

Release Notes

FortiExtender 7.4.8



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



Dec 11, 2025

FortiExtender 7.4.8 Release Notes

TABLE OF CONTENTS

Change log	4
Introduction	5
What's new	6
Supported hardware models	7
Special notes	8
Upgrade instructions	9
Firmware upgrade procedures	9
Product integration and support	10
FortiOS-FortiExtender OS compatibility	10
Modes of operation	10
Supported Web browsers	10
Resolved issues	11
Common Vulnerabilities and Exposures	11
Known issues	12

Change log

Date	Change Description
2025-10-23	Initial release.
2025-11-18	Updated Resolved issues on page 11 .
2025-12-11	Updated Common Vulnerabilities and Exposures on page 11 .

Introduction

This Release Notes highlights the important information about the FortiExtender 7.4.8 (Build 0268) release. It covers the following topics:

- [What's new on page 6](#)
- [Supported hardware models on page 7](#)
- [Special notes on page 8](#)
- [Upgrade instructions on page 9](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 11](#)
- [Known issues on page 12](#)

What's new

FortiExtender 7.4.8 is a patch release only. No new features have been implemented in this release. For more information, see [Resolved issues on page 11](#).

Supported hardware models

FortiExtender 7.4.8 supports the following hardware models:

Model	Market
FortiExtender 201E	North and South Americas, EMEA, and some APAC carriers
FortiExtender 211E	Global
FortiExtender 101F-AM	North America
FortiExtender 101F-EA	EMEA, Brazil, and some APAC carriers
FortiExtender 200F	Global
FortiExtender 201F-AM	North America
FortiExtender 201F-EA	EMEA, Brazil, and some APAC carriers
FortiExtender 202F-AM	North America
FortiExtender 202F-EA	EMEA, Brazil, and some APAC carriers
FortiExtender 212F	Global
FortiExtender 311F	Global
FortiExtender 511F	Global
FortiExtenderVehicle 211F	Global
FortiExtenderVehicle 211F-AM	North America
FortiExtenderVehicle 212F	Global
FortiExtenderVehicle 212F-AM	North America

For more information about FortiExtender OS and hardware compatibility, see [FortiExtender OS & Hardware Platform Compatibility Matrix](#).



All built-in modems can be upgraded with compatible, wireless service provider-specific modem firmware.



FortiExtender 201E, 211E, 101F, 201F, 202F, 212F, 311F, 511F and FortiExtenderVehicle 211F devices come with a Bluetooth button, which is turned off by default. When it is turned on, anyone can access the devices via Bluetooth. To safeguard your network, we strongly recommend setting passwords for all your devices before deploying them in your environment.

Special notes

- For FortiExtender 511F devices, the Telstra modem must connect to an LTE/5G network following the first attach request.
- For FortiExtender 511F devices, the Telstra modem requires that a PDN be set for each and every LTE data plan.
- Not all receivers can receive SMS notifications. Be sure to adjust the receiver sequence to ensure that the first receiver always gets SMS notifications.
- Upon reboot, FortiExtender will try to discover the FortiGate or FortiEdge Cloud that manages it, depending on your existing configuration. Because of this, there might be a short delay before the device reconnects to the FortiGate or FortiEdge Cloud.
- In order for FortiExtender to forward syslog messages to a remote syslog server, the syslog server and the FortiExtender LAN port must be part of the same subnet.
- FortiExtender and FortiGate share the same LTE IP in WAN-extension mode. To distinguish local services from FortiGate services, you must configure FortiExtender to use different ports. Otherwise, all traffic to these default services will be sent to FortiExtender locally instead of the FortiGate.
- To avoid a known Quectel RACH issue on FEX-511F, Fortinet has disabled T-Mobile 5G Band n41 (see [Known issues on page 12](#)).

Upgrade instructions



- You can upgrade to the FortiExtender 7.4.8 OS image from FortiExtender 7.0 or later.
 - FEX-201E, FEX-211E, FEX-101F, FEX-201F, FEX-202F, FEX-212F, FEX-311F, FEX-511F, and FEV-211F devices may not be loaded with the latest modem firmware when shipped. To ensure their optimal performance, you **MUST** upgrade their modem firmware with the firmware package (preferably version 22.0.0 or later) specific to your wireless service provider before putting the devices into operation.
-

Firmware upgrade procedures

You can download and install the modem firmware upgrade package in its entirety using the FortiOS CLI, or the FortiExtender GUI or CLI.

To upgrade via the FortiExtender (device) GUI:

1. Log into your FortiExtender.
 2. On the navigation bar on the left, click *Settings*.
 3. From the top of the page, select *Firmware*.
 4. Select *Extender Upgrade > Local*.
-



When connected to the internet, FortiExtender is able to pull the OS images and modem firmware directly from FortiEdge Cloud, irrespective of its deployment status.

Product integration and support

FortiOS-FortiExtender OS compatibility

FortiExtender 7.4.8 supports all FortiOS releases since FortiOS 6.2.0. For more information, see [FOS & FortiExtender OS Compatibility Matrix](#).

Modes of operation

FortiExtender 7.4.8 can be managed from FortiGate or FortiEdge Cloud, or locally independent of FortiGate or FortiEdge Cloud. When deployed in the Cloud, FortiExtender can be centrally managed from FortiEdge Cloud; when managed by FortiGate, the device searches for a nearby FortiGate to transition to Connected UTM mode; when managed locally, it functions as a router providing services to other devices. For more information, see [FortiEdge Cloud Admin Guide](#) and [FortiExtender \(managed\) 7.6.0 Admin Guide](#).

The table below describes FortiExtender's modes of operations in these scenarios.

Management scenario	Mode of operation	
	NAT	IP Pass-through
FortiGate	No	Yes
FortiEdge Cloud	Yes	Yes
Local	Yes	Yes

Supported Web browsers

FortiExtender 7.4.8 supports the latest versions of the following web browsers:

- Google Chrome
- Mozilla Firefox



Other web browsers may function as well, but have not been fully tested.

Resolved issues

The following are the issues fixed in FortiExtender 7.4.8. For inquiries about a particular issue or to report an issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
1097682	The backup mode option was missing when configuring the DHCP server on physical, LAN Switch, VLAN, and Switch interfaces.
1110949	Read-only users are able to make system changes.
1138478	Upgraded third-party libraries.
1149881	Potential to overwrite files using execute CLI commands
1188385	SSH access stops working after FortiEdge Cloud applies a credential plan to the FortiExtender.
1188662	Added the SHA-256 signature into the FortiExtender firmware and included a verification step before upgrading.
1191479	Changed from MD5 to SHA512 for firmware verification.

Common Vulnerabilities and Exposures

Visit <https://www.fortiguard.com/psirt> for more information.

Bug ID	Description
1148265	FortiExtender 7.4.8 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none">• CVE-2025-46775
1148266	FortiExtender 7.4.8 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none">• CVE-2025-46776
1155294	FortiExtender 7.4.8 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none">• CVE-2025-26466
1194557	FortiExtender 7.4.8 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2025-64153

Known issues

The following are the known issues discovered in FortiExtender 7.4.8. For inquiries about a particular issue or to report an issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
0720017	SMS notification is not supported on FortiExtender 511F, 311F, or 101F.
0952615	To avoid a known Quectel RACH issue on FEX-511F, Fortinet has disabled T-Mobile 5G Band n41.
1013515	Depending on the type of serial cable you use, the number of USB OBM connections may be limited on FEX-200F, 201E, 211E, 101F, 201F, 202F, 212F, 311F, and 511F models. When using a 1-16 USB-Serial adapter, those models can only detect 11 ports. When using a 1-4 USB hub with four 1-4 USB-Serial adapters, those models can detect 16 ports.



www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.