FortiExtender - Release Notes

Version 7.0.0

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://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 9, 2021
FortiExtender 7.0.0 Release Notes

TABLE OF CONTENTS

Introduction

This Release Notes highlights the important information about the FortiExtender 7.0.0 (Build 024) release. It covers the following topics:

- What's new in FortiExtender 7.0.0
- Supported hardware models
- Special notes
- Upgrade instructions
- Product integration and support
- Known issues
- Resolved issues

For more information, see the FortiExtender 7.0.0 Admin Guide.

What's new in FortiExtender 7.0.0

FortiExtender 7.0.0 offers the following new features:

Administration access profile

This release enables you to configure access permissions to the registered users under System>Account Profile and System>Administration.

Access control

Access permission control applies to all the top-level configuration sections (system, LTE, firewall, etc.) Accessibility to the configuration sections are permission-based upon successful user login.

Three types of access privileges supported:

- Read-write—The configuration section is viewable and fully editable.
- Read-only—The configuration section is viewable, and not editable.
- No-access—The configuration section is inaccessible.

User account setup

The default admin user owns the super_admin profile to access the entire configuration, and is able to add new users with different levels of access permissions to the device accordingly.

OSPF

This release enables you to configure the following basic OSPF features using both CLI and GUI:

- OSPF Status
- OSPF Router-ID
- OSPF Area
- OSPF Network
- OSPF Interface
- Redistribution

The release supports basic features for point-to-point network type over IPSec tunnel and Area 0, and static routes and connected routes are allowed to be redistributed into OSPF routing domain.

Advanced features, such as the network type, authentication type, multiple areas, stub areas and summary-address, etc., are not supported.

For more information, refer to the FortiExtender 7.0.0 Admin Guide.

For detailed information and implementation of the features, refer to the FortiExtender 7.0.0 Admin Guide.

Supported hardware models

FortiExtender 7.0.0 supports the following hardware models:

- FortiExtender-201E
- FortiExtender-211E
- FortiExtender-200F

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

Special notes

- FortiExtender running in local IP-passhrough mode is accessible at 192.168.1.2 over SSH or HTTPS on Port 4.
- 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 7.0.0, 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.
- FortiExtender and FortiGate share the same LTE IP in WAN-extension mode. In pre-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 4.2.2:

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

Upgrade instructions

- You can upgrade your FortiExtender to the FortiExtender 7.0.0 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 7.0.0 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 7.0.0 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 7.0.0 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 7.0.0.

Bug ID	Description
0543535	When using thinner-than-normal SIM cards, you may have to use some extra materials such as a tape to fit them into the SIM card sockets properly.
0672164	LTE1 route was missing in IP route because the Linux IP route tool doesn’t support adding more default routes with the same metric.

Resolved issues

The following are the issues fixed in FortiExtender 7.0.0.

Bug ID	Description
0671749	FortiExtender would encounter routing issues after phase1 key lifetime expiry while using IKE v1.
0693884	Traffic destined for any management port could not be routed through FortiExtender in private network mode.
0704856	CAPWAP channel could not be established when FortiExtender is in auto-discovery mode with FGT static discovery type.

Change log

Publishing Date	Change Description
May 9, 2021	First update, adding Bugs 0693884 and 0704856 to the "Resolved issues" section.
April 27, 2021	FortiExtender 7.0.0 initial release.