FortiAP - Release Notes

Version 6.4.6

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

June 1, 2021
FortiAP 6.4.6 Release Notes
20-646-722103-20210601

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Supported models 5
What's new in FortiAP version 6.4.6 5
Special notices **6**
Upgrade and downgrade information **7**
Upgrading to FortiAP version 6.4.6 7
Downgrading to previous firmware versions 7
Firmware image checksums 7
Supported upgrade paths 7
Product integration support **8**
Resolved issues **9**
Common vulnerabilities and exposures 9
Known issues **10**

Change log

Date	Change description
2021-06-01	Initial release.

Introduction

This document provides the following information for FortiAP version 6.4.6, build 0178:

- Supported models on page 5
- What's new in FortiAP version 6.4.6 on page 5
- Special notices on page 6
- Upgrade and downgrade information on page 7
- Product integration 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 version 6.4.6, build 0178 supports the following models:

Models
FAP-231F, FAP-234F, FAP-23JF
FAP-431F, FAP-432F, FAP-433F
FAP-831F

What's new in FortiAP version 6.4.6

The following list includes FortiAP version 6.4.6 new features:

- Supports new model FAP-831F.
- 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.
- Supports "SKIP CAPWAP Offload" flag in CAPWAP header of certain packets as required by new FortiGate models with NP7 acceleration module.
- Supports DFS channels on FAP-231F with region code J.
- Supports DFS channels on FAP-234F with region code A
- Supports DFS channels on FAP-23JF with region code E, I, V, Y, and D.

Special notices

New Wi-Fi 6/802.11ax models FAP-431F, FAP-433F and FAP-231F initially supported in the FortiAP-W2 6.4.0 release have been moved to FortiAP 6.4.3 and later for continuing support.

Upgrade and downgrade information

Upgrading to FortiAP version 6.4.6

FortiAP 6.4.6 supports upgrading from FortiAP version 6.4.3 and later.

Downgrading to previous firmware versions

FortiAP 6.4.6 supports downgrading to FortiAP version 6.4.3 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_221C-v6-build0030-FORTINET.out.
5. Click **Get Checksum Code**.

Supported upgrade paths

To view all previous FortiAP versions, build numbers, and their supported upgrade paths, see the Fortinet Documentation website.

Product integration support

The following table lists product integration and support information for FortiAP version 6.4.6:

FortiOS	6.4.6 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 version 6.4.6. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
638494	802.11ax FAP models cannot support rogue AP suppression.
684825	Unable to establish MESH between two FortiAP units when DHCP relay is used on FortiGate.
694252	Wi-Fi client connected to FAP-431F stops passing traffic intermittently.
701896	After long idle time, WiFi clients cannot reconnect to FortiAP Cloud SSID with PMF enabled.
710922	FortiAP units cannot stay on the channels assigned by FortiGate DARRP function.
718756	FAP-231F 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 6.4.6 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) references:

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

Visit https://fortiguard.com for more information.

Known issues

There are no known issues in this release.

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.