

A decorative pattern of concentric hexagons in a light blue color, scattered across the top dark blue header area.

# FortiExtender - Release Notes

Version 4.2.0

**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](mailto:techdoc@fortinet.com)

July 10, 2020

FortiExtender 4.2.0 Release Notes

# TABLE OF CONTENTS

<b>Introduction</b>	<b>4</b>
<b>What's new in FortiExtender 4.2.0</b>	<b>5</b>
Support for SNMP (read-only) and traps	5
Low-cost SD-WAN strategy	5
Enhanced LTE configurations	5
IPsec VPN support for third-party certificates	6
FortiGate-FortiExtender zero-touch provisioning (ZTP)	6
<b>Supported hardware models</b>	<b>7</b>
<b>Special notes</b>	<b>8</b>
<b>Upgrade instructions</b>	<b>9</b>
Firmware upgrade procedures	9
<b>Product integration and support</b>	<b>10</b>
Modes of operation	10
Supported Web browsers	10
<b>Known issues</b>	<b>11</b>
<b>Resolved issues</b>	<b>12</b>
<b>Change log</b>	<b>13</b>

# Introduction

This Release Notes highlights the important information about the FortiExtender 4.2.0 (Build 237) release. It covers the following topics:

- [What's new in FortiExtender 4.2.0](#)
- [Supported hardware models](#)
- [Special notes](#)
- [Upgrade instructions](#)
- [Product integration and support](#)
- [Known issues](#)
- [Resolved issues](#)

For more information, see the FortiExtender 4.2.0 Admin Guide.

# What's new in FortiExtender 4.2.0

FortiExtender 4.2.0 offers the following new features:

## Support for SNMP (read-only) and traps

As an SNMP agent, FortiExtender responds to SNMP managers query on v1/v2c and v3 protocol. It supports the following SNMP trap events (which can be configured in both SNMP community and user events):

- system-reboot
- data-exhausted
- session-disconnect
- low-signal-strength
- os-image-fallback
- mode-switch
- fgt-backup-mode-switch

## Low-cost SD-WAN strategy

FortiExtender supports Software-Defined Wide Area Network (SD-WAN) to provide link load-balancing (LLB) among different links. It provides the following features:

- Virtual interface in system for routing system and firewall.
- Adding targets as members and balancing traffic among them.
- Link Load-balancing (LLB) for WAN interfaces or VPN tunnels.
- LTE interface as members of SD-WAN, or combined with a physical interface as members of SD-WAN.
- Support for multiple LLB algorithms:
  - Redundant
  - Weighted Round Robin (WRR)
- Redundant algorithm using a SD-WAN member for data transmission based on:
  - Priority
  - Cost
- Two LTE interfaces as members of SD-WAN redundant by cost algorithm:
  - The lowest cost target works as primary. When primary fails, the next lowest cost target will take over the primary role (fail-over).
  - When a dead primary comes back to life, it will retake the primary role (fail-back).
  - The cost of LTE interface is calculated based on the capacity and monthly-fee of the LTE plan.
- When the LTE and physical interface(s) are members of SD-WAN redundant by cost algorithm:
  - The physical interface must always be selected as lowest cost target and works as the primary.

## Enhanced LTE configurations

The LTE configuration settings have gone through a number of enhancements, namely:

- The default SIM can now be set by carrier, SIM slot, or cost (a new property in LTE plan settings).
- SIM-switching can be configured by data plan, disconnect settings, signal strength, coupled with switch back by time or by timer. All these options are under the renamed "Auto switch" setting.
- The RSSI-interval and RSSI-threshold in LTE settings have been relegated to a new feature, Controller Report.
- The selection method to match plans to SIMs in LTE plan configuration has been consolidated: you can specify the type of plan matching by default, ICCID, carrier, or slot.  
**Note:** Options such as "set iccid", "set carrier", and "set slot" are available only after the "type" has been specified.

## IPsec VPN support for third-party certificates

FortiExtender now is able to use third-party CA certificates at phase 1 to verify identity of peers and to establish IPsec VPN tunnels.

## FortiGate-FortiExtender zero-touch provisioning (ZTP)

FortiExtender supports FortiGate-FortiExtender ZTP. The process is outlined stepwise as follows:

1. Set FortiExtender default discovery mode to auto, and enable the DHCP server over the LAN interface.
2. Acting as a DHCP client, FortiGate connects to the FortiExtender LAN interface to obtain a private IP to reach FortiManager.
3. FortiGate reports the discovered FortiExtender to FortiManager to authorize it (FortiExtender).
4. Once authorized, FortiExtender switches to IP-Passthrough mode disabling DHCP server over the LAN interface, and then reboots itself.
5. Upon booting up in IP-passthrough mode, FortiExtender serves as the FortiExtender-WAN interface of FortiGate, as it does in previous releases.

## Supported hardware models

FortiExtender 4.2.0 supports the following hardware models:

- FortiExtender-201E
- FortiExtender-211E



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

---

## Special notes

- Not all receivers can receive SMS notifications. Be sure to adjust the receiver sequence to ensure that the first receiver always gets SMS notifications.
- When upgrading to FortiExtender 4.2.0, 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 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 to the FortiExtender 4.2.0 OS image from FortiExtender 4.0 or later.
  - 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 4.2.0 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 4.2.0 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
FortiExtender Cloud	Yes	Yes
Local	Yes	Yes

## Supported Web browsers

FortiExtender 4.2.0 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 4.2.0.

Bug ID	Description
0629503	SSH and HTTPS access to FortiExtender over the LTE public IP is not supported.
0607020	FortiGate-managed IP-passthrough mode (capwap) plan would allow traffic over overage-disabled plan capacity.
0608885	The VWAN status does not show correct output with multiple VWAN interfaces.
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.
0574663	Pushing FortiExtender configuration from FortiGate would overwrite data-plan configuration on the device.

## Resolved issues

The following are the issues fixed in FortiExtender 4.2.0.

### Bug fixes

Bug ID	Description
0614487	The DM modem log collection does not work properly.
0587235	SMS notifications were not sent to all recipients.
0620649	The static route would be deleted upon reconnect.
0620533	ESP traffic was dropped every 1 hour, requiring reboot to fix it.
0623310	Implementations of the routing feature on the GUI and in the CLI are not consistent.

## Change log

Publishing Date	Change Description
July 10, 2020	Second revision, removing reference to FortiExtender-212E.
May 4, 2020	First revision, removing reference to "FortiExtender 40D-AMEU" and "FortiExtender OS 3.3.x or earlier" from the "Upgrade instructions" section.
April 27, 2020	FortiExtender 4.2.0 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.