Release Notes

FortiAP 7.0.4

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

FORTINET®

Mar 21, 2023
FortiAP 7.0.4 Release Notes
20-704-818180-20230321

TABLE OF CONTENTS

Change log 4

Introduction 5

Supported models 5

New features or enhancements 6

Region/country code update and DFS certification 6

Upgrade and downgrade information 7

Upgrading to FortiAP version 7.0.4 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
2022-06-21	Initial release.
2023-03-21	Added Common vulnerabilities and exposures to Resolved issues on page 9.

Introduction

This document provides release information for FortiAP version 7.0.4, build 0082.

For more information about your FortiAP device, see the *FortiWiFi and FortiAP Configuration Guide*.

Supported models

FortiAP version 7.0.4, build 0082 supports the following models:

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

New features or enhancements

The following table includes FortiAP version 7.0.4 new features and enhancements:

Bug ID	Description
746500	Optimize Broadcast and Multicast Suppression on the FortiAP side.

Region/country code update and DFS certification

Bug ID	Description
730032	The region code of Qatar is changed from "I" to "E".
775246	Supports DFS channels on FAP-831F with region code "N" (Brazil).
789308	Supports DFS channels on FAP-234F with region code "K" (Korea).

Upgrade and downgrade information

Upgrading to FortiAP version 7.0.4

FortiAP 7.0.4 supports upgrading from FortiAP version 6.4.5 and later.

Downgrading to previous firmware versions

FortiAP 7.0.4 supports downgrading to FortiAP version 6.4.5 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 7.0.4:

FortiOS	7.0.6 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 7.0.4. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
606388	Sometimes, FortiGate would report SSIDs from authorized FortiAP devices as "`fake-ap-on-air`".
651452	The console port of FAP-231F, 234F and 23JF would occasionally lock-up.
711919	Probe requests and responses were not logged by 802.11ax-capable FortiAP models.
724927	FortiAP would take a long time to connect back to the WiFi Controller after implementing `reboot` from the FortiAP CLI.
767941	802.11ax clients got low throughput when connected to an SSID with PMF set to optional.
778554	REST-API support: Expose max interface speed of all Ethernet ports on FortiAP.
779712	FortiAP would stop responding SNMP queries sometimes.
786273	Add Station RSSI and SNR inside Probe logs. **Note:** FortiGate needs to run FOS 7.2.0 or later.
787499	Wireless clients were unable to complete authentication on the captive portal page.
790245	Sometimes, FortiAP could not reconnect to FortiLAN Cloud and received error message: "`Too many DTLS setup failures 5. Restart wtp daemon`".
790913	Add server IP/Name information to RADIUS, DNS and DHCP wireless event logs. **Note:** FortiGate needs to run FOS 7.2.0 or later.
791692	When FAP-23JF is managed by FortiLAN Cloud, the LAN ports aren't actually down after configured to be offline.

Common vulnerabilities and exposures

FortiAP 7.0.4 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) references:

Bug ID	Description
786638	CVE-2022-29058 (Command injection in CLI).

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

Known issues

The following issues have been identified in FortiAP version 7.0.4. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
692160	Wireless packets captured by FortiAP radio in Sniffer mode are corrupted.
761298	FAP-234F Bluetooth Low Energy (BLE) function cannot work.
767916	When wireless clients are connected to different radios of the same tunnel-mode SSID with static or dynamic VLAN, they cannot ping each other.
795661	Wireless clients cannot communicate with wired clients behind a switch connected to a mesh-Ethernet bridge.

FORTINET®

www.fortinet.com