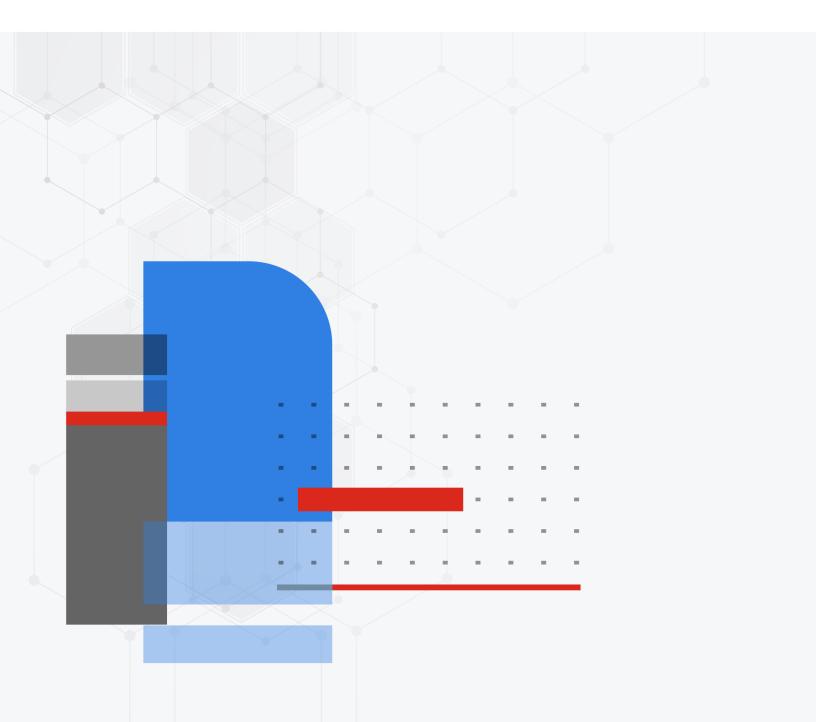# Release Notes

FortiAP 7.4.1

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

FORTINET TRAINING 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

TABLE OF CONTENTS

Change log

Date	Change description
2023-09-26	Initial release.

Introduction

This document provides release information for FortiAP version 7.4.1, build 0591.

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

Supported models

FortiAP version 7.4.1, build 0591 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-431G, FAP-433G

New features or enhancements

The following table includes FortiAP version 7.4.1 new features and enhancements:

Bug ID	Description
382534	Display the Patch number in firmware version, and report the version information with Patch number to the FortiGate. **Note:** FortiGates running FortiOS version 7.4.0 and earlier still can show the FortiAP version without the Patch number.
753332	Foreground scanning improvements: The 2.4GHz, 5GHz, and 6GHz channels to be scanned can be pre-configured from the FortiGate. This way, channels are not being scanned all the time.
819611	Support for new model FortiAP-432FR. **Note:** FortiAP-432FR can be managed by FortiGate running FortiOS 7.0.8, 7.2.1 and later.
890279	Support logging BLE raw data and sending it to the FortiPresence server.
892552	Local-bridging and external-web captive-portal SSID supports dynamic VLAN assignment.

903097	Wi-Fi 6E Models only: Support Trusted Platform Module (TPM).
	The TPM feature is disabled by default.
	To enable TPM, enter the following commands in the FortiAP CLI:
	`cfg -a TPM=1`
	`cfg -c`
	To disable TPM:
	`cfg -a TPM=0`
	`cfg -c`

909586	Support Polestar NAO Track integration and asset management. To check the PoleStar RTLS configuration, enter `cw_diag -c ble-polestar` in the FortiAP CLI.
920073	Site Survey improvements. 1. Configure channel-bonding bandwidth for site survey SSID New CLI variables are added for 2.4GHz and 5GHz bandwidth respectively: `SURVEY_CW_24 = 0(20MHz)	1(40MHz)` `SURVEY_CW_50 = 0(20MHz)	1(40MHz)	2(80MHz)	3(160MHz)` 2. Support 6 GHz spectrum (Wi-Fi 6E Models only) New CLI variables are added for 6GHz channel, bandwidth, and transmit power: `SURVEY_CH_60 = <6GHz channel number>` `SURVEY_CW_60 = 0(20MHz)	1(40MHz)	2(80MHz)	3(160MHz)` `SURVEY_TX_POWER_60 = <6GHz transmit power in dBm>`
920579	Enhance dynamic VLAN assignment based on the RADIUS attribute `Tunnel-Private-Group-Id`: 1. A pool of VLAN IDs (up to 8) can be configured per VLAN name tag; 2. Assign each client a VLAN ID from the pool by a Round-robin method.

Bug ID	Description
921109	Support for MIMO mode configuration.
931158	CAPWAP Auto Health Check feature. FortiAP periodically checks the real-time status of CAPWAP connections to the AP controllers (AC). In the FortiAP CLI, enter `cw_diag -c acs-chan-stats` to get the current results. For additional diagnosis, use `cw_diag debug ping_ac` to enable AC IP ping check and set ping interval (disabled by default).
940570	Improve DNS mechanism for AC Discovery. 1. FortiAP retrieves the AC domain suffix from DHCP option 15 (e.g. "example.com"), which can be configured on a 3rd-party DHCP server; 2. FortiAP has the default AC hostname "`fortinet-capwap-controller`" and combines it with the AC domain suffix as one FQDN (e.g. "`fortinet-capwap-controller.example.com`") for AC discovery by DNS method; 3. When necessary, the AC hostname can be customized by configuring `AC_HOSTNAME_ 1/2/3` without the "`.`" character on the FortiAP.

Region/country code update and DFS certification

Bug ID	Description
601676	Enable 5GHz UNII-1 and UNII-2 channels and adjust transmit power for region code "F" (Indonesia).
911456	Support 6GHz channels for more countries: Malaysia, Singapore, Thailand, Tunisia, and etc.
913393	Enable DFS channels for FAP-432F with region code "K".
919757	Enable DFS channels for FAP-231G/233G with region code "A", "S", "N" (Brazil not included), and "J".
924432	Enable DFS channels for FAP-231G/233G with region code "F".
924783	Enable DFS channels for FAP-231G/233G with region code "K" and "T".
926677	Enable DFS channels for FAP-431G/433G with region code "A", "S", and "N" (Brazil not included).
936150	Support 6GHz channels for more countries: Austria, Bulgaria, Croatia, Greece, Isle of Man, Italy, Latvia, Luxembourg, Mauritius, Monaco, Poland, Romania, Slovakia, Slovenia, and Togo.

Upgrade and downgrade information

Upgrading to FortiAP version 7.4.1

FortiAP 7.4.1 supports upgrading from FortiAP version 7.2.2 and later.

Downgrading to previous firmware versions

FortiAP 7.4.1 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 **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 7.4.1:

FortiOS	FortiOS 7.4.1 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 7.4.1. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
784096	Fixed a kernel panic issue `PC is at _ieee80211_free_node+0x2d0/0x678 [umac].`
890425	FortiAP would sometimes not forward packets from wireless clients to the Ethernet side.
912812	Fixed a kernel panic issue `PC is at bstm_disassociation+0x2c/0x1f0 [umac].`
914341	LLDP daemon should be started by factory default.
928319	With a single 802.3at (PoE+) power supply, FortiAP-431G/433G should support 2.4GHz, 5GHz, and 6GHz 4x4 MIMO while reducing the transmit power and disabling the USB port.
929371	Fixed a kernel panic issue `PC is at wlan_wnm_free_tclass+0x54/0xb8 [umac].`
938988	Wi-Fi clients could not connect after the FortiAP has been running for 24 hours with `dtls-policy ipsec-vpn`.

Known issues

The following issues have been identified in FortiAP version 7.4.1. 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.

FÜRTINET