FortiAP-S and FortiAP-W2 - Release Notes

Version 6.4.2

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/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 6, 2020
FortiAP-S and FortiAP-W2 6.4.2 Release Notes
40-642-654248-20200806

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Supported models 5
What's new in FortiAP-S and FortiAP-W2 version 6.4.2 5
Upgrade and downgrade information **7**
Upgrading to FortiAP-S and FortiAP-W2 version 6.4.2 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
2020-08-06	Initial release.

Introduction

This document provides the following information for FortiAP-S and FortiAP-W2 version 6.4.2, build 0437:

- Supported models on page 5
- What's new in FortiAP-S and FortiAP-W2 version 6.4.2 on page 5
- Upgrade and downgrade information on page 7
- Product integration and support on page 8
- Resolved issues on page 9
- Known issues on page 10

For more information about your FortiAP device, see the *FortiWiFi and FortiAP Configuration Guide*.

Supported models

FortiAP-S and FortiAP-W2 version 6.4.2, build 0437 support the following models:

FortiAP-S	FAP-S221E, FAP-S223E FAP-S421E, FAP-S422E, FAP-S423E
FortiAP-W2	FAP-221E, FAP-222E, FAP-223E, FAP-224E, FAP-231E FAP-321E FAP-421E, FAP-423E

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

What's new in FortiAP-S and FortiAP-W2 version 6.4.2

The following list includes new features in FortiAP-S and FortiAP-W2 version 6.4.2 managed by FortiGate (running FortiOS version 6.4.2):

- Automatic Radio Resource Provisioning (ARRP) Enhancement.
- Multiple pre-shared key (MPSK) Enhancement.
- Support Electronic Shelf Label (ESL) tags via USB dongle.

  Note: This requires FAP models equipped with a USB port. Currently, only FAP-S421E, FAP-S423E, FAP-421E, and FAP-423E can support this feature.
- Support per antenna/Rx Chain Statistics and fault alarm mechanism.
- Query new FortiGuard service to determine IoT device details.
- Enable DFS channels for FAP-224E with region A, and FAP-321E with region A, N, S and T.

- Add country Turkmenistan to region "I" and make country/region code up-to-date.
- Wi-Fi driver upgraded to Qualcomm Atheros SPF 6.1.

Upgrade and downgrade information

Upgrading to FortiAP-S and FortiAP-W2 version 6.4.2

FortiAP-S and FortiAP-W2 version 6.4.2 support upgrading from FortiAP-S and FortiAP-W2 version 6.2.3 and later.

Downgrading to previous firmware versions

FortiAP-S and FortiAP-W2 version 6.4.2 support downgrading to FortiAP-S and FortiAP-W2 version 6.2.3 and later.

Configurations made when FAP-231E is running a version later than 6.2.3 will not be saved if it is downgraded to 6.2.3.

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-S and 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-S and FortiAP-W2 version 6.4.2:

FortiOS	6.4.2 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-S and FortiAP-W2 version 6.4.2. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
634124	In case of local-standalone and external-portal SSID, RADIUS NAS-IP-Address attribute should be the FAP's IP address.
644080	Client authentication should be cleared after client is disconnected by RADIUS COA from the local-bridge captive-portal SSID.
652258	FAP static address mode lost DNS entry and couldn't resolve hostnames.

Known issues

The following issues have been identified in FortiAP-S and FortiAP-W2 version 6.4.2. 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.
651975	The USB port of FAP-S221E and FAP-S223E doesn't support Electronic Shelf Label (ESL).
655887	FAP-221E/223E gets low throughput on tunnel SSID when its wtp-profile has set dtls-policy ipsec-vpn.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.