



FortiAP-U - Release Notes

Version 6.2.2

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/training-certification>

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



Dec 17, 2021

FortiAP-U 6.2.2 Release Notes

42-622-735646-20211217

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
New features or enhancements	6
Region/country code update and DFS certification	6
Changes in CLI	7
Special notice	8
Upgrade and downgrade information	9
Upgrading to FortiAP-U version 6.2.2	9
Downgrading to previous firmware version	9
Firmware image checksums	9
Product integration and support	10
Resolved issues	11
Common vulnerabilities and exposures	11
Known issues	12

Change log

Date	Change description
2021-08-12	Initial release for FortiAP-U 6.2.2.
2021-10-08	Updated Special notice on page 8 .
2021-12-17	Added FortiAP-U234F and FortiAP-U432F as supported models. Updated Product integration and support on page 10 .

Introduction

This document provides release information for FortiAP-U version 6.2.2 build 0267.

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

Supported models

FortiAP-U version 6.2.2 supports the following models:

Wi-Fi standard	Models
802.11ac	FortiAP-U221EV, FortiAP-U223EV, FortiAP-U24JEV, FortiAP-U321EV, FortiAP-U323EV, FortiAP-U421EV, FortiAP-U422EV, FortiAP-U423EV
802.11ax	FortiAP-U231F, FortiAP-U234F FortiAP-U431F, FortiAP-U432F, FortiAP-U433F

New features or enhancements

The following table includes new features and enhancements in FortiAP-U version 6.2.2 when managed by a FortiGate running FortiOS version 6.2.4 and later, or by FortiLAN Cloud:

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

Bug ID	Description
587765, 715013	Enables Airtime Fairness (ATF) by default and accepts the configuration from FortiGate.
588031	Supports RADIUS-based MAC address authentication on local-standalone SSID.
640758	Supports configuration rollback after a new configuration causes a disconnection from the WiFi controller.
658501	Supports Agile multiband (MBO) setting from FortiGate running FortiOS 7.0.0 and later.
666741	Supports FAP signing for device registration, which is applicable to FortiGate running FortiOS 6.4.3 and later. From the FortiGate web UI go to WiFi & Switch Controller > Managed FortiAPs , admins can register the authorized FortiAP-U units to FortiCloud directly.
699308	Supports the URL redirection method for client devices after logging into an external Captive-Portal SSID.
705116	Supports new models FortiAP-U234F and FortiAP-U432F.
711545	Supports "SKIP CAPWAP Offload" flag in the CAPWAP header of certain packets as required by new FortiGate models with NP7 acceleration module.
713805	<p>802.11ax FortiAP-U models support UTM security profiles on bridge-mode SSIDs.</p> <p>Note: FortiGate needs to run FortiOS 7.0.1 and later.</p> <p>The UTM feature is disabled by default to save FAP-U resources. To enable UTM, run following commands on the FAP-U CLI:</p> <pre> cfg -a FAP_UTM_FEATURE=1 cfg -c </pre> <p>The FAP-U unit will then reboot itself to activate UTM functions.</p>

Region/country code update and DFS certification

Bug ID	Description
667008	<p>Enable DFS channels on FAP-U231F with region code E, I, V, Y, and D.</p> <p>Note: FortiGate needs to run FortiOS 6.4.6, 7.0.1, and later.</p>
730135	Change the region code of Qatar from I to E.

Changes in CLI

Bug ID	Description
670587	A new command "fap-tech" is added to collect all basic debug information from the customer side.
696698	"ALLOW_TELNET" is removed as a configurable variable from the "cfg" command.
716544	A new variable "FAP_UTM_FEATURE" is added to the "cfg" command to enable or disable the UTM feature.
727463	For site-survey mode SSID, allow setting different transmit power levels for 2.4 and 5 GHz respectively. The previous "SURVEY_TX_POWER" has been replaced with "SURVEY_TX_POWER_24" and "SURVEY_TX_POWER_50".

Special notice

FAP-U431F and FAP-U433F firmware version 6.2.2 requires a mandatory change in data partitions, so they can NOT be directly upgraded from 6.2.1 to 6.2.2



FAP-U431F and FAP-U433F running firmware version 6.2.2 can no longer be managed by FortiWLC. A factory reset will reset FAP-U431F and FAP-U433F to the default configuration for FortiGate and FortiLAN Cloud management only.

Administrators who use FortiGate or FortiLAN Cloud to manage FAP-U431F and/or FAP-U433F units must upgrade them carefully using the following steps:

1. Ensure your FAP-U431F and FAP-U433F units are running FAP-U 6.2.1 GA build 0237.
2. Upgrade them to the special transit images `FAP_U431F-v6-build4001-FORTINET.out` and `FAP_U433F-v6-build4001-FORTINET.out` respectively, which are available from the support site.
3. On FAP-U431F and FAP-U433F units running the special build 4001, continue to upgrade them to FAP-U 6.2.2 GA build 0267.



You may receive a downgrade note on the FortiOS GUI when upgrading from build 4001 to build 0267. This is due to the 0267 build number being read as a lower version number than build 4001. The process is not a downgrade and the note can be ignored.

Upgrade and downgrade information

Upgrading to FortiAP-U version 6.2.2

FortiAP-U version 6.2.2 supports upgrading from FortiAP-U version 6.2.1.



FAP-U431F and FAP-U433F cannot be upgraded directly from 6.2.1 to 6.2.2. See [Special notice on page 8](#) for more information.

Downgrading to previous firmware version

FortiAP-U version 6.2.2 supports downgrading to FortiAP-U version 6.2.1.

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 log in.
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 6.2.2:

Item	Supported versions
FortiOS	6.0.6, 6.2.2, 6.4.3, 7.0.0 and later. Note: <ul style="list-style-type: none">FAP-U431F and FAP-U433F are only supported by FortiOS 6.2.2 and later.FAP-U231F is only supported by FortiOS 6.4.3 and later.FAP-U234F and FAP-U432F are only supported by FortiOS 6.4.4 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.
AV Engine	6.4.251
IPS Engine	6.2.64



FortiGate WiFi Controller should use a FortiOS version listed in the preceding table. Other variations of FortiOS and FortiAP-U versions may technically work, but are not guaranteed full functionality. If problems arise, the FortiGate device may need to be upgraded to the latest FortiOS GA version.

Resolved issues

The following issues have been resolved in FortiAP-U version 6.2.2. For more details about a particular bug, visit the [Fortinet Customer Service & Support](#) website.

Bug ID	Description
616096, 666613	Implement WPA3-Enterprise 192-bit encryption (using AES-GCM-256), WPA3-Enterprise only and WPA3-Enterprise Transition.
649153	FAP-U incorrectly reported interfering AP with RSSI of -12dBm.
659638	When FAP-U24JEV LAN port is configured as "bridge-to-ssid", multicast traffic over the LAN port was getting dropped.
662313	When WAN-LAN mode is enabled and the LAN port is bridged to a local-standalone SSID with NAT enabled, the NAT configuration could not work.
665798	When background scan is enabled, clients could experience ping loss when AP executes scan.
684349	FAPs were not failing over between primary and secondary FGTs when inter-controller-mode is in "1+1" fast failover mode.
707932	Low TCP throughput was observed for mesh link on 5GHz radio of FAP-U422E.
708745	Fixed an issue that some wireless clients were disconnected at midnight due to daily automatic channel selection (ACS) scanning.
723584	Supports a new Bluetooth low energy (BLE) chipset in FAP-U231F.
727279	FAP-U units got disconnected from FortiLAN Cloud with the reason "received unexpected discovery".

Common vulnerabilities and exposures

FortiAP-U 6.2.2 is no longer vulnerable to the following CVE-References:

Bug ID	CVE References
719019	<div>FRAG attack<ul style="list-style-type: none">• CVE-2020-24586• CVE-2020-24587• CVE-2020-24588</div>

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

Known issues

The following capabilities are not supported by FortiAP-U 6.2.2 when managed by a FortiGate or FortiLAN Cloud:

Bug ID	Description
587771	Config mode support via Reset button.
587774	FAP-U direct REST API support.
587779	Extension information for statistics of AP, SSID, and station.
587804	Hotspot 2.0 Feature Support.
588016	Support for L2TP & GRE Tunnels on local-bridging SSID.
615311	Band Steering Support on Standalone VAP.
640771	Layer-3 Firewall (wireless access control list).
644209	DARRP Improvements II (arp-profile from FGT).
663672	Support ESL USB Dongle (Hanshow) on 802.11ax Series.
731733	FAP-U Auto VLAN Name assignment from RADIUS attribute.
739303	Support Electronic Shelf Label Products (SES-Imagotag).
739305	Client should be able to log out after authenticated with bridge external captive-portal SSID.
739307	Support for Service Assurance Manager (SAM) mode.
739309	Supports "hitless" failover in FortiGate HA cluster.
739312	Reports AP operating temperature to FortiGate WiFi Controller.
739313	Local-standalone NAT-mode SSID can configure optional DNS servers to assign out to wireless clients through DHCP.
739314	Support for location-based services (LBS) station info via PUSH API.



In general, features not explicitly mentioned in [New features or enhancements](#) and previous versions, are not supported.



FORTINET



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.