



Release Notes

FortiAP-U 7.0.5



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



Jan 16, 2025

FortiAP-U 7.0.5 Release Notes

42-705-1113156-20250116

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
New features or enhancements	6
Special notice	7
Upgrade and downgrade information	8
Upgrading to FortiAP-U version 7.0.5	8
Downgrading to previous firmware version	8
Firmware image checksums	8
Product integration and support	9
Resolved issues	10
Known issues	11

Change log

Date	Change description
2025-01-16	Initial release for FortiAP-U 7.0.5.

Introduction

This document provides release information for FortiAP-U version 7.0.5 build 0146.

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

Supported models

FortiAP-U version 7.0.5 supports the following models:

Wi-Fi 5 models

FortiAP-U221EV, FortiAP-U223EV, FortiAP-U24JEV,
FortiAP-U321EV, FortiAP-U323EV,
FortiAP-U421EV, FortiAP-U422EV, FortiAP-U423EV

Wi-Fi 6 models

FortiAP-U231F, FortiAP-U234F,
FortiAP-U431F, FortiAP-U432F, FortiAP-U433F

New features or enhancements

FortiAP-U version 7.0.5 contains stability improvements and bug fixes when managed by a FortiGate, or by FortiLAN Cloud.

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

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 or later versions. If your FAP-U431F and FAP-U433F units are currently running firmware version 6.2.1 or earlier and are managed by a FortiGate or FortiLAN Cloud, follow the instructions below to upgrade them.



FAP-U431F and FAP-U433F running firmware version 6.2.2 and later 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.

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 in the FortiAP-U 6.2.2 image folder on the support site.
3. On FAP-U431F and FAP-U433F units running the special build 4001, continue to upgrade them to firmware version 7.0.5.

Upgrade and downgrade information

Upgrading to FortiAP-U version 7.0.5

FortiAP-U version 7.0.5 supports upgrading from FortiAP-U version 6.2.2 and later.

Downgrading to previous firmware version

FortiAP-U version 7.0.5 supports downgrading to FortiAP-U version 6.2.2 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.
5. Click **Get Checksum Code**.

Product integration and support

The following table lists the product integration and support information for FortiAP-U version 7.0.5:

Item	Supported versions
FortiWLC-SD	8.5.1 and later.
FortiOS	6.0.6, 6.2.2, 6.4.3, 7.0.0, 7.2.0 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.
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	6.00276 and later.
IPS Engine	7.00512 and later.



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 7.0.5. For more details about a particular bug, visit the [Fortinet Customer Service & Support](#) website.

Bug ID	Description
1008829	FAP-U24JE would encounter a watchdog crash if the CPU usage was high.
1048833	FortiAP-U made false positive "radar-detected" reports against DFS channels.
1054731	Wireless devices couldn't get an IP address when connected to a Multiple-PSK SSID using RADIUS-MAC authentication.
1056441, 1087980	Fixed multiple wireless connectivity and packet loss issues.
1073902	FortiAP-U couldn't record the source IP for failed admin login attempts on the web UI.

Known issues

There is no outstanding issue known at present in this release.



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



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.