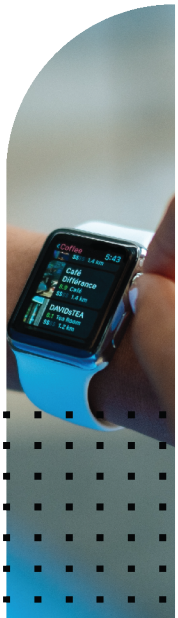
Release Notes

FortiAP 7.0.2



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

Nov 4, 2021
FortiAP 7.0.2 Release Notes
20-702-756155-20211104

TABLE OF CONTENTS

Change log

Date	Change description
2021-11-04	Initial release.

Introduction

This document provides release information for FortiAP version 7.0.2, build 0056.

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

Supported models

FortiAP version 7.0.2, build 0056 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 7.0.2 new features and enhancements:

Bug ID	Description
670724	FortiAP accepts hexadecimal values of EddyStone namespace ID and instance ID in Bluetooth low energy (BLE) profile.
701339	FortiAP admin password supports up to 128 characters for local `LOGIN_PASSWD` variable and `wtp/wtp-profile login-passwd` configured from WiFi Controller.
702766	FortiAP supports the Release 3 of Hotspot 2.0.
713612	FortiPresence PUSH API update: FortiAP sends its region map information to FortiPresence server for positioning wireless stations.
718009	FortiAP can send log messages to a Syslog server.
731714	FortiAP can advertise its name, model, and/or serial number in the vendor specific element of beacon frames.
733596	When RADIUS-based MAC authentication is enabled, FortiAP can implement multiple pre-shared key (MPSK) authentication by checking passphrase together with MAC address of each client.
735630	FortiAP admin password requires a minimum of 5 characters and no longer allows blank password.
735632	From WiFi Controller `wtp-profile` configuration, FortiAP WAN port can be set as an 802.1X supplicant to authenticate to local infrastructure network using EAP protocols.
736558	FortiAP reports more information (SGI, bandwidth, max rate, PHY mode) of rogue APs to the FortiGate WiFi controller.
746045	FortiAP supports FQDN address mode of FortiPresence server configured from WiFi Controller.

Region/country code update and DFS certification

Bug ID	Description
730739, 750252	Supports DFS channels on FAP-231F with region code N (including Brazil) and S.
735175, 744412, 750252	Supports DFS channels on FAP-234F with region code J, N (including Brazil) and T.
733996, 735187, 751657	Supports DFS channels on FAP-23JF for region and A, J, N (including Brazil), S and T.

Bug ID	Description
730759, 751585	Supports DFS channels on FAP-431F and FAP-433F with region code N (including Brazil) and S.
735187, 744395	Supports DFS channels on FAP-432F with region code N (including Brazil) and T.
720805, 748136, 749849	Supports DFS channels on FAP-831F with region code A, D, E, I, N (except Brazil), S, T, V and Y.

Changes in CLI

Bug ID	Description
577504	A stronger encryption has been adopted to better protect all password inputs, including `LOGIN_PASSWD`, `AC_DISCOVERY_FCLD_PASSWD`, `MESH_AP_PASSWD` and `WAN_1X_PASSWD`.

721033	The `restore` command has new options added for server type, `tftp` or `ftp`:
	• `tftp`: to download FAP firmware from a TFTP server.
	• `ftp`: to download FAP firmware from an FTP server.
	If not explicitly set, it defaults to `tftp`, the same behavior as before.
	`restore [tftp] <FAP firmware name> <TFTP server IP>`
	`restore ftp <FAP firmware name> <FTP server IP> <username> <password>`

735632	When WiFi Controller won't overwrite FAP WAN port authentication, FAP can configure its own 802.1X supplicant locally.
	New cfg variables:
	`WAN_1X_ENABLE` WAN port 802.1x supplicant enable/disable [0(Disabled), 1(Enabled)]. default=0
	`WAN_1X_USERID` WAN port 802.1x supplicant user ID
	`WAN_1X_PASSWD` WAN port 802.1x supplicant password
	`WAN_1X_METHOD` WAN port 802.1x supplicant EAP methods [0(EAP-ALL), 1(EAP-FAST), 2(EAP-TLS), 3(EAP-PEAP)]. default=0
	Diagnose command:
	`cw_diag -c wan1x`
	`cw_diag -c wan1x [show-ca-cert|show-client-cert|del-all|del-ca-cert|del-client-cert|del-private-key|[<get-ca-cert|get-client-cert|get-private-key> <TFTP server IP> <file name>]]`

750308	A new command is added for FortiAP to upload Target Assert logs to a specified TFTP server. `cw_diag wlanfw-dump <TFTP server IP>`

Upgrade and downgrade information

Upgrading to FortiAP version 7.0.2

FortiAP 7.0.2 supports upgrading from FortiAP version 6.4.5 and later.

Downgrading to previous firmware versions

FortiAP 7.0.2 supports downgrading to FortiAP version 6.4.5 and later.

Any password effective with firmware 7.0.2 (refer to Bug ID 577504) will NO LONGER work after downgrade. You can configure the FortiAP admin password from the WiFi Controller for managed FortiAP units; or you can press and hold the RESET button on the FortiAP for 10 seconds to factory reset. Then, log in to the FortiAP to configure other password variables when necessary.

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 7.0.2:

FortiOS	7.0.2 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 7.0.2. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
421233	FortiAP failed to disable wireless multimedia (WMM) setting in QoS profile.
716641	On local-standalone SSID, RADIUS authentication request was not sent to secondary RADIUS server when first one was unreachable.
731369	Draeger M300 devices in Power Save mode would disconnect from FortiAP after a few hours.
733260	Draeger Delta devices suffered from multicast packets loss for a long period of time.
737343	FortiAP with location-based service enabled was reporting a specific client as both station and rogue AP.
738596	FortiAP SSH server limited the credentialed scan performed with Nessus Scanner.
743241	FortiAP mesh link dropped while using Cisco Webex/Telepresence devices.
746769	Fixed a Target Assert issue: `ar_wal_peer.c:4578 Assertion 0 failedparam0 :zero, param1 :zero, param2 :zero.`
754775	FortiAP might send corrupted IPv6 client information to FortiGate when reconnected.

Common vulnerabilities and exposures

FortiAP 7.0.2 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) references:

Bug ID	Description
719016	FRAG attack: • CVE-2020-24586 • CVE-2020-24587 • CVE-2020-24588

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

Known issues

The following issues have been identified in FortiAP version 7.0.2. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
645121	FortiAP should report detected station information from radio1 and radio2 when FortiPresence is enabled.

www.fortinet.com