

# FortiAP-S and FortiAP-W2 - Release Notes

Version 6.2.3

**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/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



Feb 13, 2020

FortiAP-S and FortiAP-W2 6.2.3 Release Notes

40-623-601221-20200213

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
Supported models .....	5
What's new in FortiAP-S and FortiAP-W2 version 6.2.3 .....	5
<b>Upgrade and downgrade information</b> .....	<b>7</b>
Upgrading to FortiAP-S and FortiAP-W2 version 6.2.3 .....	7
Downgrading to previous firmware versions .....	7
Firmware image checksums .....	7
Supported upgrade paths .....	7
<b>Product integration and support</b> .....	<b>8</b>
<b>Resolved issues</b> .....	<b>9</b>
Common vulnerabilities and exposures .....	9
<b>Known issues</b> .....	<b>10</b>

# Change log

Date	Change description
2019-12-23	Initial release.
2019-12-30	Added new supported FAP-321E model.
2020-02-13	Added a note about supporting FAP-231E model with a FortiOS 6.2.3 special branch in <a href="#">Product integration and support on page 8</a> .

# Introduction

This document provides the following information for FortiAP-S and FortiAP-W2 version 6.2.3, build 0277:

- [Supported models on page 5](#)
- [What's new in FortiAP-S and FortiAP-W2 version 6.2.3 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 6.2.3, build 0277 support the following models:

<b>FortiAP-S</b>	FAP-S221E, FAP-S223E FAP-S421E, FAP-S422E, FAP-S423E
<b>FortiAP-W2</b>	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 6.2.3

The following list includes new features in FortiAP-S and FortiAP-W2 version 6.2.3 managed by FortiGate (running FortiOS version 6.2.3):

- FortiAP can report port names as actual hardware labels to FortiGate for LLDP and FortiAP Health functions.
- FortiAP can report Radio Transmit Retry Percentage to FortiGate.
- FortiAP can report locally detected station OS information to FortiGate.
- Added RSSI threshold for rogue AP detection.
- Wi-Fi country and region code adjustments:
  - Changed Bahamas to region "A".
- FortiAP can support a new "style-3" of Circuit ID insertion in DHCP Option 82.

**Note:** FortiGate will support this setting in FortiOS 6.4.0.

- Supports the newly released FAP-231E model.
- Enables DFS channels on FAP-231E with region code E, I, V, Y, and D.
- Supports the newly released FAP-321E model.
- Enables DFS channels on FAP-321E with region code E, I, V, Y, and D.

# Upgrade and downgrade information

## Upgrading to FortiAP-S and FortiAP-W2 version 6.2.3

FortiAP-S and FortiAP-W2 version 6.2.3 support upgrading from FortiAP-S and FortiAP-W2 version 6.0.5, 6.0.6, and later.

## Downgrading to previous firmware versions

FortiAP-S and FortiAP-W2 version 6.2.3 support downgrading to FortiAP-S and FortiAP-W2 version 6.0.5, 6.0.6, and later.



- FAP-231E running version 6.2.3 firmware can only be downgraded to version 6.0.5 build 5528.
  - FAP-321E running version 6.2.3 firmware can only be downgraded to version 6.0.5 build 5523.
- 

## 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 6.2.3:

<b>FortiOS</b>	6.2.3 and later
<b>Web browsers</b>	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.



FAP-231E running on firmware 6.2.3 is compatible only with FortiGates running a special 6.2.3 FortiOS branch build. For instructions on downloading the special FortiOS build, see the [6.2.3 FortiOS Release Notes](#).



## Resolved issues

The following issues have been resolved in FortiAP-S and FortiAP-W2 version 6.2.3. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
519724	The Status LED on applicable FortiAP models remain amber even after the FortiAP is successfully managed by a FortiGate.
535670	The initial release of FAP-321E does not support the Bluetooth low energy (BLE) function.
576429	The username should be reported to FortiGate after the client passes the external authentication on bridge-mode captive-portal SSID.
588097	Wireless event logs "client-denial" and "client-deauthentication" should be created when a client is denied by MAC-based RADIUS authentication.
591381	WPA2-Enterprise SSID in standalone mode should support the "acct-all-servers" setting in RADIUS configuration.
592775	WiFi clients get disconnected within 30 minutes from a local-bridging SSID that has dynamic VLAN function enabled.

## Common vulnerabilities and exposures

FortiAP-S and FortiAP-W2 version 6.2.3 are no longer vulnerable to the following common vulnerabilities and exposures (CVE) references:

- CVE-2019-15709

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

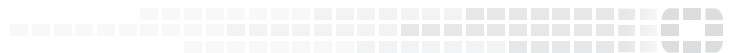
## Known issues

The following issues have been identified in FortiAP-S and FortiAP-W2 version 6.2.3. For inquiries about a particular bug or to report a bug, visit the [Fortinet Support](#) website.

Bug ID	Description
276655	The USB port on all FortiAP-S and FortiAP-W2 models is disabled.
374645	FortiAP-S and FortiAP-W2 models do not support the spectrum-analysis feature.
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.
573364	FAP-231E cannot support the Bluetooth low energy (BLE) function.



**FORTINET®**



Copyright© 2020 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.