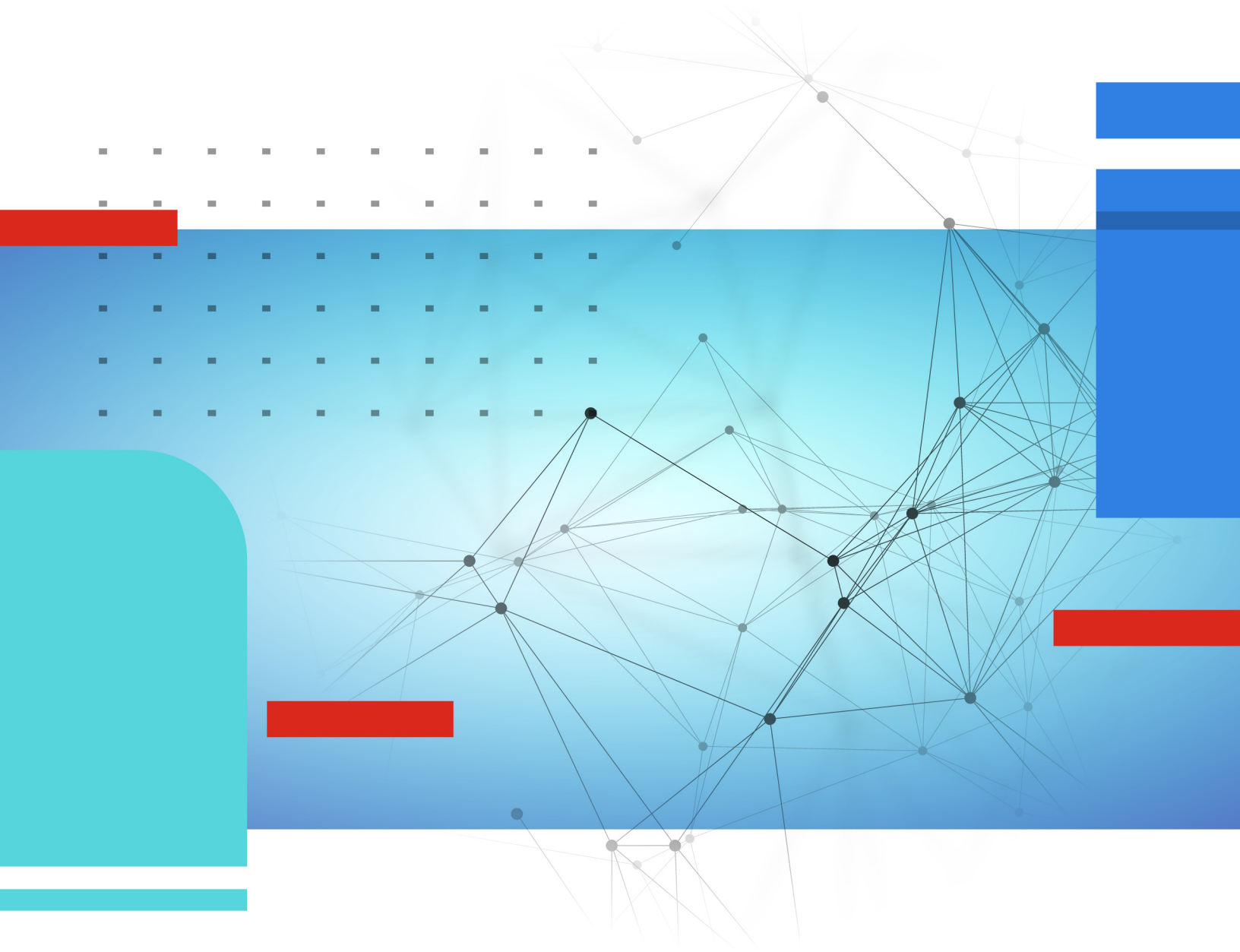
Release Notes

FortiAP 7.4.3



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

Jun 4, 2024
FortiAP 7.4.3 Release Notes
20-743-1034973-20240604

TABLE OF CONTENTS

Change log

Date	Change description
2024-06-04	Initial release.

Introduction

This document provides release information for FortiAP version 7.4.3, build 0680.

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

Supported models

FortiAP version 7.4.3, build 0680 supports the following models:

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

Wi-Fi 6E Models
FAP-231G, FAP-233G, FAP-234G, FAP-431G, FAP-432G, FAP-433G

New features or enhancements

The following table includes FortiAP version 7.4.3 new features and enhancements:

Bug ID	Description
951641	FortiAP Wi-Fi 6E models can support Media Access Control Security (MACsec) in the WAN-port 802.1X authentication. **Note:** FortiAP can work with the `confidentiality-offset` value `0` or `30`.
951643	FortiAP Wi-Fi 6E models can support Lightweight UTM functions such as Application Control and Website/URL filter.
999314	You can enable or disable the USB port on FortiAP through FortiOS when the input power mode is "full".
1001339	Support User MPSK management via FortiGuest or FortiAuthenticator.
1013337	Support the RADIUS NAS-Filter-Rule attribute in wireless 802.1X authentication and create dynamic Access Control Lists (dACLs) for Wi-Fi stations.
1017633	Remove the 250 Mbps upper limit for encrypted CAPWAP-data traffic (when `wtp-profile` > `dtls-policy` is set to `dtls-enabled`, `ipsec-vpn`, or `ipsec-sn-vpn`).
1033486	Improve the Service Assurance Manager (SAM) ping test result to include latency info.

Region/country code update and DFS certification

Bug ID	Description
970429	The region code of the following countries has changed from "N" to "A": Barbados, Belize, Colombia, Dominican Republic, Grenada, Guyana, Honduras, Micronesia, and Panama.
982021	Enable DFS channels for FAP-234G with region code "E", "I", "Y", "S", "V" and "N" (without Brazil Anatel).
1003143	Enable DFS channels for FAP-234G with region code "A".
1024954	Enable DFS channels for FAP-23JF, FAP-231G and FAP-233G with region code "U".

Changes in CLI

Bug ID	Description

951641	FortiAP Wi-Fi 6E models can enable or disable MACsec locally using the following command (when `WAN_1X_ENABLE` has been set to `1`).
	To enable MACsec:
	`cfg -a WAN_1X_MACSEC_POLICY=1`
	`cfg -c`
	To disable MACsec:
	`cfg -a WAN_1X_MACSEC_POLICY=0`
	`cfg -c`
	Note: In general, FortiAP can enable or disable MACsec from the FortiAP Profile's `wan-port-auth-macsec` setting.

Upgrade and downgrade information

Upgrading to FortiAP version 7.4.3

FortiAP 7.4.3 supports upgrading from FortiAP version 7.2.2 and later.

Downgrading to previous firmware versions

FortiAP 7.4.3 supports downgrading to FortiAP version 7.2.2 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 **Support > Firmware Image Checksum**.
4. Enter the image file name, including the extension. For example, FAP_231F-v7-build0365-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 7.4.3:

FortiOS	FortiOS 7.4.4 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 7.4.3. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
692160	Wireless packets captured by FortiAP radio in Sniffer mode were corrupted.
815950	HTTPS access to the FortiAP web UI would randomly become inaccessible.
865368	When FIPS-CC mode is enabled, FortiAP should report relevant FIPS logs to the FortiGate.
926213	Fixed a kernel panic issue in `target_if_spectral_finite_scan_update` with `INFO: rcu_preempt self-detected stall on CPU`.
928135	FAP-231G/233G 2.4GHz radio sometimes would stop beaconing multiple SSIDs.
931520, 1027267	FortiAP could not properly scan wireless stations with new MAC addresses.
961896	Fixed the Polestar tag detection and relevant BLE issues in FortiAP Wi-Fi 6E models.
962577	FAP-432FR should be able to enable the same DFS channels as FAP-432F.
963924	Wi-Fi clients failed to access the Internet after roaming over local-bridging SSID from one FortiAP to another.
968461	FortiAP sometimes failed to report channel information so the FortiGate would show the operating channel as 0.
978378	FortiAP would leave the FortiGate at seemingly random times during HA setup.
979621	After a radar signal was detected on the operating DFS channel, FortiAP would leave the FortiGate and then join again.
985255	FortiAP models had incorrect antenna gain configuration.
990868	Wireless clients sometimes could not connect to FortiAP Wi-Fi 6E models due to a "4-Way Handshake timeout" error.
992823	FortiAP LLDP daemon should send the customized AP hostname in the System Name TLV.
995222	The mesh-leaf FortiAP could not connect due to a `QDF ASSERT in wlan_mlme_start_sta_vdev Line 404` issue.
1008655	FortiAP was rebooted by a watchdog timer because the LLDP daemon became stuck.
1011732	FortiAP could not reconnect to FortiLAN Cloud after the network recovered from power outages.
1017829	FortiAP failed to report its LLDP neighbors to the new primary FortiGate after a HA failover.
1026503	FortiAP repeatedly left and rejoined the FortiGate when the FortiGate Session Life Support Protocol (FGSP) between two locations is enabled in the FortiGate HA setup.

Known issues

The following issues have been identified in FortiAP version 7.4.3. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
980717	FAP-234G/432G outdoor mode cannot work on the 6GHz radio band.
981982	FAP-234G as mesh leaf cannot create a connection with mesh root FAP. **Workaround:** On the FortiGate, edit the `wtp-profile` of FAP-234G, and set `indoor-outdoor-deployment` to `indoor`.

www.fortinet.com