

A decorative pattern of overlapping, multi-lined hexagons in a light blue color, set against a dark blue background, located at the top of the page.

FortiExtender - Release Notes

Version 4.1.3

A decorative pattern of overlapping, multi-lined hexagons in a light blue color, set against a dark blue background, located at the bottom of the page.

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://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

July 10, 2020

FortiExtender 4.1.3 Release Notes

TABLE OF CONTENTS

Introduction	4
What's new in FortiExtender 4.1.3	5
Supported hardware models	6
Special notes	7
Upgrade instructions	8
Firmware upgrade procedures	8
Product integration and support	9
Modes of operation	9
Supported Web browsers	9
Known issues	10
Resolved issues	11
Change log	12

Introduction

This Release Notes highlights the important information about the FortiExtender 4.1.3 (Build 181) release. It covers the following topics:

- [What's new in FortiExtender 4.1.3](#)
- [Supported hardware models](#)
- [Special notes](#)
- [Upgrade instructions](#)
- [Product integration and support](#)
- [Known issues](#)
- [Resolved issues](#)

For more information, see the FortiExtender 4.1.3 Admin Guide.

What's new in FortiExtender 4.1.3

FortiExtender 4.1.3 offers the following new features:

- **LTE MTU settings**—The system now allows the user to reset MTU settings to default, including the LTE interface.
- **CLI security enhancement**—More stringent parameter checks have been added to the CLI, removing shell access in non-debug builds.
- **Syslog export to remote syslog servers**—The system is now able to forward system logs to remote syslog servers per user configuration. See [Special notes on page 7](#).
- **USB to multiple serial consoles**—The system now enables the user to connect to multiple serial consoles via a single USB port.
- **SIM switch-back**—FortiExtender is now able to fail back to the preferred SIM card according to user configuration.
- **ICMP error message for DF flagged big packet**— When in IP-passthrough mode, the system is now able to de-fragment large data packets before forwarding them to their destination.
- **Remote diagnose via SMS**—FortiExtender now supports remote diagnostics by SMS.

Supported hardware models

FortiExtender 4.1.3 supports the following hardware models:

- FortiExtender-40D-AMEU
- FortiExtender-201E
- FortiExtender-211E



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

Special notes

- When upgrading to FortiExtender 4.1.3, you must also upgrade the modem firmware. You can either upgrade the entire firmware package version 19.0.0 (or later) or only the firmware/pri inside the package.
- Upon reboot, FortiExtender will try to discover the FortiGate or FortiExtender Cloud that manages it, depending on your existing configuration. Because of this, there might be a one or two minute delay before the device can reconnect to the FortiGate or FortiExtender Cloud.
- FortiExtender 201E and/or 211E devices come with a Bluetooth button, which is off by default. However, 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.
- In order for FortiExtender to forward syslog messages to a remote syslog server, the syslog server and FortiExtender's LAN port must be part of the same subnet.

Upgrade instructions



- You can upgrade your FortiExtender-40D-AMEU to the FortiExtender 4.1.3 OS image from FortiExtender 4.0 or later.
 - For a FortiExtender running FortiExtender OS 3.3.x or earlier, you must upgrade it to 4.0.1 before upgrading it to 4.1.2.
 - Your FEX-201E and/or FEX-211E 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 19.0.0 or later) specific to your wireless service provider before putting them to use.
-

Firmware upgrade procedures



You can upgrade the modem firmware package in its entirety using the FOS CLI, or the FortiExtender OS GUI or CLI. You can also upgrade a specific piece of firmware or PRI file (if you are an experienced professional user).

Modem firmware packages with `.out` extensions can be downloaded and unzipped from [Fortinet Support](#) website. Your unzipped package contains either the Sierra LTE-A EM7455 or the Sierra LTE-A PRO EM7565 modem firmware, which consists of two types of files:

- A PRI file with the filename extension `".nvu"`
- A firmware file with the filename extension `".cwe"`

You must flash both files onto the modem to connect to the wireless service provider of your choice.

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 FortiExtender Cloud, irrespective of its deployment status.

Product integration and support

Modes of operation

FortiExtender 4.1.3 can be managed from FortiGate, FortiExtender Cloud, or locally independent of FortiGate or FortiExtender Cloud. When deployed in the Cloud, FortiExtender can be centrally managed from FortiExtender 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 FortiExtender Cloud Admin Guide and FortiExtender 4.1.3 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
FortiExtender Cloud	Yes	Yes
Local	Yes	Yes

Supported Web browsers

FortiExtender 4.1.3 supports the latest version of the following web browsers:

- Google Chrome
- Mozilla Firefox



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

Known issues

The following are the known issues discovered in FortiExtender 4.1.3.

Bug ID	Description
0586396	FortiExtender models FEX-201E and FEX-211E are not yet supported by FortiExtender Cloud.
0543535	When using thinner-than-normal SIM cards, the user may need to use some extra materials such as a tape to fit them into the SIM card sockets properly
0601997	The user would not be able to cancel uploading modem firmware image from the cloud using the GUI if his/her data-plan was exhausted.
0587235	SMS notifications were not sent to all recipients.
0574663	Pushing FortiExtender configuration from FortiGate would overwrite data-plan configuration on the device.

Resolved issues

The following are the issues fixed in FortiExtender 4.1.3.

Bug fixes

Bug ID	Description
0559512	DHCP server configurations may not be applied correctly.
0562982	FortiExtender-201E does not support VLAN mode.
0588171	Firewall policies would not load in cases involving VRRP configurations. The user had to reboot to make it work properly.
0585753	[switchback] FortiExtender would get stuck in a SIM-switch loop when data usage threshold was reached and the timer is set.
0584768	The GUI would show incorrect interface status.
0584109	Committing VWAN interface, member, and health check configurations would not take effect, resulting in a 404 error instead.
0583865	The user could not delete ports from the LAN switch properly using the GUI.
0583825	The GUI would show memory use of 81% while device is idle.
0577020	FortiExtender did not check the input for the "execute modemfw delete" command.
0576146	Tcpdump sometimes could not be terminated right away, despite of repeated use of "Ctrl+C".
0570742	The system would allow the user to delete or modify auto-generated targets.

Change log

Publishing Date	Change Description
July 10, 2020	First revision, removing reference to FortiExtender 202E and 212E.
February 12, 2020	FortiExtender 4.1.3 Release Notes, first edition.



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.