FortiExtender - Release Notes

Version 4.1.2

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 4.1.2 Release Notes

TABLE OF CONTENTS

Introduction

This Release Notes highlights the important information about the FortiExtender 4.1.2 (Build 0159) release. It covers the following topics:

For more information, see the FortiExtender 4.1.2 Admin Guide.

What's new in FortiExtender 4.1.2

FortiExtender 4.1.2 offers the following new features:

New hardware models

FortiExtender 4.1.2 supports the following four new hardware models built upon a new hardware platform featuring one WAN port and four LAN ports.

- FortiExtender 201E
- FortiExtender 211E

Support for VRRP

FortiExtender now supports Virtual Router Redundancy Protocol (VRRP), enabling it to work as a backup of the attached router in IP Pass-Through mode.

SMS Notifications

FortiExtender now supports notification via Short Message Service (SMS), thus is able to notify users of system events as they occur.

Multicast forwarding

FortiExtender now supports multicast forwarding which enables it to disseminate data to multiple clients at the same time.

CA #2 certificate support

FortiExtender is now compatible with FOS with Fortinet Certificate Authority (CA) #2.

Health monitoring

FortiExtender now provides health monitoring on up-links by probing a remote service using probe HTTP and DNS probe methods.

Supported hardware models

FortiExtender 4.1.2 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 4.1.2, 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.

Upgrade instructions

- You can upgrade your FortiExtender-40D-AMEU to the FortiExtender 4.1.2 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).

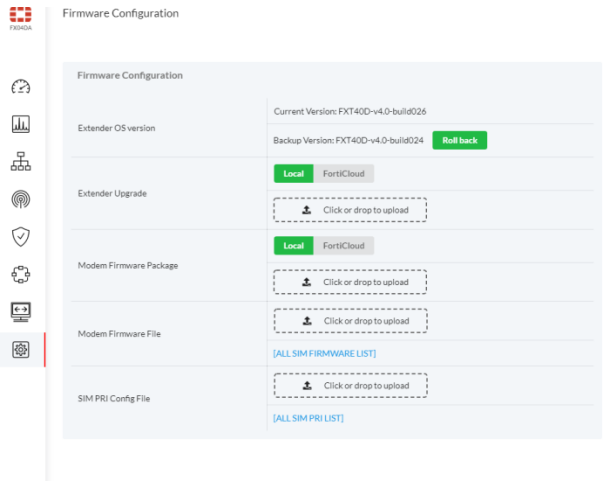
Modem firmware packages with `.out` extensions can be downloaded and unzipped from Fortinet Support website. Your unzipped package contains either the Sierra LTE-A EM7455 or the Sierra LTE-A PRO EM7565 modem firmware, which consists of two types of files:

- 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,** as illustrated below.



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 4.1.2 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 4.1.2 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 4.1.2 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.

Configuration help

FortiExtender 4.1.2 supports the following CLI commands for device status and configuration. For more use cases and advanced configuration options, refer to the FortiExtender 4.1.2 Admin Guide.

Status commands

Command	Description
`get system version`	Displays the device's hardware and software versions.
`get modem status`	Displays detailed modem status information.
`get extender status`	Displays the connectivity status of the FortiExtender device to its master.
`get cpm status`	Displays SSL tunnel information and connectivity status.

Configuration commands

When FortiExtender is deployed in the Cloud, it can download configurations from FortiExtender Cloud. However, you can still configure the device locally using the following commands:

Change the default SIM

The default SIM is sim1. You can change it to sim2 using the following commands:

```
config lte setting modem1
   set default-sim sim {1 | 2}
end
```

Select a preferred carrier

```
config lte setting modem1
   set preferred-carrier <carrier name>
end
```

Enable SIM-switch

```
config lte setting modem1
   set smart-switch enable
end
```

Add a new carrier profile

```
config lte carrier
edit <carrier>
   set firmware <firmware name>
   set pri <pri name>
next
```

Add new carrier

```
config lte simmap
edit <carrier>
   set mcc <first 3 digits of the IMSI number>
   set mnc <next 2 digits the IMSI number>
   set carrier <carrier name from the newly created carrier profile>
next
```

Add new data plan

```
config lte plan
   edit <plan name>
      set carrier <carrier name>
      set apn <carrier apn>
      set capacity <data plan in MB>
      set billing-date <billing date>
      set overage {enable | disable}
   next
end
```

Manage FortiExtender locally

```
config system management
   set discovery-type local
   config local
      set mode ip-passthrough
   end
end
```

Configure VRRP mode

This feature applies to the newly released FEX-201E and /or FEX-211E only. It is not applicable to FEX-40D-AMEU.

```
config system management
 set discovery-type fortigate
  config fortigate
  set ac-discovery-type broadcast
```

```
  set ac-ctl-port 5246
  set ac-data-port 25246
 end


 config fortigate-backup
  vrrp-interface <vrrp interface i.e por1>
  vrrp-id < vrrp id greater than Fortigate>
  status enable
 end
end


config system interface
 edit lan
  config vrrp
   set version 2 <only 2 is supported currently>
   set id <vrrp id>
   set ip <IP of virtual router>
   set priority <priority>
   set adv-interval <advertisement interval in seconds>
   set start-time <initialization timer for backup router, typically 1>
   set preempt <enable | disable> (preempting master typically disable)
   set status enable
  end
 next
end
```

To display the status of virtual router on FortiExtender, use the following command:

```
get router info vrrp
```

Configure health monitoring (HMON)

```
config hmon
    config interface-monitoring
        edit < interface specific monitor name >
            set interval <interval size in seconds, default:30>
            set interface <interfaces to monitor: lte1, lte2>
            set filter <interested fields: rx_bytes,tx_bytes,rx_packets,tx_packets,rx_
dropped,tx_dropped,rx_bps,tx_bps,rx_pps,tx_pps>
        next
    end
    config hchk
        edit < health check type name >
            set protocol <ping|http|dns, default: ping>
            set interval <interval size in seconds, default :30>
            set probe-cnt <probes to be sent within an intervalm default:1>
            set probe-tm <probe timeout, default:2>
            set probe-target <target to be probed>
            set interface <uplink interfaces on which probe has to be sent>
            set src-iface <interface whose source IP is to be used>
            set filter <rtt |loss>
        next
    end
end
```

To display interface statistics by filter:

```
get hmon interface-monitoring <interface specific monitor name>
```

To get health parameters:

```
get hmon hchk <health check type name>
```

To run health check monitor to display all interface statistics:

```
execute hmon interface-monitoring <interface>
```

To run health check on a specific interface:

```
execute hmon hchk protocol ping -I <interface> <probe ip or url>
```

Configure route multicasting

FortiExtender is capable of running PIM-SM to discover terminal devices and join multicast routing group accordingly.

```
config router multicast
 config pim-sm-global
 set join-prune-interval <Periodic JOIN/PRUNE message interval, default 60>
 set bsr-priority 5 <BSR priority , default 5>
 set spt-threshold <SPT threahold, default 3000 >
 set hello-interval < Periodic Hello message interval, default 30 >
 config rp-address
        edit 1
        set address <RP ip adddress>
        set group <Group for this RP >
 next
 end
 end

 config interface
  edit lan //the interfaces PIM running on
  next
  edit rp //the interfaces PIM running on
  next
  end
end
```

Configure SMS

FortiExtender supports the configuration of mobile phone numbers, thus enabling the reception of SMS-based alerts.

To create receivers:

```
config system sms-notification
set notification enable/disable
config receiver
edit <user1>
                set receiver enable/disable
                set phone-number <mobile phone number>
                set alert <type of alerts i.e system-reboot,data-exhausted,session-disconnect,etc >
                next
 edit <user2>
                        set receiver enable/disable
                        set phone-number <mobile phone number>
                        set alert <type of alerts i.e system-reboot,data-exhausted,session-disconnect,
                next
 end
```

To use/tune alert messages:

The following messages can be edited, but no new categories can be created.

```
config system sms-notification alert
    set system-reboot rebooting
    set data-exhausted data plan is exhausted
    set session-disconnect LTE data session is disconnected
    set low-signal-strength LTE signal strength is too low
    set os-image-fallback system start to fallback OS image
    set mode-switch system working mode switched
end
```

Known issues

The following are the known issues discovered in FortiExtender 4.1.2.

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
0559512	DHCP server configurations may not be applied correctly.
0562982	FortiExtender-201E does not support VLAN mode.

Resolved issues

The following are the issues fixed in FortiExtender 4.1.2.

Bug fixes

Bug ID	Description
0563503	The range of time zones for DHCP server configuration was erroneous.
0563069	The user could not set the SIM pin from FortiGate to FortiExtender.
0562573	VWAN interface members did not show up on the FortiView page.
0562564	VPN configurations deleted from the GUI still remained on the backend server.
0562551	The user was unable to modify timeout values from the GUI.
0562439	NAT-disable policies would still cause packets to be NAT'ed.
0562413	VWAN members could not be deleted from the GUI.
0562368	The user was unable to change the default CAPWAP control port.
0562030	The GUI still allowed the user to sort firewall rules by clicking the column headers.
0559512	DHCP server configuration was not applied correctly.

Common vulnerabilities and exposures

Bug ID	Description
0576703	FortiExtender 4.1.2 is no longer vulnerable to the following CVE Reference: • CVE-2019-15710 For more information, visit https://fortiguard.com/psirt.

Change log

Publishing Date	Change Description
July 10, 2020	First revision, removing reference to FortiExtender 202E and 212E.
October 30, 2019	FortiExtender 4.1.2 Release Notes, first edition.