPs were not failing over between primary and secondary FGTs when inter-controller-mode is in "1+1" fast failover mode.
696255	Leaf FAP rebooted with " <code>cwWtp_health_monitor vap wlan10 stuck in INIT</code> " error message on console port when DFS channel is used.
701896	After long idle time, WiFi clients cannot reconnect to FortiLAN Cloud SSID with PMF enabled.
709421	FortiCloud SSID would deny station connections after running one day or two due to an issue in station counter.
717014	Fix a kernel panic trace " <code>PC is at kmem_cache_alloc</code> ", caused by a memory corruption in WiFi driver.
718756	FAP in a remote location is unable to come online on a FGT in a central location via MPLS/site-to-site VPN.
719640	WiFi clients cannot connect bridge-mode SSID when NP7 FGT has capwap-offload enabled.

Common vulnerabilities and exposures

FortiAP-W2 version 7.0.1 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) reference:

Bug ID	Description
719016	FRAG attack: <ul style="list-style-type: none">• CVE-2020-24586• CVE-2020-24587• CVE-2020-24588

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

Known issues

The following issues have been identified in FortiAP-W2 version 7.0.1. 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.