



FortiAP-U - Release Notes

Version 6.0.0

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://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



Nov 7, 2019

FortiAP-U 6.0.0 Release Notes

42-600-591291-20191107

TABLE OF CONTENTS

| | |
|---|-----------|
| Change log | 4 |
| Introduction | 5 |
| Supported models | 5 |
| What's new in FortiAP-U version 6.0.0 | 5 |
| Special notice | 6 |
| Upgrade information | 7 |
| Upgrading from FortiAP-U version 5.4.6 | 7 |
| Upgrading FAP-U431F/433F trial version firmware | 7 |
| Downgrading to previous firmware version | 8 |
| Firmware image checksums | 8 |
| Product integration and support | 9 |
| Resolved issues | 10 |
| Common vulnerabilities and exposures | 10 |
| Known issues | 11 |

Change log

| Date | Change description |
|------------|---|
| 2019-10-31 | Initial release for FortiAP-U 6.0.0. |
| 2019-11-07 | Added a Special notice and instructions for Upgrading FAP-U431F/433F trial version firmware . |

Introduction

This document provides the following information for FortiAP-U version 6.0.0 build 0017:

- [Supported models](#)
- [What's new in FortiAP-U version 6.0.0](#)
- [Special notice](#)
- [Upgrade information](#)
- [Product integration and support](#)
- [Resolved issues](#)
- [Known issues](#)

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

Supported models

FortiAP-U version 6.0.0 supports the following models:

| Models |
|------------------------------------|
| FAP-U431F, FAP-U433F |
| FAP-U421EV, FAP-U422EV, FAP-U423EV |
| FAP-U321EV, FAP-U323EV |
| FAP-U24JEV |
| FAP-U221EV, FAP-U223EV |

What's new in FortiAP-U version 6.0.0

For FortiAP-U features managed by a FortiWLC, see the [Wireless Controller documentation](#).

The following is a list of new features and enhancements in FortiAP-U version 6.0.0, when managed by a FortiGate running FortiOS version 6.2.2 and later, or by FortiAP Cloud:

- Support for new "Wi-Fi 6" (IEEE 802.11ax standard) AP models: FAP-U431F and FAP-U433F
 - FAP-U431F and FAP-U433F profiles have two configurable platform modes:
 - "Dual 5GHz" mode: Configure 3 radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.
 - "Single 5GHz" mode: Configure 3 radios as one full 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.
 - High Efficiency (HE) configured per SSID
 - Target Wake Time (TWT) configured per SSID
- FAP-U421EV, FAP-U422EV, and FAP-U423EV support 160MHz channel bonding on the 5GHz 802.11ac band

(DFS certification required).

Note: FAP-U431F and FAP-U433F will support 160MHz channel bonding on the 5GHz 802.11ax/ac band after DFS certification.

- Wireless Intrusion Detection System (WIDS)
- Rogue station scan and rogue AP suppression
- Protected Management Frames (PMF) on mesh-backhaul SSID
- Bonjour gateway
- ACK Timeout adjustable by the max-distance setting in `wtp-profile`.
- FAP-U24JEV LAN ports bridged to tunnel-mode SSIDs support split-tunneling function for wired clients.
- FortiPresence v7.1 Push API update
 - Send AP Tx power as part of the FAP ID packets
- Up-to-date WiFi and country code adjustments.
- Dynamic frequency selection (DFS) certified stock keeping units (SKU):
 - FAP-U221EV-D, FAP-U223EV-D, FAP-U421EV-D, FAP-U422EV-D, FAP-U423EV-D
 - FAP-U422EV-N
 - FAP-U422EV-S

Special notice

FortiGates running FortiOS version 6.2.2 have the following limitations when managing FAP-U431F and FAP-U433F.

- FAP-U431F and FAP-U433F profiles, even if available, are not supported on the FortiGate web UI and can only be configured via the FortiGate CLI.

The FortiAP Profiles page in the FortiGate web UI does not fully support FAP-U431F and FAP-U433F profiles; not all configurations will work. For more information, see the Known issues section in the [FortiOS 6.2.2 Release Notes](#).

- Some radio channels might be unavailable in certain countries or regions, such as EU countries.

By default, FAP-U431F and FAP-U433F profiles have a "dual-5G" platform mode. This "dual-5G" platform mode sets the second radio of FAP-U431F and FAP-U433F devices to the upper 5GHz band including channels 100~144 and 149~165. However, those channels are not available in all countries or regions (e.g. EU countries) due wireless regulations and/or DFS certifications.

To work around this issue, edit the `wtp-profile` of your FAP-U431F or FAP-U433F devices, and set the platform mode to "single-5G" via the FortiGate CLI.

Upgrade information

Upgrading from FortiAP-U version 5.4.6

FortiAP-U version 6.0.0 supports upgrading from FortiAP-U version 5.4.6.

Upgrading FAP-U431F/433F trial version firmware

Some FAP-U431F and FAP-U433F devices come preinstalled with the trial version firmware "FortiAP-U431F v6.0,build0000" or "FortiAP-U433F v6.0,build0000". FortiAP-U devices running trial version firmware are not supported by FortiGate. To upgrade from the trial version firmware to the latest supported version, you must disable the third radio of your FAP-U431F and FAP-U433F devices.

To upgrade your FAP-U431F and FAP-U433F devices

1. Connect your FAP-U431F and FAP-U433F devices to a FortiGate running FortiOS version 6.2.2.
2. Log in to the FortiGate web UI and go to **WiFi & Switch Controller > Managed FortiAPs**.
3. Locate your discovered FAP-U431F and FAP-U433F devices and then authorize them.
4. Access the FortiGate CLI and edit the `wtp-profile` of your FAP-U431F or FAP-U433F devices to disable the third radio.

For example:

```
config wireless-controller wtp-profile
  edit FAPU431F-default
    config radio-3
      set mode disabled
    end
  end
```

5. Go to the [Fortinet Support](#) website to download the latest supported FortiAP-U firmware files to your local disk.
6. Go to **WiFi & Switch Controller > Managed FortiAPs** and select the FAP-U431F or FAP-U433F devices you want to upgrade.
7. Right-click and select **Upgrade** from the context menu.
The Upgrade FortiAPs window loads.
8. Click **Browse** and select the appropriate firmware file from your local disk, and click **Upgrade**.
The FAP-U431F or FAP-U433F devices upgrade to your selected firmware. When the upgrade is complete, the FortiAP status changes to "Online".
9. After the FortiAP-U firmware is upgraded, you can re-enable the third radio of your FAP-U431F or FAP-U433F devices.

Downgrading to previous firmware version

FortiAP-U version 6.0.0 supports downgrading to FortiAP-U version 5.4.6.

Firmware image checksums

To get the MD5 checksum code for a Fortinet firmware image, perform the following steps:

1. Go to the [Fortinet Customer Service and Support](#) website.
2. Log in to your account. If you do not have an account, create one and then login.
3. Select **Download > Firmware Image Checksums**.
4. Enter the image file name including the extension.
5. Click **Get Checksum Code**.

Product integration and support

The following table lists the product integration and support information for FortiAP-U version 6.0.0:

| Item | Supported versions |
|--------------|---|
| FortiOS | 6.0.6, 6.2.2 and later Note: FAP-U431F and FAP-U433F are only supported by FortiOS 6.2.2 and later. |
| FortiWLC-SD | 8.5.1 and later |
| Web browsers | <ul style="list-style-type: none">• Microsoft Edge 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 function correctly but Fortinet does not support them. |

Resolved issues

The following issues have been resolved in FortiAP-U version 6.0.0. For more details about a particular bug, visit the [Fortinet Customer Service & Support](#) website.

| Bug ID | Description |
|--------|---|
| 530701 | Slow downloading speed as traffic DSCP value is 48. |
| 552053 | Improved automatic channel selection (ACS). |
| 567180 | Fixed an issue where transmitting data to/from iPhone X or newer mobile devices became stuck. Note: On FortiGates, the wtp-profile should <code>set transmit-optimize</code> to default values. |
| 588099 | Dynamic frequency selection (DFS) channels could not be assigned when running ACS or distributed automatic radio resource provisioning (DARRP). |

Common vulnerabilities and exposures

FortiAP-U 6.0.0 is no longer vulnerable to the following CVE-References:

- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479
- CVE-2019-15708

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

Known issues

The following table lists capabilities that are not supported by FortiAP-U 6.0.0 when managed by a FortiGate or FortiCloud:

| Bug ID | Description |
|--------|---|
| 547865 | FAP-U431F and U433F cannot support Bluetooth Low Energy (BLE) function. |
| 564316 | Receiver Start of Packet Detection Threshold (RX-SOP). |
| 566884 | QoS profile (traffic shaper, WMM call admission control, override DSCP mapping for WMM clients). |
| 586196 | Detailed wireless event logs for trouble shooting. |
| 587765 | Airtime Fairness. |
| 587776 | VLAN Probe tool. |
| 587779 | Extension information for statistics of AP, SSID and station. |
| 587802 | WPA3 security modes. |
| 588019 | Unified schedules for DARRP, background scan, SSID up/down state, LED on/off state, and multiple pre-shared key (MPSK). |
| 588023 | External captive portal on local-bridging SSID. |
| 588034 | MAC address filter on local-standalone SSID. |



In general, features not explicitly mentioned in [What's new in FortiAP-U version 6.0.0](#) and previous versions, are not supported.



FORTINET®



Copyright© 2019 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.