Release Notes

FortiAP 7.2.1

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

Mar 21, 2023
FortiAP 7.2.1 Release Notes
20-721-832873-20230321

TABLE OF CONTENTS

Change log

Date	Change description
2022-08-11	Initial release.
2022-11-15	Updated Supported models on page 5, New features or enhancements on page 6, and Product integration support on page 9
2023-03-21	Added Common vulnerabilities and exposures to Resolved issues on page 10.

Introduction

This document provides release information for FortiAP version 7.2.1, build 0295.

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

Supported models

FortiAP version 7.2.1, build 0295 supports the following models:

Wi-Fi 6 Models
FAP-231F, FAP-234F, FAP-23JF, FAP-431F, FAP-432F, FAP-433F, FAP-831F

Wi-Fi 6E Models
FAP-231G (build 4789), FAP-233G (build 4789), FAP-431G (build 4789), FAP-433G (build 4789)

New features or enhancements

The following table includes FortiAP version 7.2.1 new features and enhancements:

Bug ID	Description
802708	Re-design 802.11ac and 802.11ax MCS rate control.
802838	FortiAP support to enable/disable 802.11d.
811132	WPA3 Enhancement (Wi-Fi 6 Rel 2); Support WPA3-SAE Public Key (PK) and Hash-to-Element (H2E) only.
812264	Layer-3 roaming over bridge-mode SSID across FortiAP networks.
815472	DSCP marking based on client's application attribute as determined by NDPI engine (for bridge-mode SSID).
843939	Support for new models FAP-231G, FAP-233G, FAP-431G and FAP-433G, released with special build 4789 based on FortiAP 7.2.1. **Note:** The new models can be managed by FortiGate running FortiOS 7.0.8, 7.2.1 and later.

Region/country code update and DFS certification

Bug ID	Description
816718, 816719, 816995	Supports DFS channels on FAP-431F, FAP-231F and FAP-432F with region code "C".
817725	Supports DFS channels on FAP-831F with region code "J".
823674	The region code of Jordan is changed from "I" to "E".
823679	Mongolia (MN) is added in region code "I".

Changes in CLI

Bug ID	Description
815472, 822042	In order to utilize the NDPI-based DSCP marking feature, you must first enable "`application-dscp-marking`" under the FortiGate VAP configuration. Then, from the FortiAP CLI, implement the following command to map application attribute(s) to DSCP value(s), one by one: `cw_diag -c ndpi-dscp [attribute name or no.] [dscp value] [direction]`

Bug ID	Description
	Note: The direction can be both (as default), uplink or downlink.

Upgrade and downgrade information

Upgrading to FortiAP version 7.2.1

FortiAP 7.2.1 supports upgrading from FortiAP version 7.0.3 and later.

Downgrading to previous firmware versions

FortiAP 7.2.1 supports downgrading to FortiAP version 7.0.3 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 7.2.1:

FortiOS	FortiOS 7.2.1 and later. **Note:** FortiOS 7.0.8, 7.2.1 and later for FAP-231G, FAP-233G, FAP-431G and FAP-433G management.
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 7.2.1. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
790245	Sometimes, FortiAP could not reconnect to FortiLAN Cloud and received error message: "`Too many DTLS setup failures 5. Restart wtp daemon`".
796778	FortiAP should be able to clear RADIUS-based MPSK cache per MAC address and shorten the cache timeout (300 ~ 864000 sec, 0 to disable caching).
797019	FortiAP should generate DNS process success logs for wireless stations. **Note:** FortiGate won't generate such logs due to the high volume.
798677	A notice-level wireless event log should be generated when Probe Request is dropped due to low RSSI.
801972	Wireless event logs should be generated when wireless clients get deauthenticated or disassociated.
817235	FAP-431F would randomly change DFS channel to 0 after detecting a radar signal.
820997	FortiAP units were sending an excessive amount of CPU and memory statistics to FortiLANCloud.
821831	PoE Mode Configured value and Operating value were shown inconsistently on FortiAP GUI.

Common vulnerabilities and exposures

FortiAP 7.2.1 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 7.2.1. 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 mesh-Ethernet bridge.

FORTINET®

www.fortinet.com