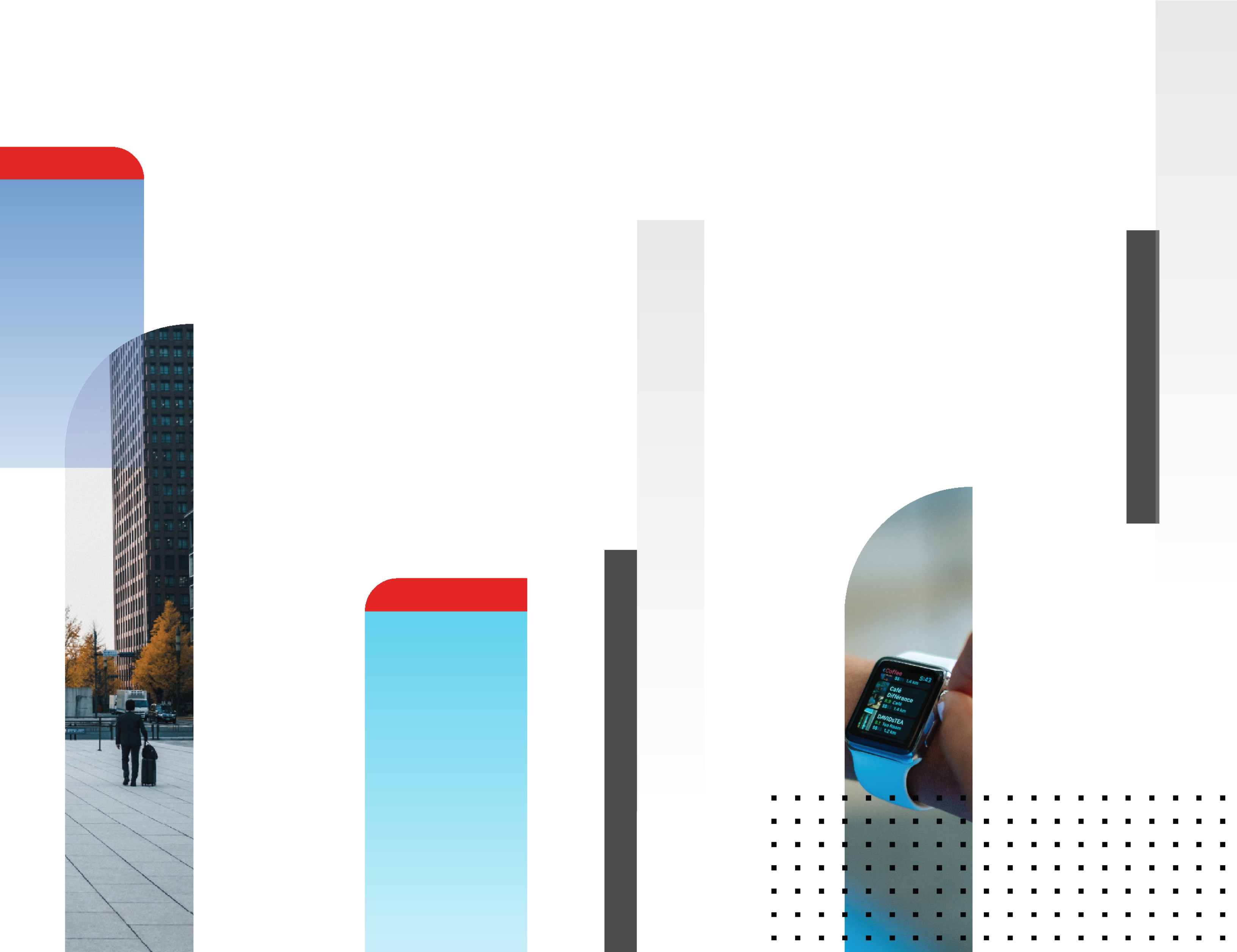
Release Notes

FortiAP-W2 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 12, 2021
FortiAP-W2 7.0.2 Release Notes
40-702-0759567-20211112

TABLE OF CONTENTS

Change log

Date	Change description
2021-11-12	Initial release.

Introduction

This document provides release information for FortiAP-W2 version 7.0.2, build 0049:

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

Supported models

FortiAP-W2 version 7.0.2, build 0049 supports the following models:

Models
FAP-221E, FAP-222E, FAP-223E, FAP-224E, FAP-231E

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

New features or enhancements

The following table includes FortiAP-W2 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 preshared key (MPSK) authentication by checking passphrase together with the 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
753783	Supports DFS channels on FAP-221E Gen3 and FAP-223E Gen3 with region code A, E, I, V, Y and D.

Changes in CLI

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>577504</td><td>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.</td></tr>
<tr><td>735632</td><td>When the WiFi Controller won't overwrite FortiAP WAN port authentication, FortiAP 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&gt;]]</td></tr>
</table>

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.0.2

FortiAP-W2 version 7.0.2 support upgrading from FortiAP-W2 version 6.4.5 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.0.2 support downgrading to FortiAP-W2 version 6.4.5 and later.

FAP-221E Gen3 and FAP-223E Gen3 cannot be downgraded to firmware 7.0.0 and earlier versions.

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

Supported upgrade paths

To view all previous 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-W2 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-W2 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.
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.
738845	Fix a kernel panic trace "`PC is at _raw_spin_lock_bh`".
742221	Fix a kernel crash in `ftnt_m2u_convert() and ol_ath_tx_mgmt_wmi_send().`
746769	Fix a Target Assert issue: `ar_wal_peer.c:4578 Assertion 0 failedparam0 :zero, param1 :zero, param2 :zero.`
750612	Fix a kernel crash in `ieee80211_deliver_data().`
754775	FortiAP might send corrupted IPv6 client information to FortiGate when reconnected.

Known issues

The following issues have been identified in FortiAP-W2 version 7.0.2. 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.
655887	FAP-221E/223E gets low throughput on tunnel SSID when its wtp-profile has set `dtls-policy ipsec-vpn`.

FORTINET®

www.fortinet.com