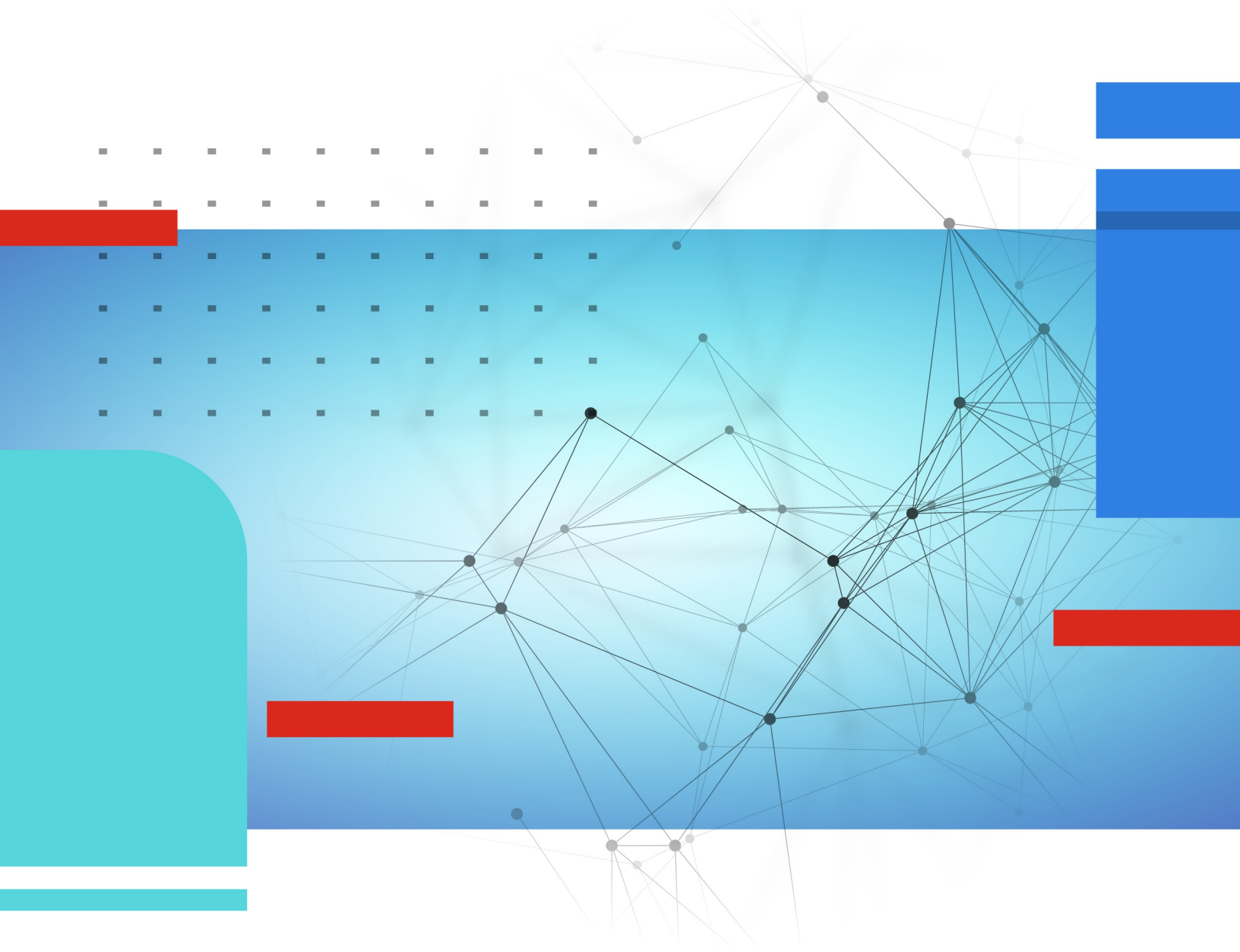
Release Notes

FortiAP 7.6.1



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

Apr 1, 2025
FortiAP 7.6.1 Release Notes
20-761-1117022-20250401

TABLE OF CONTENTS

Change log

Date	Change description
2025-02-20	Initial release.
2025-04-01	Updated Region/country code update and DFS certification on page 7.

Introduction

This document provides release information for FortiAP version 7.6.1, build 0941.

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

Supported models

FortiAP version 7.6.1, build 0941 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

Wi-Fi 7 Models
FAP-241K, FAP-243K, FAP-441K, FAP-443K

New features or enhancements

The following table includes FortiAP version 7.6.1 new features and enhancements:

Bug ID	Description
0471150	**FortiAP Wi-Fi 6E models only:** Send local-bridging UTM logs in Syslog format to the FortiAnalyzer as configured by the FortiGate. **Note:** This feature is only supported on FortiOS 7.6.1 and FortiAnalyzer 7.6.2.
1006876	Support FortiAP Wi-Fi 7 models: FAP-241K, FAP-243K, FAP-441K and FAP-443K.
1012689	Support WPA3 Beacon Protection on FortiAP Wi-Fi 6E and Wi-Fi 7 models.
1029527	Improve the configuration of BLE-based Real-Time Location Service (RTLS) and support "Evresys" RTLS solution.
1032950	Support updating the MAC address database from the FortiGate WiFi Controller.
1043785	Support RADIUS-based MAC-address MPSK authentication on WPA3-SAE SSID.
1044333	Support Console, SSH, or HTTPS login using remote user accounts from a third-party TACACS server.
1045944	Support secure RADIUS over TCP and TLS (RadSec) in WPA2/WPA3-Enterprise authentication.
1056860	Support uploading the portal server's certificate with wildcard or matching DNS names to improve HTTPS host redirection over bridge-mode captive-portal SSID.
1060577	Support advanced Wireless Intrusion Detection System (WIDS) options.
1065958	Support the "AP Name:SSID" format for the "Called-Station-Id" attribute in RADIUS "Access-Request" packets.
1078490	Support secure RADIUS over TCP and TLS (RadSec) in bridge-mode captive-portal authentication.
1078727	Improve FortiAP failover mechanism across layer-3 boundaries. FortiAP devices will not unnecessarily reboot when the following conditions are met: 1. The hostnames of the primary and secondary FortiGate devices contain the same prefix with at least four characters; and 2. The secondary FortiGate is running the same or newer version of FortiOS.
1086517	Support RADIUS accounting messages with the FortiGuest server for local-standalone MPSK SSID.
1093242	Add support for Zoom and Webex applications in the nDPI application detection and DSCP marking function.

Region/country code update and DFS certification

Bug ID	Description
0911455	Add Nigeria (NG) to region code "I". On FortiAP Wi-Fi 6E and Wi-Fi 7 models, add Djibouti (DJ), Gabon (GA), Gambia (GM), Liberia (LR), Somalia (SO), and Swaziland (SZ) to region code "E".
0936150	Enable 6GHz channels for Faroe Islands (FO).
1043895	Enable 6GHz channels (1 - 93) for Taiwan and Macau.
1056641	Enable DFS channels for FAP-441K with region code "J".
1061658	Change Uzbekistan to region code "P"; enable 6GHz channels (1 - 93) for region "P".
1061666	Enable 6 GHz channels (1 - 93) for Philippines and Pakistan.
1063701	Enable DFS channels for FAP-432G with region code "A".
1070912	On FortiAP Wi-Fi 6 and Wi-Fi 6E models, the region code of the following countries has changed from "A" to "N": Barbados, Belize, Colombia, Dominican Republic, Grenada, Guyana, Honduras, Micronesia, and Panama. **Note:** On FortiAP Wi-Fi 7 models, these country codes are still in region code "A".
1072151	Enable DFS channels for FAP-234G with region code "D".
1077770	Disable 6GHz channels for FAP-234G, FAP-432G, FAP-243K and FAP-443K in Brazil, Japan, and Taiwan.
1077772	Disable 6GHz channels for FAP-234G and FAP-432G with region code "A".
1077778	FAP-443K with region code "A" has disabled the 6GHz radio due to limitations of the Automated Frequency Coordination (AFC) module.
1081220	FAP-243K with region code "A" has disabled the 6GHz radio due to limitations of the Automated Frequency Coordination (AFC) module.
1091791	Enable DFS channels for FAP-241K and FAP-243K with region code "A", "E", "I", "Y", "S", "V", "H", "D", and "N" (without Brazil).
1097776	Enable DFS channels for FAP-441K and FAP-443K with country code "BR" (Brazil in region code "N").
1097806	Enable DFS channels for FAP-241K and FAP-243K with region code "T".
1110734	Disable DFS channels for FAP-443K with region code "D".

Changes in CLI

Bug ID	Description

1078727	Add `AC_PRI_PREFERENCE` for Access Controller (AC) priority preference in HA failover and fallback.
	The default value of `AC_PRI_PREFERENCE` is 0, meaning FortiAP prefers the AC with a relatively low load, maintaining the same behavior as before. When necessary, `AC_PRI_PREFERENCE` can be set to 1, so that FortiAP prefers the first available AC in priority order.
	To configure:
	`cfg -a AC_PRI_PREFERENCE=1`
	`cfg -c`
	For example, given two FortiGate WiFi controllers AC1 (high priority) and AC2 (low priority), FortiAP connects with AC1 at first. Once AC1 is down, FortiAP can connect with AC2. Later, after AC1 comes back online, FortiAP will reconnect with AC1.

Upgrade and downgrade information

Upgrading to FortiAP version 7.6.1

FortiAP 7.6.1 supports upgrading from FortiAP version 7.4.3 and later.

Downgrading to previous firmware versions

FortiAP 7.6.1 supports downgrading to FortiAP version 7.4.3 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 *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 7.6.1:

FortiOS	FortiOS 7.6.1 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 7.6.1. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
0790543	Fixed a kernel panic issue `PC is at osif_delete_vap_wait_and_free+0x3ac/0x430 [umac].`
0901543	Fixed a kernel panic issue in FortiAP Wi-Fi 6E models: `Excep :0 Exception detectedparam0 :zero, param1 :zero, param2 :zero.`
0910271	When managed by FortiEdge Cloud, FortiAP preserved the records of disconnected clients. Those clients could not access the Internet after reconnecting with the FortiAP.
0923964	Some Wi-Fi devices couldn't acknowledge DHCP packets transmitted by FortiAP over the 802.11ax band.
1024137	After operating for an extended period of time, FortiAP stops sending EAPOL packets and de-authenticates wireless stations with 4-way handshake timeout.
1025627	FortiAP sometimes stopped forwarding downlink data traffic to roaming clients.
1028653	Ekahau tag blink mode couldn't work with FortiAP.
1054107	In rare instances, FortiAP sent probe response without including the SSID name.
1055682	Fixed a kernel crash issue `sched_algo_txbf.c:1034 Assertion.`
1056451	FortiAP goes offline after a switch connects over the FortiAP mesh bridge.
1056857	When two SSIDs were assigned to the 6GHz radio, some Wi-Fi devices can only detect one SSID.
1056861	Fixed a kernel crash issue PC is at `run_timer_softirq+0x138/0x1c8.`
1066509	FortiAP should report the BLE MAC address to the FortiGate.
1070627	FortiAP sometimes experienced an LLDP daemon crash when connected to a Juniper EX2300 switch.
1071967	FortiAP sometimes experienced high CPU usage and would disconnect from the FortiGate.
1082885	Alcatel 8168s Wireless Phones experienced choppiness in voice calls.
1091187	The Block page was not displayed when UTM Web Filter is triggered for HTTPS website.
1094022	Wireless clients were randomly denied due to incorrect RSSI calculations.
1094048	FortiAP could not automatically change its operating channel after `tx_retries` exceeded the threshold under high channel utilization.
1102995	The 5GHz radio of FortiAP Wi-Fi 7 models would change to 802.11a mode after channel switching.

Bug ID	Description
1114804	FortiAP would experience a kernel-crash issue when FortiAP WAN-LAN mode is enabled and wireless clients ping wired clients on the LAN port that has been bridged to a local-standalone NAT-mode VAP.
1123818	In FortiGate HA setup, a few FortiAP units could not connect with the secondary FortiGate.

Known issues

The following issues have been identified in FortiAP version 7.6.1. 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