FortiAP-S and FortiAP-W2 - Release Notes

Version 6.4.6

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/support-and-training/training.html

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

June 8, 2021
FortiAP-S and FortiAP-W2 6.4.6 Release Notes
40-646-0722105-20210608

TABLE OF CONTENTS

Change log

Date	Change description
2021-06-09	Initial release.

Introduction

This document provides the following information for FortiAP-S and FortiAP-W2 version 6.4.6, build 0465:

- Supported models on page 5
- What's new in FortiAP-S and FortiAP-W2 version 6.4.6 on page 5
- Special notices on page 6
- Upgrade and downgrade information on page 7
- Product integration and support on page 8
- Resolved issues on page 9
- Known issues on page 10

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

Supported models

FortiAP-S and FortiAP-W2 version 6.4.6, build 0465 support the following models:

FortiAP-S	FAP-S221E, FAP-S223E FAP-S421E, FAP-S422E, FAP-S423E
FortiAP-W2	FAP-221E, FAP-222E, FAP-223E, FAP-224E, FAP-231E FAP-321E FAP-421E, FAP-423E

FortiAP-W2 models do not have the unified threat management (UTM) functionality.

What's new in FortiAP-S and FortiAP-W2 version 6.4.6

The following list includes new features in FortiAP-S and FortiAP-W2 version 6.4.6:

- Supports VLAN ID assignment according to RADIUS attribute "Tunnel-Private-Group-Id" when it is a text string, and matches one interface name of sub-VLAN interfaces of VAP.
- Supports "SKIP CAPWAP Offload" flag in CAPWAP header of certain packets as required by new FortiGate models with NP7 acceleration module.

Special notices

1. New Wi-Fi 6/802.11ax models FAP-431F, FAP-433F and FAP-231F initially supported as in FortiAP-W2 6.4.0 release have been moved to FortiAP 6.4.3 and later for continuing support.
2. FAP-221E/223E units encounter a specific upgrade issue when connected with HPE PoE switches (refer to Bug ID 643738). Those switches can unilaterally reset/power cycle connected FAP units after not receiving any LLDP response for more than 120 seconds. HPE PoE switch users must first disable LLDP function on the switches before upgrading the FAP units. After all FAP units have been successfully upgraded to firmware version 6.4.3 (or later), LLDP function on the switches can be enabled.

Upgrade and downgrade information

Upgrading to FortiAP-S and FortiAP-W2 version 6.4.6

FortiAP-S and FortiAP-W2 version 6.4.6 support upgrading from FortiAP-S and FortiAP-W2 version 6.2.3 and later.

Downgrading to previous firmware versions

FortiAP-S and FortiAP-W2 version 6.4.6 support downgrading to FortiAP-S and FortiAP-W2 version 6.2.3 and later.

> ⚠ Configurations made when FAP-231E is running a version later than 6.2.3 will not be saved if it is downgraded to 6.2.3.

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_S221E-v600-build0233-FORTINET.out.
5. Click **Get Checksum Code**.

Supported upgrade paths

To view all previous FortiAP-S and FortiAP-W2 versions, build numbers, and their supported upgrade paths, see the Fortinet Documentation website.

Product integration and support

The following table lists product integration and support information for FortiAP-S and FortiAP-W2 version 6.4.6:

FortiOS	6.4.6 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-S and FortiAP-W2 version 6.4.6. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
684825	Unable to establish MESH between two FortiAP units when DHCP relay is used on FortiGate.
701896	After long idle time, WiFi clients cannot reconnect to FortiAP Cloud SSID with PMF enabled.
703088	Fix two TARGET ASSERT issues (in `_HTCPipeProcessControlMsg` and `_tx_send_seq_start_sequence`); Fix kernel panic "`PC is at nss_core_handle_napi`".
710922	FortiAP units cannot stay on the channels assigned by FortiGate DARRP function.
718756	FAP in a remote location is unable to come online on a FGT in a central location via MPLS/site-to-site VPN.
719640	WiFi clients cannot connect bridge-mode SSID when NP7 FGT has capwap-offload enabled.

Common vulnerabilities and exposures

FortiAP-S and FortiAP-W2 version 6.4.6 are no longer vulnerable to the following common vulnerabilities and exposures (CVE) references:

Bug ID	Description
681061	CVE-2021-26106: FortiAP OS command injection through hidden kdbg CLI command.

For details, visit the FortiGuard Labs website.

Known issues

The following issues have been identified in FortiAP-S and FortiAP-W2 version 6.4.6. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
537931	FAP-222E doesn't support the FortiAP Configuration mode. Push and hold the RESET button on the POE adapter for more than 5 seconds to reset FAP-222E to the factory default.
651975	The USB port of FAP-S221E and FAP-S223E doesn't support Electronic Shelf Label (ESL).
655887	FAP-221E/223E gets low throughput on tunnel SSID when its wtp-profile has set `dtls-policy ipsec-vpn`.