FortiExtender - Release Notes

Version 4.2.1

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

October 19, 2020
FortiExtender 4.2.1 Release Notes

TABLE OF CONTENTS

Introduction

This Release Notes highlights the important information about the FortiExtender 4.2.1 (Build 0274) release. It covers the following topics:

- What's new in FortiExtender 4.2.1
- Supported hardware models
- Special notes
- Upgrade instructions
- Product integration and support
- Known issues
- Resolved issues

For more information, see the FortiExtender 4.2.1 Admin Guide.

What's new in FortiExtender 4.2.1

FortiExtender 4.2.1 offers the following new features:

A RESTful API

FortiExtender now offers a RESTful API.

Periodically generated Syslog reports

FortiExtender is now able to send reports of its system status, such as CPU and memory usage, to the Syslog server at user-configured intervals.

LTE data usage limit enforcement

When LTE data usage has exceeded the limit, all traffic other than management traffic gets blocked. The following traffic to and from the LTE interface is impacted:

- NAT'ed traffic
- VPN data traffic on IPsec Tunnel
- VWAN traffic
- IP-passthrough traffic

FortiGate discovery over multiple interfaces

FortiExtender is able to discover FortiGate by sending discovery messages on multiple ports, one at a time, until it has successfully connected to a FortiGate.

Configurable interface metric

FortiExtender now offers a configurable "distance" parameter per interface.

SIM-switch enhancement

The SIM-switch feature has been enhanced to speed up the SIM-switching process.

DHCP relay support

FortiExtender now supports DHCP relay agent, which enables it to fetch DHCP leases from a remote DHCP server and service its clients.

Reserved addresses on DHCP server

FortiExtender now supports DHCP server with reserved addresses, which allows it to reserve an IP address for a given MAC address.

Modem's QXDM log collection from WEB GUI

FortiExtender is now able to extract QXDM logs from a modem over the WEB GUI.

VLAN support

FortiExtender now supports the creation, deletion, and update of VLAN interfaces. All services such as VRRP, DHCP server, and DHCP relay can also run on VLAN interfaces.

Configuration backup from WEB GUI

FortiExtender now supports configuration backup from its Web GUI in addition to the CLI.

IPsec VPN phase2 linkage to network address objects

IPsec VPN phase2 now supports references to network address objects instead of ip/mask.

System enhancements

- **Reformatted warning messages**—All warning messages have been reformatted for consistency and better readability.
- **Support for read-only file system**—FortiExtender now supports read-only file system for FortiExtender 201E and 211E.
- **Factory reset with graceful shutdown**—FortiExtender now supports graceful shutdown and factory-reset with shutdown option.

For detailed information and implementation of the features, refer to the FortiExtender 4.2.1 Admin Guide.

Supported hardware models

FortiExtender 4.2.1 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 4.2.1, 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 4.2.1 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 4.2.1 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 4.2.1 Admin Guide.

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

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

Supported Web browsers

FortiExtender 4.2.1 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 4.2.1.

Bug ID	Description
0671749	FortiExtender might encounter routing issues after phase1 key lifetime expiry while using IKE v1.
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.
0646519	The DHCP reserved address should be in same subnet as the DHCP server IP address.
0642897	The Unset interface distance value is different from the default one.

Resolved issues

The following are the issues fixed in FortiExtender 4.2.1.

Bug ID	Description
0608885	The VWAN status does not show correct output with multiple VWAN interfaces.
0531223	With FortiExtender running in FortiGate-managed mode, the user would be directed to FortiExtender GUI instead of FortiGate when accessing the unit using SSH, HTTPS, or Telnet over the LTE IP.
0607020	FortiGate-managed IP-passthrough mode (CAPWAP) plan would allow traffic over overage-disabled plan capacity.
0621816	GUI element DHCP server for LAN switch interface contains mandatory fields "DNS server 1*".
0526551	The FortiExtender daemon would restart upon configuration changes.
0625170	FortiExtender needs support VRRP failover on multiple VLAN interfaces.
0574663	Pushing FortiExtender configuration from FortiGate would overwrite data-plan configuration on the device.
0629503	SSH and HTTPS access to FortiExtender over the LTE public IP is not supported.

Change log

Publishing Date	Change Description
October 19, 2020	First update, adding Bug 0671749 to the Known issues section.
August 10, 2020	FortiExtender 4.2.1 initial release.