FortiAP-U - Release Notes

Version 6.0.3

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

Sep 17, 2020
FortiAP-U 6.0.3 Release Notes
42-603-644474-20200917

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Supported models 5
What's new in FortiAP-U version 6.0.3 5
Upgrade information **7**
Upgrading from FortiAP-U version 6.0.2 7
Downgrading to previous firmware version 7
Firmware image checksums 7
Product integration and support **8**
Resolved issues **9**
Common vulnerabilities and exposures 9
Known issues **10**

Change log

Date	Change description
2020-07-09	Initial release for FortiAP-U 6.0.3.
2020-09-17	Added the Bug ID associated the resolved CVE.

Introduction

This document provides the following information for FortiAP-U version 6.0.3 build 0062:

- Supported models
- What's new in FortiAP-U version 6.0.3
- 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 6.0.3 supports the following models:

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

What's new in FortiAP-U version 6.0.3

For FortiAP-U features managed by a FortiWLC, see the Wireless Controller documentation.

FortiAP-U version 6.0.3 supports the following new features, when managed by a FortiGate running FortiOS version 6.2.4 and later, or by FortiAP Cloud:

- WPA3 security modes.
- Enforce admin password upon initial login.
- Report WiFi clients' real noise-floor value to FortiGate.
- MU-MIMO control per SSID (enabled by default).
- Schedules of multiple pre-shared key (MPSK).
- External captive-portal SSID and RADIUS CoA support in Bridge mode and Local-Standalone mode.
- DHCP snooping and option 82 insertion.
- Security-exempt list support on captive-portal SSID.
- Receiver Start of Packet Detection Threshold (RX-SOP).
- Report FortiAP uplink status and interface transmitting and receiving counters to FortiGate.

- Client OS detection via DHCP fingerprint and report to FortiGate.
- Report scanned Bluetooth devices to FortiPresence.
- Extended wireless event logs for WiFi station health.
- Wireless Quality-of-Service (QoS) profile.
- MAC address filter on Local-Standalone SSID.
- Report FAP-U admin login and logout activities to FortiGate system event logs.
- Management frame (authentication request and association request) flood detection in WIDS profile.
- Added TLS v1.2 cipher suites.
- Enable DFS channels on FAP-U431F and FAP-U433F with region T, and J.
- DHCP option 43 insertion through local-bridging SSID (FortiGate needs FortiOS 6.4.1 or later).
- 802.11ax BSS Coloring on FAP-U431F and FAP-U433F (FortiGate needs FortiOS 6.4.2 or later).
- New Spectrum Analysis on FAP-U431F and FAP-U433F (FortiGate needs FortiOS 6.4.2 or later).

  Note: The 3rd radio of FAP-U431F and FAP-U433F doesn't support Spectrum Analysis. Before implementing Spectrum Analysis on FortiGate side, the 3rd radio of FAP-U431F and FAP-U433F should be disabled.

Upgrade information

Upgrading from FortiAP-U version 6.0.2

FortiAP-U version 6.0.3 supports upgrading from FortiAP-U version 6.0.2.

Downgrading to previous firmware version

FortiAP-U version 6.0.3 supports downgrading to FortiAP-U version 6.0.2.

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 6.0.3:

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	• 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.

We recommend that customers use a FortiOS version listed in the support table. Other variations of FortiOS and FortiAP-U versions may technically work, but are not guaranteed full functionality. If problems arise, Fortinet Support will ask that you use the recommended version before troubleshooting.

Resolved issues

The following issues have been resolved in FortiAP-U version 6.0.3. For more details about a particular bug, visit the Fortinet Customer Service & Support website.

Bug ID	Description
590303	FortiAP Cloud captive-portal SSID on FAP-U431F and FAP-U433F cannot authenticate WiFi clients.
603422	Fixed a kernel panic issue (`soc_watchdog+0x208/0x22c`) on FAP-U24JEV.
605492	Wired device cannot get DHCP IP address from LAN1/PSE port of FAP-U24JEV.
607962	Fixed a kernel panic issue (`PC is at wlc_scbfindband`).
612420	FAP-U should not send IGMP query periodically (every 125 seconds).
622965	AeroScout D5 messages (AP tag report) contained wrong data payload.
631641	FAP-U431F leaked multicast packets to LAN2 port on LACP mode.
633200	FAP-U421EV and U321EV encountered a kernel panic (`PC is at __bug+0x1c/0x28`).
636576	WiFi client could not re-associate to a second FortiAP when roaming over SSID with fast BSS transition (802.11r) enabled.
638956	FAP-U422EV link aggregation lost connection after its "LAN2 PSE" port was unplugged.

Common vulnerabilities and exposures

FortiAP-U 6.0.3 is no longer vulnerable to the following CVE-References:

CVE ID	Bug ID
CVE-2019-15126	0614793

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

Known issues

The following table lists capabilities that are not supported by FortiAP-U 6.0.3 when managed by a FortiGate or FortiCloud:

Bug ID	Description
587765	Airtime Fairness.
587776	VLAN Probe tool.
587779	Extension information for statistics of AP, SSID, and station.
588019	Unified schedules for DARRP, background scan, SSID up/down state, LED on/off state, and multiple pre-shared key (MPSK).
616096	FAP-U cannot support OWE-Transition security mode and the 192-bit encryption option in WPA3-Enterprise security mode.

In general, features not explicitly mentioned in What's new in FortiAP-U version 6.0.3 and previous versions, are not supported.