FortiExtender - Release Notes

Version 4.1.7

March 4, 2021
FortiExtender 4.1.7 Release Notes

TABLE OF CONTENTS

Introduction

This Release Notes highlights the important information about the FortiExtender 4.1.7 (Build 0314) release. It covers the following topics:

- What's new in FortiExtender 4.1.7
- Supported hardware models
- Special notes
- Upgrade instructions
- Product integration and support
- Known issues
- Resolved issues

For more information, see the FortiExtender 4.1.7 Admin Guide.

What's new in FortiExtender 4.1.7

FortiExtender 4.1.7 is a patch release only; no new feature has been implemented in this release.

Supported hardware models

FortiExtender 4.1.7 supports the following hardware model:

- FortiExtender-40D-AMEU

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

Special notes

- FortiExtender 4.1.7 works more smoothly with FortiGate running on FortiOS 6.2 or earlier.
- FortiExtender 4.1.7 introduces a new encryption method sha256, which is not backward compatible with 4.1.6. You must use the Console CLI to for admin password change when downgrading to 4.1.6.
- When upgrading to FortiExtender 4.1.7, 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.
- 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.
- FortiExtender and FortiGate share the same LTE IP in WAN-extension mode. In pre-4.1.7/4.2.2 releases, FortiExtender does not allow access to ssh/https/http/telnet service via the LTE interface, so all the traffic to those default service goes to FortiGate. FortiExtender 4.1.7/4.2.2 adds local ssh/https/telnet/http service support via the LTE interface. 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. Below are the configuration changes you must make after upgrading to FortiExtender 4.1.7:

```
config system management
     config local-access
          set https 22443
          set ssh 2222
     end
end
```

Upgrade instructions

- You can upgrade your FortiExtender-40D-AMEU to the FortiExtender 4.1.7 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.

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 4.1.7 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 4.1.7 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 4.1.7 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 4.1.7.

Bug ID	Description
0671749	FortiExtender might encounter routing issues after phase1 key lifetime expiry while using IKE v1.
0614487	The DM modem log collection does not work properly.
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 4.1.7.

Bug ID	Description
0688429	Upon changing the password from the GUI, the user would be automatically logged out and would not be able to log back in with the new password.
0614863	The system would experience SIM-read failure.
0663150	FortiExtender should not disclose software version prior to authentication.
0657950	Log-in password check was limited to first eight characters.
0649636	FortiGate-managed FortiExtender in static mode might lose its configuration upon reboot.
0677000	Some fields in system interface configuration were missing after factory reset.
0676961	Configuration updates should be written to memory only, not flash.
0660314	Code clean-up was needed for coverity issues.
0671749/0645160	There were some issues in IKEv1 rekeying.
0683105	Policy-based routes were not loaded.

Change log

Publishing Date	Change Description
March 4, 2021	First update, documenting FortiExtender local ssh/https/http/telnet service support via the LTE interface.
January 15, 2021	FortiExtender 4.1.7 initial release.