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

FortiExtender - Admin Guide

Version 4.1.3

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

TABLE OF CONTENTS

Introduction	6
Network topologies	7
Integrated with FortiGate	7
Deployed on FortiExtender Cloud	7
Managed locally	8
Main features and benefits	9
Supported hardware models	9
Cellular capabilities	9
Supported wireless carriers	10
SIM mapping	11
Add a data plan and APN	11
Global SIM with roaming on	12
SIM-switch	12
SIM switch-back	13
Get modem status	13
Modes of operation	15
IP pass-through mode	15
NAT mode	17
Get controller status	17
Interface management	18
Interface configuration guideline	18
Physical interface(s)	19
LTE interface	19
Tunnel interface	19
Virtual-WAN interface	19
Access allowance	19
Get interface status	20
Configure LAN switch	21
Configure DHCP server	23
Network utilities	25
Address	25
Service	25
Target	25
System routing	27
Configure static routing	27
Configure PBR routing	28
View routing configurations	29
Move PBR rules	30
Configure multicast routing	30
Firewalls	32
Configure address/subnet	32

Configure protocol/port range	32
Configure firewall policies	33
Move firewall policies	34
VPN	36
Configure VPN	36
Check VPN tunnel status	38
SD-WAN	40
Configure an SD-WAN	40
Check SD-WAN health	41
Define an SD-WAN member	43
Health monitoring	44
Monitor interface status	44
Perform link health check	45
Configure health monitoring	47
System management	49
Get system version	49
Upgrade OS firmware	49
TFTP	49
FTP	49
USB	50
FortiExtender Cloud	50
GUI	50
Upgrade modem firmware	50
TFTP	50
FTP	50
USB	51
FortiExtender Cloud	51
GUI	51
SMS notification	51
Remote diagnostics via SMS	52
Export system logs to remote syslog servers	52
Configure LTE settings	54
Add a new carrier profile	54
Add a new operator/carrier	54
Set preferred carrier	54
Add a private network	55
Change default SIM	55
Enable SIM-switch	55
Use cases	56
Extended cellular WAN of FortiGate	56
Connect to FortiGate	56
VLAN mode and performance	57
Modem connectivity	58
Dual FortiExtender operations	58
Redundant with FGT in IP Pass-through mode	61

Manage from FortiExtender Cloud	63
Configure with FortiExtender Cloud	64
IP Pass-through mode with Cloud management	64
NAT mode with Cloud management	65
OBM management	66
FEX-201E for FortiGate HA configuration	67
Network topology	67
Prerequisites	67
Configuration procedures	67
Troubleshooting, diagnostics, and debugging	71
Troubleshooting	71
Can't detect FortiExtender on FortiGate	71
Can't manage the FortiExtender from FortiExtender Cloud	71
Can't start an Internet session	71
Status, diagnostics, and debugging commands	72
Diagnose FortiExtender	72
Diagnose from FortiGate	73
Diagnose from FortiExtender Cloud	74
Diagnose from Telnet	74
Collect complete diagnostics information	75
Change Log	76

Introduction

FortiExtender is a plug-and-play customer premises equipment (CPE) device. As a 3G/4G LTE wireless WAN extender, FortiExtender can provide a primary WAN link for retail POS, ATM, and kiosk systems, or a failover WAN link to your primary Internet connection to ensure business continuity. It can be deployed indoors and outdoors, and function as a stand-alone wireless router, or integrate with FortiGate or FortiExtender Cloud.



- Dual-modem FortiExtender devices such as FEX-212E have not been integrated with FortiGate yet.
 - This Admin Guide applies to FortiExtender OS version 4.1.3 and later.
-

Network topologies

FortiExtender 4.1.3 comes in two form factors: one with a single LAN Ethernet port (i.e., FEXT-40D-AMEU) and the other with four LAN Ethernet ports and one WAN Ethernet port (i.e., FEX-201E, FEX-202E, FEX-211E, and FEX-212E). They all can support multiple devices in NAT mode or a single device in IP pass-through mode. FortiExtender works as an extended WAN interface when configured in IP pass-through mode, but it functions as a router when in NAT mode.

The following paragraphs highlight the network topologies for the three common use cases for FortiExtender:

- [Integrated with FortiGate on page 7](#)
- [Deployed on FortiExtender Cloud on page 7](#)
- [Managed locally on page 8](#)

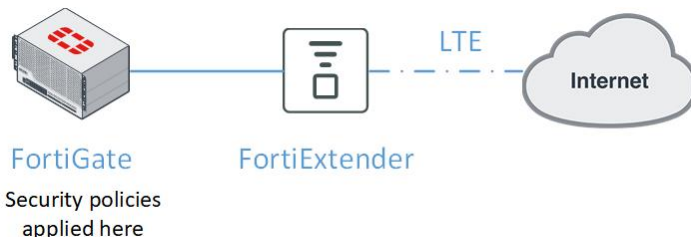
Integrated with FortiGate



Integration with FortiGate requires FortiOS version 6.0.5 or later.

Dual-modem FortiExtender devices such as FEX 202E and FEX212E have not been integrated with FortiGate yet.

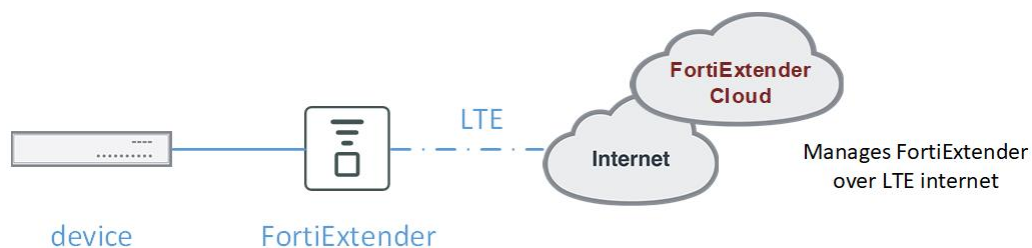
In this scenario, FortiGate manages FortiExtender over the Control and Provisioning of Wireless Access Points (CAPWAP) protocol in IP pass-through mode. Unlike a stand-alone 3G/4G wireless WAN extender, FortiExtender integrates directly into the FortiGate Connected UTM (Unified Threat Management) and is managed from the familiar FortiOS interface. This not only allows security policies to be seamlessly applied to FortiExtender, but also provides visibility to the performance and data usage of the connection.



In this scenario, you can connect a FortiExtender to two FortiGate devices for a high availability (HA) configuration.

Deployed on FortiExtender Cloud

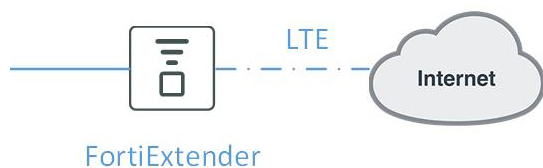
FortiExtender Cloud offers hosted management for an unlimited number of FortiExtender devices deployed anywhere around the globe in either IP pass-through or NAT mode.



FortiExtender Cloud provides hosted management of up to three FortiExtender devices free of charge to each of its registered customers. A license is required for any additional devices. For more information, see FortiExtender Cloud [Admin Guide](#).

Managed locally

In this scenario, FortiExtender works as a stand-alone device without FortiGate or FortiExtender Cloud. The configuration is done locally on the device itself. It can work in either IP pass-through or NAT mode.



Main features and benefits

FortiExtender offers the following main features and benefits:

- [Supported hardware models on page 9](#)
- [Cellular capabilities on page 9](#)
- [Supported wireless carriers on page 10](#)
- [SIM mapping on page 11](#)
- [Add a data plan and APN on page 11](#)
- [Global SIM with roaming on on page 12](#)
- [SIM-switch on page 12](#)
- [Get modem status on page 13](#)



To access your FortiExtender device through its console port, you must set the baud rate to 115200.

Supported hardware models

Model	Market
FEX-40D-AMEU	Americas and Europe
FEX-201E	Americas and Europe
FEX-211E	Global coverage
FEX-212E	Global coverage



FortiExtender 201E, 211E, and 212E 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.

Cellular capabilities

FEX-40D-AMEU, FEX-201E, and FEX-202E use the CAT6 EM7455 built-in modem to cover countries in Americas and Europe using the following frequencies:

- **LTE/4G Bands:** 1, 2, 3, 4, 5, 7, 12, 13, 20, 25, 26, 29, 30, and 41
- **3G UMTS Bands:** 1, 2, 3, 4, 5, and 8

FEX-211E and FEX-212E use the CAT12 EM7565 built-in modem to cover countries in Americas and Europe using the following frequencies:

- **LTE/4G Bands:** 1, 2, 3, 4, 5, 7, 8, 9, 12, 13, 18, 19, 20, 26, 28, 29, 30, 32, 41, 42, 43, 46, 48, and 66
- **3G UMTS Bands:** 1, 2, 3, 4, 5, 6, 8, 9, and 19

Supported wireless carriers

By default, FortiExtender supports all major wireless carriers in Europe and North America.

Region	Carrier
Europe	<ul style="list-style-type: none"> • A1MobilKom • Bouygues • O2 • Orange • SFR • Swisscom • T-Mobile • Vodafone
North America	<ul style="list-style-type: none"> • AT&T • Bell • Rogers • Sasktel • Sprint • Telus • T-Mobile • Verizon



If necessary, you can use the following commands to add a new carrier to the list of supported wireless carriers:

```
config lte carrier
edit free
    set firmware SWI9X30C_02.30.01.01cwe
    set pri SWI9X30C_02.30.01.01_GENERIC_002.045_001.nvu
next
```



FortiExtender may also support other wireless carriers in other parts of the world, depending on the technology and bands used, and with specific configuration changes such as APN. Operation of FortiExtender with any unlisted service provider in any country is not guaranteed. Although the technology and bands may overlap, many variables, such as carrier, SIM card, and certification, must be taken into consideration for reliable operation. Fortinet VARs (Value Added Resellers and Distributors) must confirm compatibility prior to placing a customer order.

SIM mapping

A Public Land Mobile Network (PLMN) is a combination of wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a Mobile Country Code (MCC) and a Mobile Network Code (MNC).

FortiExtender uses a PLMN list to identify the carrier of the SIM cards you are using.

You can also use the following commands to add customized entries to the PLMN list to support the SIMs of unlisted carriers, or create a new PLMN list of any listed carrier:

```
# config lte simmap
(simmap) # edit vzw-222-33
(vzw-222-33) <M> # set mcc 222
(vzw-222-33) <M> # set mnc 333
(vzw-222-33) <M> # next
(simmap) # end
```



FortiExtender automatically switches its modem firmware based on the carrier and technology you are using. If the carrier can't be identified or is unlisted, the generic firmware is used. The generic firmware works with most carriers.

To help FortiExtender recognize the correct carrier name, you can add the MCC and MNC to the configuration file, but this isn't required normally.

Add a data plan and APN

You must have an Access Point Name (APN) to establish a Packet Data Network (PDN) connection with a wireless carrier. For this reason, an APN is a required component in an LTE data plan configuration. In most cases, your SIM card comes with the carrier's APN. If it doesn't or you are not sure what it is, you must find it out from your carrier and add it when creating a data plan.

Use the following commands to create a 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
```



A PDN can't be established without a valid APN. Always be aware of the APN of the SIM card you are using. If you are not sure, contact your network service provider (NSP) for assistance.

Global SIM with roaming on

FortiExtender must always run on the modem firmware compatible with the native wireless operator's SIM. However, this does not apply to roaming operators because roaming agreements require that roaming service providers consider all data service requests. For this reason, there is no need to adjust the configuration for roaming.

SIM-switch

FortiExtender comes with two SIM-card slots, with the first one (i.e., sim1) being the default. SIM-switch is a default feature which works only when you have two SIM cards installed on a FortiExtender device. That way, FortiExtender automatically switches to sim2 to maintain the current LTE connection when any of the following situations occurs:

- An Internet session gets disconnected. By default, FortiExtender automatically switches to sim2 if sim1 gets disconnected for three times within 600 seconds. You can change the values using the following commands:

```
config lte setting modem1
    set disconnect-threshold <3> /*Number of disconnects for sim-switch*/
    set disconnect-period <600> /*Disconnect evaluation period for sim-switch*/
end
```

- Data usage has exceeded the set limit of your data plan and overage is disabled. By default, overage is disabled. SIM-switch does not occur if overage is enabled. You can use the following commands to set the capacity of your data plan and enable or disable overage:

```
config lte plan
edit <plan>
    set carrier <carrier_name>
    set capacity <data plan in MB>
    set billing-date <billing date>
    set overage {enable | disable}
    set signal-threshold <-100> /*RSSI to be evaluated*/
    set signal-period <600> /*Signal evaluation time in seconds*/
next
```

- The relative signal (RSSI value) stays lower than the specified value for a major part of the time period defined. By default, the RSSI value is -100, and the time period is 600 seconds. This means that SIM-switch occurs if the RSSI value stays below -100 for more than 300 seconds.



SIM-switch is a feature in data plan configuration which can be configured from FortiExtender Cloud and/or locally from the GUI. It can't be configured in FortiGate. All the three aforementioned parameters can be configured from the FortiExtender CLI.

SIM switch-back

Following a fail-over, FortiExtender is able to fail back to the preferred SIM card according to user configuration.

To enable SIM switch-back:

```
FX202E5919000011 # config lte setting modem1
FX202E5919000011 (modem1) # show
config lte setting modem1
    set cert-mode disable
    set default-sim
    set preferred-carrier
    set rssi-interval 300
    set rssi-threshold 10
    set gps enable
    set smart-switch enable
    set switch-back-time
    set switch-back-timer 0
    set ipv6 disable
    set disconnect-threshold 3
    set disconnect-period 600
    set sim1-pin disable
    set sim2-pin disable
end

FX202E5919000011 (modem1) # set
switch-back-time          switch over to preferred sim/carrier at a specified (UTC) time
(HH:MM)
switch-back-timer         switch over to preferred sim/carrier after the given time (3600-
2147483647 sec)
```

Get modem status

You can use the following command to get your modem status:

```
FX04DA5918004527 # get modem status
Modem status:
modem                : Modem1
usb path              : Modem index1
vender                : Sierra Wireless, Incorporated
product               : Sierra Wireless, Incorporated
model                 : EM7455
SIM slot              : SIM2
revision              : SWI9X30C_02.24.05.06 r7040 CARMD-EV-FRMWR2 2017/05/19 06:23:09
imei                  : 359073060807702
iccid                  : 89014103275962034129
imsi                   : 310410596203412
pin status             : disable
pin code               : N/A
carrier                : AT&T
```

```
APN                : broadband
service            : LTE
phone number       : 14084069495
sim pin (sim0)     : 3 attempts left
sim puk (sim0)     : 9 attempts left
rssi (dBm)         : -49
signal_strength    : 99
ca state           : INACTIVE
cell ID            : 0A38ED09
band               : B2
band width         : 20
sinr (dB )         : 8.6
rsrp (dBm)         : -80
rsrq (dB )         : -15.5
plan_name          : For-Fortinet-demo
connect_status     : connected
reconnect count    : 0
up time (sec)      : 1418
clock (UTC)        : 18/12/26,19:03:51
temperature        : 38
activation_status   : N/A
roaming_status     : N/A
usb_wan_mac        : da:1e:bf:9a:71:08
Latitude           : 37.376281
Longitude          : -122.010817
```

Modes of operation

Depending on the way it is managed, FortiExtender can operate in IP pass-through or NAT mode(s):

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

This section covers the following topics:

- [IP pass-through mode on page 15](#)
- [NAT mode on page 17](#)
- [Get controller status on page 17](#)

IP pass-through mode

In IP pass-through mode, FortiExtender distributes the WAN IP address provided by the NSP to the device behind it. It can be managed from FortiGate, FortiExtender Cloud, or locally as a stand-alone device.



It is important to note that IP pass-through mode is the only mode of operation for managing FortiExtender from FortiGate.

Enable IP pass-through mode from FortiGate

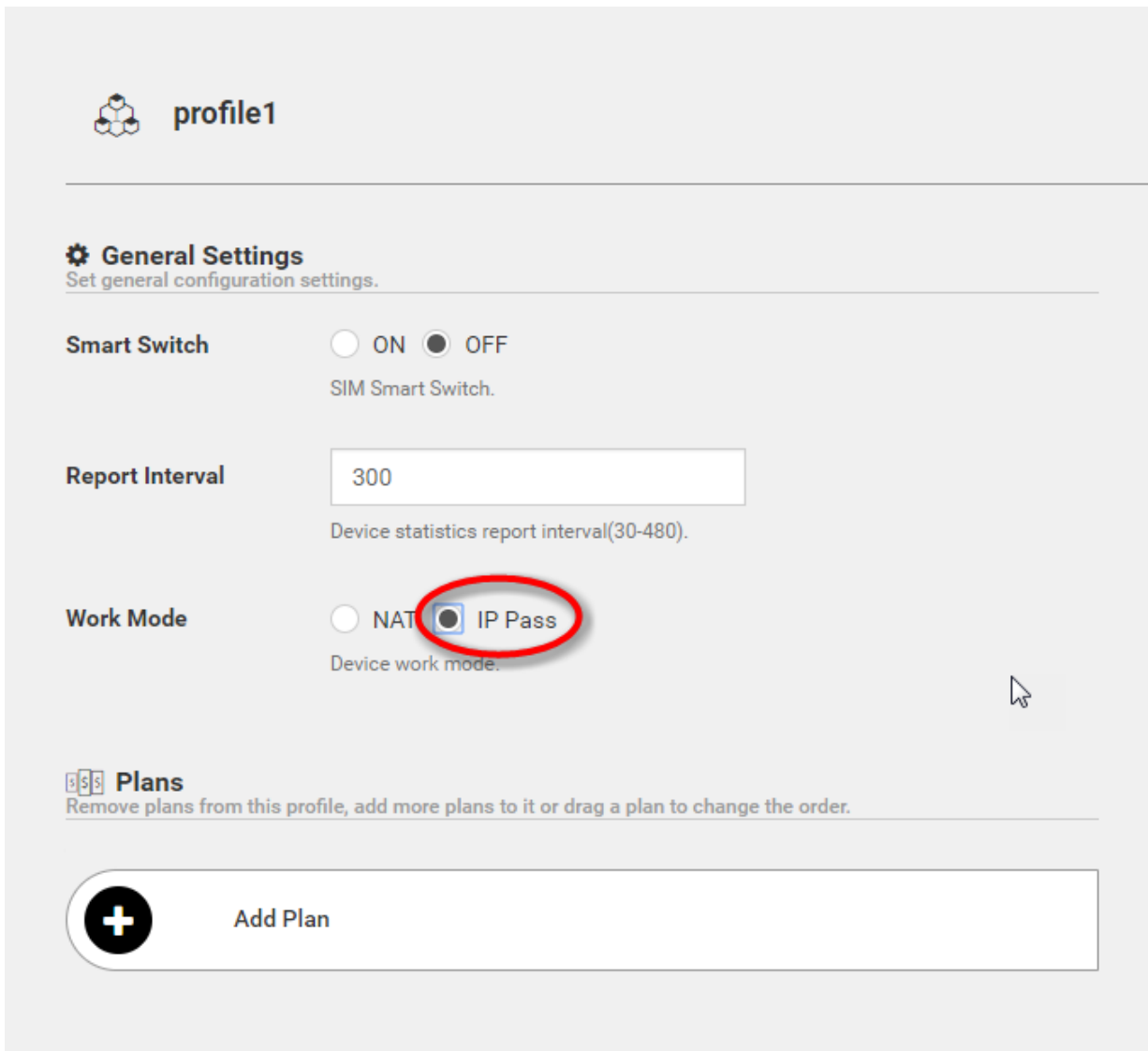
You can enable IP pass-through mode on FortiGate using the following commands:

```
# config system management
  (management) # set discovery-type fortigate
  (management) # end
#
```

Enable IP pass-through mode from FortiExtender Cloud

You can also enable IP pass-through mode from FortiExtender Cloud using the following commands, and then create a profile with IP pass-through enabled, as illustrated below.

```
# config system management
  (management) # set discovery-type cloud
  (management) # end
#
```



The screenshot shows the configuration page for 'profile1'. Under the 'General Settings' section, the 'Smart Switch' is set to 'OFF'. The 'Report Interval' is set to '300'. The 'Work Mode' is set to 'IP Pass', which is highlighted with a red circle. Below this, there is a 'Plans' section with an 'Add Plan' button.

profile1

General Settings
Set general configuration settings.

Smart Switch ☐ ON ☒ OFF
SIM Smart Switch.

Report Interval
Device statistics report interval(30-480).

Work Mode ☐ NAT ☒ IP Pass
Device work mode.

Plans
Remove plans from this profile, add more plans to it or drag a plan to change the order.

Add Plan

Enable IP pass-through mode for local setup and management

FortiExtender can be used as a stand-alone device, without integration with FortiGate or FortiExtender Cloud. In this scenario, all configuration is done locally on the FortiExtender device. We call this mode of operation "local" mode.

You can enable IP pass-through in local mode using the following commands:

```
# config system management
(management)# set discovery-type local
(management) <M># config local
(local)# set mode ip-passthrough
```


NAT mode

The LAN port on FortiExtender can support multiple devices (e.g., PCs, printers, etc.) in NAT mode . In this mode, FortiExtender works as a gateway of the subnet behind it to forward traffic between the LAN and the LTE WAN.

The following features are supported in NAT mode:

- [Interface management on page 18](#)
- [Configure DHCP server on page 23](#)
- [System routing on page 27](#)
- [Configure PBR routing on page 28](#)
- [Firewalls on page 32](#)
- [VPN on page 36](#)
- [SD-WAN on page 40](#)
- [Health monitoring on page 44](#)

Get controller status

You can configure or manage FortiExtender from FortiGate, FortiExtender Cloud, or locally. If you are not sure "who" is your FortiExtender's controller, use the following command to find out:

```
FX04DA5918004527
# get extender status
Extender Status
name                : FX04DA5918004527
mode                : CLOUD
fext-addr           : 192.168.2.1
fext-wan-addr       : 10.4.82.55
controller-addr     : fortiextender-dispatch.forticloud.com:443
management-state    : CWWWS_RUN
base-mac            : 70:4c:a5:fd:1b:38
network-mode        : nat
discovery-type      : cloud
discovery-interval  : 5
echo-interval       : 30
report-interval     : 30
statistics-interval : 120
```

Interface management

FortiExtender-40D-AMEU comes with one LAN interface and one LTE interface, whereas FortiExtender-201E comes with one WAN interface, one LTE interface, and four LAN interfaces. The table below describes the CLI commands used to configure the system interface.

CLI command	Description
<code>config system interface</code>	Enters system interface configuration mode.
<code>edit <interface_name></code>	Specify or edit an interface name.
<code>set type <type></code>	Select the interface type: <ul style="list-style-type: none"> <code>physical</code>—LAN interface, i.e., <code>nas1</code> (Can be edited only). <code>lte</code>—LTE interface, i.e., <code>eth1</code> (Can be edited only). <code>loopback</code>—Loopback interface (Can be edited only). <code>tunnel</code>—Tunnel interface (Can be created, edited, or deleted). <code>virtual-wan</code>—Virtual WAN interface (Can be created, edited, or deleted).
<code>set status {up down}</code>	Specify the interface state: <ul style="list-style-type: none"> <code>up</code>—Enabled. <code>down</code>—Disabled.
<code>set mode {static dhcp}</code>	Set the interface IP addressing mode: <ul style="list-style-type: none"> <code>static</code>—If selected, FortiExtender will use a fixed IP address to connect to the Internet. See <code>set ip <ip></code> below. <code>dhcp</code>—If selected, FortiExtender will work in DHCP client mode.
<code>set ip <ip></code>	(Applicable only when IP addressing mode is set to "static".) Specify an IPv4 address and subnet mask in the format: <code>x.x.x.x/24</code>
<code>set gateway <gateway></code>	Set an IPv4 address for the router in the format: <code>x.x.x.x</code>
<code>set mtu <mtu></code>	Set the interface's MTU value in the range of 0–4294967295.
<code>allowaccess {ping http https telnet capwap}</code>	Select the types of management traffic allowed to access the interface: <ul style="list-style-type: none"> <code>ping</code>—PING access. <code>http</code>—HTTP access. <code>https</code>—HTTPS access. <code>telnet</code>—TELNET access. <code>capwap</code>—CAPWAP access.

Interface configuration guideline

The following are the general guidelines regarding system interface configurations.

Physical interface(s)

FortiExtender LAN interface(s) can be configured in DHCP or static IP addressing mode. When FortiExtender is in NAT mode, you can also configure a DHCP server to distribute IP addresses from the FortiExtender physical Ethernet interface to the devices behind it.

FortiExtender-201E also comes with a WAN physical interface.

LTE interface

The LTE interface only works in DHCP mode and acquires IP addresses directly from wireless NSPs. See [Cellular capabilities on page 9](#).

Tunnel interface

Tunnel interfaces are automatically created when IPsec VPN Tunnels are created. A tunnel interface is a Layer-3 interface which doesn't have an IP address. All traffic sent to the tunnel interface is encapsulated in a VPN tunnel and received from the other end point of the tunnel. It can be used by firewall, routing, and SD-WAN, but cannot be used by VPN.

Virtual-WAN interface

A Virtual-WAN interface is an aggregation of multiple up-links. It works as a common interface because all traffic to it is load-balanced among multiple links.

It can be used by firewall, routing, but cannot be used by SD-WAN or VPN.

Interface configuration example:

```
# config system interface
(interface) # edit lan
    (lan) # set type physical
    (lan) # set status up
    (lan) # set mode static
    (lan) # set ip 192.168.2.1/24
    (lan) # set mtu 1400
    (lan) # set allowaccess http ping telnet
    (lan) # end
```

Access allowance

Both the physical and the LTE interfaces can be configured with access allowance to allow the administrator to access FortiExtender using the following tools:

- SSH
- Telnet
- ping

- CAPWAP
- HTTP
- HTTPS



Access allowance doesn't apply to a tunnel or Virtual-WAN interface.



Access from the LTE WAN side is not supported. If you need to manage FortiExtender via LTE, you must use FortiExtender Cloud.

Get interface status

Use the following command to get system interface status:

```
get system interface
= [ lo ]
name: lo status: online/up/link up type:
loopback mac: 00:00:00:00:00:00 mode: static ip:
127.0.0.1/8 mtu: 65536 gateway: 0.0.0.0
== [ lte1 ]
name: lte1 status: online/up/link up type:
lte mac: d2:82:f4:b7:db:27 mode: dhcp ip:
10.220.139.33/30 mtu: 1500 gateway: 10.220.139.34 dns:
172.26.38.1
== [ lan ]
name: lan status: online/up/link up type:
physical mac: 70:4c:a5:fd:1a:da mode: static ip:
192.168.2.1/24 mtu: 1500 gateway: 0.0.0.0
== [ vwan1 ]
name: vwan1 status: online/up/link up type:
virtual-wan mac: d2:10:5f:ed:71:e8 mode: static ip:
0.0.0.0/0 mtu: 1364 gateway: 0.0.0.0
== [ fcs-0-phase-1 ]
name: fcs-0-phase-1 status: online/up/link up type:
tunnel mac: 00:00:00:00:00:00 mode: static ip:
0.0.0.0/0 mtu: 1364 gateway: 0.0.0.0
== [ fcs-1-phase-1 ]
name: fcs-1-phase-1 status: online/up/link up type:
tunnel mac: 00:00:00:00:00:00 mode: static ip:
0.0.0.0/0 mtu: 1364 gateway: 0.0.0.0
```

Configure LAN switch

FortiExtender-201E comes with four LAN ports (i.e., Ports 1–4) which are part of a LAN switch. These ports can be separated from the LAN switch to run on different IP subnets as well.

To display the current LAN switch configuration:

```
FX202E5919000011 # config system lan-switch
FX202E5919000011 (lan-switch) # config ports
FX202E5919000011 (ports) # show
config system lan-switch ports
    edit port1
    next
    edit port2
    next
    edit port3
    next
    edit port4
    next
end
```

To remove Port 4 from the LAN switch:

```
FX202E5919000011 (ports) # delete port4
FX202E5919000011 (ports) <M> # next
FX202E5919000011 (ports) # show
config system lan-switch ports
    edit port1
    next
    edit port2
    next
    edit port3
    next
end
```

To add Port 4 back to the LAN switch:

```
FX202E5919000011 (ports) # show
config system lan-switch ports
    edit port1
    next
    edit port2
    next
    edit port3
    next
end
```

Example LAN switch configuration

```
FX202E5919000011 (ports) # edit port4
FX202E5919000011 (port4) <M> # next
FX202E5919000011 (ports) # show
config system lan-switch ports
```

```
edit port1
next
edit port2
next
edit port3
next
edit port4
next
end
```

Configure DHCP server

You can configure the DHCP server from FortiExtender Cloud or locally while the device is set in NAT mode.

To run the DHCP server, change the IP address of the LAN interface to the correct subnet, and then create the DHCP server subnet using commands described in the table below.

CLI command	Description
<code>config system dhcpserver</code>	Enters DHCP server configuration mode.
<code>edit <name></code>	Specify the name of the DHCP server.
<code>set status {enable disable}</code>	Set the DHCP server status: <ul style="list-style-type: none"> <code>enable</code>—Enable the DHCP server. <code>disable</code>—Disable the DHCP server.
<code>set lease-time <lease_time></code>	Specify the DHCP address lease time in seconds. The valid range is 300–8640000. 0 means unlimited.
<code>set dns-service {local default specify wan-dns}</code>	Select one of the options for assigning a DNS server to DHCP clients: <ul style="list-style-type: none"> <code>local</code>—The IP address of the interface of the DHCP server that is added becomes clients' DNS server IP address. <code>default</code>—Clients are assigned the FortiExtender configured DNS server. <code>specify</code>—Specify up to three DNS servers in the DHCP server configuration. <code>wan-dns</code>—The DNS of the WAN interface that is added becomes clients' DNS server IP address.
<code>set dns-server1 <dns_server1></code>	Specify the IP address of DNS Server 1.
<code>set dns-server2 <dns_server2></code>	Specify the IP address of DNS Server 2.
<code>set dns-server3 <dns_server3></code>	Specify the IP address of DNS Server 3.
<code>set ntp-service {local default specify}</code>	Select an option for assigning a Network Time Protocol (NTP) server to DHCP clients: <ul style="list-style-type: none"> <code>local</code>—The IP address of the interface of the DHCP server that is added becomes clients' NTP server IP address. <code>default</code>—Clients are assigned the FortiExtender configured NTP servers. <code>specify</code>—Specify up to three NTP servers.
<code>set ntp-server1 <ntp_server1></code>	Specify the IP address of NTP Server 1.
<code>set ntp-server2 <ntp_server2></code>	Specify the IP address of NTP Server 2.

CLI command	Description
<code>set ntp-server3 <ntp_server3></code>	Specify the IP address of NTP Server 3.
<code>set default-gateway <gateway></code>	Specify the default gateway IP address assigned by the DHCP server.
<code>set netmask <netmask></code>	Specify the netmask assigned by the DHCP server.
<code>set interface <interface></code>	Specify the interface on which the DHCP server is expected to run.
<code>set start-ip <start_ip></code>	Specify the start IP address of the DHCP IP address range. For example, 192.168.1.100.
<code>set end-ip <end_ip></code>	Specify the end IP address of the DHCP IP address range. For example, 192.168.1.120.

Example DHCP server configuration:

```

config system dhcpserver
  edit dsl
    set status enable
    set lease-time 8640000
    set dns-service specify
    set dns-server1 8.8.8.8
    set dns-server2 8.8.4.4
    set dns server3
    set ntp-service local
    set default-gateway 192.168.2.1
    set netmask 255.255.255.0
    set interface LAN
    set start-ip 192.168.2.2
    set end-ip 192.168.2.254
    set mtu 1500
  next
end

```

FortiExtender LAN interface(s) can be configured in static IP address mode locally or from FortiExtender Cloud. By default, a LAN interface requires the IP address of 192.168.2.1/24 and can run a DHCP server serving addresses from 192.168.2.2. You can enable the management of LAN-side capabilities from FortiExtender Cloud.



DHCP server mode is not applicable if your FortiExtender is managed from FortiGate.

Network utilities

You can define your network from the following aspects:

- [Address on page 25](#)
- [Service on page 25](#)
- [Target on page 25](#)

Address

Addresses are used to define the networking nodes in your network. An address can be a subnet, a single IP address, or a range of IP addresses. With addresses, you can define the source and destination of network traffic.

Service

Service defines traffic type, such as HTTP, FTP, etc. It consists of a protocol and the destination port.

For example:

```
config network service
  config service-custom
    edit ALL
      set protocol IP
      set protocol-number 0
    next
  end
end
```

Target

Target is the network connected to FortiExtender. It is usually an up-link network, such as an NSP network provided by a wireless carrier. A target consists of an outgoing interface and a next hop. Targets are always used in routing systems and SD-WANs to define the destination network to which traffic is sent.

The table below describes the commands for setting a target.

CLI command	Description
<code>config router target</code>	Enters target configuration mode.
<code>edit <name></code>	Specify the target network.

CLI command	Description
<code>set interface <interface></code>	Specify the outgoing interface of the gateway.
<code>set next-hop <next_hop></code>	Specify the IP address of the next-hop gateway.

Example target configuration:

```
# get system interface
== [ lo ]
name: lo status: online/up/link up type: loopback mac:
00:00:00:00:00:00 mode: static ip: 127.0.0.1/8 mtu: 65536
gateway: 0.0.0.0
== [ eth1 ]
name: eth1 status: online/up/link up type: lte mac:
9a:fd:56:f1:1a:08 mode: dhcp ip: 10.118.38.4/29 mtu: 1500
gateway: 10.118.38.5 dns: 172.26.38.1
== [ nas1 ]
name: nas1 status: online/up/link up type: physical mac:
70:4c:a5:fd:1b:38 mode: dhcp ip: 172.24.236.22/22 mtu: 1500
gateway: 172.24.239.254 dns: 172.30.1.105, 172.30.1.106
# config router target
(target) # edit target.lte
(target/lte) <M> # abort
(target) # edit target.lte
(target.lte) <M> # set interface eth1
(target.lte) <M> # set next-hop 10.118.38.5
(target.lte) <M> # next
(target) # end
```



A target is automatically created when an LTE is connected, with the LTE as the outgoing interface and the gateway as the next hop. The next hop is not mandatory if the outgoing interface is a tunnel interface or a Virtual-WAN interface. For example:

```
edit target.fcs-1-phase-1
  set interface fcs-1-phase-1
  set next-hop
next
edit target.vwan1
  set interface vwan1
  set next-hop
next
```

System routing

FortiExtender 4.1.3 supports [static routing](#) and [Policy Based Routing \(PBR\)](#). Dynamic routing, such as OSPF, ISIS, and EIGRP, is not supported in this release.



Both static routing and PBR apply to NAT mode only.

This section covers the following topics:

- [Configure static routing on page 27](#)
- [Configure PBR routing on page 28](#)
- [View routing configurations on page 29](#)
- [Move PBR rules on page 30](#)

Configure static routing

The table below describes the commands for configuring static routing.

CLI command	Description
<code>config router static</code>	Enters static route configuration mode.
<code>edit <name></code>	Specify the name of the static route.
<code>set status {enable disable}</code>	Set the status of the static route: <ul style="list-style-type: none">• <code>enable</code>—Enable the static route.• <code>disable</code>—Disable the static route.
<code>set dst <dst></code>	Specify the destination IP address and netmask of the static route in the format: <code>x.x.x.x/x</code>
<code>set gateway <gateway></code>	Specify the IP address of the gateway.
<code>set distance <distance></code>	Specify the administrative distance. The range is 1–255. The default is 1.
<code>set device <device></code>	Specify the name of the outgoing interface.
<code>set comment [comment]</code>	Enter a comment (optional).

Example static route configuration:

```
config router static
edit 1
set status enable
set dst 0.0.0.0/0
```

```

        set gateway 192.168.2.1
        set distance 5
        set device lan
        set comment
    next
End

```

Configure PBR routing

The table below describes the commands for configuring Policy Based Routing (PBR).

CLI Command	Description
<code>config router target</code>	Enters target configuration mode.
<code>edit <name></code>	Specify the name of the target.
<code>set interface <interface></code>	Specify the outgoing interface or tunnel.
<code>set next-hop <next_hop></code>	Specify the IP address of the next-hop gateway .

Example PBR configurations:

config router target

```

edit target.lan
    set interface lan
    set next-hop 192.168.10.99
next
edit target.vwan1
    set interface vwan1
    set next-hop
next

```

Example PBR policy configuration:

```

config router policy
    edit vwan1-pbr
        set input-device /* Incoming interface name.
        size[35] - datasource(s): system.interface.name
        set src 192.168.2.0/24 /* Source IP and mask for
        this policy based route rule.
        set srcaddr /* Source address
        set dst /* Destination IP and mask
        for this policy based route rule.
        set dstaddr /* Destination address
        set service /* Service and service
        group names.
        set target /* This PBR's out-going
        interface and next-hop.
        set status enable /* Enable/disable this
        policy based route rule.
        set comment /* Optional comments. size

```

```
[255]
next
end
```

View routing configurations

Use the following commands to view routing configurations.

View routing targets:

```
get router info target
== [ target.lo ]
device : lo
next-hop : 0.0.0.0
route type : automatic
routing-table : target.lo.rt.tbl
reference counter : 0

== [ target.lan]
device : lan
next-hop : 192.168.10.99
route type : automatic
routing-table : target.lan.rt.tbl
reference counter : 0

== [ target.vwan1 ]
device : vwan1
next-hop : 0.0.0.0
route type : automatic
routing-table : target.vwan1.rt.tbl
reference counter : 0
```

View PBR configurations:

```
get router info policy
== [ vwan1-pbr ]
seq : 100
status : enable
input-interface :
src : 192.168.2.0/24
src-addr :
dst :
dst-addr :
service :
target : target.vwan1
routing-table : target.vwan1.rt.tbl
comment :
```

View routing tables:

```
get router info routing-table all
Codes: K - kernel, C - connected, S - static
* - candidate default
```



* 0.0.0.0/0 is the default routing.

Move PBR rules

You can use the `move` command to change the order of the PBR rules you've created.

In the following example, you have created two policy rules:

```
config router policy
  edit one
    set input-device nas1
    set srcaddr
    set dstaddr all
    set service
    set target target.lo
    set status enable
    set comment
  next
  edit two
    set input-device lo
    set srcaddr
    set dstaddr
    set service
    set target target.eth1
    set status enable
    set comment
  next
```

If you want to move policy one after two, you can use either of the following commands:

```
move one after two
```

or

```
move two before one
```

Configure multicast routing

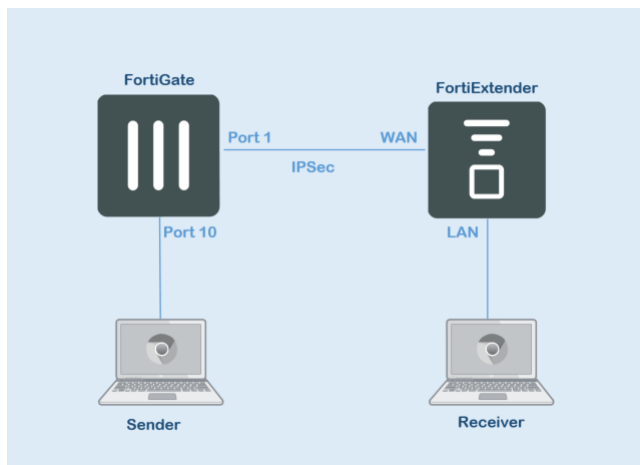


This feature applies to FEX-201E, FEX-202E, FEX-211E, and FEX-212E only.

FortiExtender is capable of running PIM-SM to discover terminal devices which can join multicast routing groups accordingly. Other than supporting multicasting routing directly on LTE WAN links (mostly for private networks), this feature can also be used to run on top of IPSEC interfaces of FortiExtender to enable private and secure multicast routing.

```
FX201E5919000012 # config router multicast
FX201E5919000012 (multicast) # show
config router multicast
  config pim-sm-global
    set join-prune-interval 60
    set hello-interval 30
    config rp-address
      edit 1
        set address 169.254.254.1
        set group 224.0.0.0/4
      next
    end
  end
end
config interface
  edit lan
  next
  edit fex
  next
end
end
```

Multicasting network topology



Firewalls

Firewalls allow you to control network access based on Layer-3 or Layer-4 information. Also, SNAT is provided to perform Source Net Address Translation.

Firewall configuration involves the following tasks:

- [Configure address/subnet on page 32](#)
- [Configure protocol/port range on page 32](#)
- [Configure firewall policies on page 33](#)
- [Move firewall policies on page 34](#)

Configure address/subnet

Use the following commands to specify the IP address/subnet to which you can apply firewall policies.

CLI command	Description
<code>config network address</code>	Enters network IP address configuration mode.
<code>edit <name></code>	Specify the name of the IP address configuration object.
<code>set type {ipmask iprange}</code>	Select either address type: <ul style="list-style-type: none">• <code>ipmask</code>—IPv4 address/mask in the format: <code>x.x.x.x/x</code>• <code>iprange</code>—IP addresses range.

Example address/mask configurations:

```
config firewall address
  edit internet
    set type ipmask
    set subnet 0.0.0.0/0
  next
  edit src
    set type iprange
    set start-ip 192.168.2.3
    set end-ip 192.168.2.4
  next
end
```

Configure protocol/port range

Use the following commands to specify the network protocols and ports to which you want to apply firewall policies.

CLI command	Description
<code>config network service service-custom</code>	Enters the network service configuration mode.
<code>edit <name></code>	Specify the name of the service configuration object.
<code>set protocol <Protocol Type></code>	Specify the protocol (service).
<code>set protocol number <0-255> *</code>	Specify the protocol number (if you are not sure of the name of the protocol).
<code>set protocol udp-portrange</code>	Specify the port range for UDP protocol.
<code>set protocol tcp-portrange</code>	Specify the port range for TCP protocol.

Example protocol/port range configurations:

```
config network service service-custom
  edit service1
    set protocol tcp
    set tcp-portrange 5000-5555
  next
  edit service2
    set protocol udp
    set udp-portrange 6000-6350
  next
  edit service3
    set protocol icmp
  next
  edit service4
    set protocol ip
    set protocol-number 47
  next
end
```

Configure firewall policies

Once you have completed setting the IP addresses/mask and services (protocols)/port ranges you want to control with firewall policies, you can then use the following commands to impose firewall policies on them.

CLI command	Description
<code>config firewall policy</code>	Enters firewall policy configuration mode.
<code>edit <name></code>	Specify the name of the firewall configuration object.
<code>set srcintf</code>	Specify the ingress interface.
<code>set dstintf</code>	Specify the egress interface.

CLI command	Description
<code>set srcaddr</code>	Specify the source IP address, which can be either a single IP address or a range of IP addresses.
<code>set action {allow deny}</code>	Select either of the following actions: <ul style="list-style-type: none"> allow—Allow access. deny—Deny access.
<code>set status {enable disable}</code>	Set the status of the policy: <ul style="list-style-type: none"> enable—Enable the policy. disable—Disable the policy.
<code>set nat {enable disable}</code>	Select an option for NAT: <ul style="list-style-type: none"> enable—Enable NAT. disable—Disable NAT.

Example firewall policy configurations:

```
config firewall policy
  edit filter
    set srcintf any
    set dstintf any
    set srcaddr rec
    set dstaddr internet
    set action deny
    set status enable
    set service service1 service2 service3 service4
    set nat disable
  next
end
```



The FortiExtender firewall is in White List mode, which blocks all traffic by default. You must create a policy to allow traffic into your network.

Move firewall policies

You can use the `move` command to change the order in which your firewall policies are applied.

In the following example, you have created two policy rules:

```
config firewall policy
  edit filter1
    set srcintf any
    set dstintf any
    set srcaddr rec
    set dstaddr internet
    set action deny
    set status enable
    set service service1 service2 service3 service4
    set nat disable
```

```
next
edit filter2
    set srcintf lan
    set dstintf wan
    set srcaddr wow
    set dstaddr internet
    set action allow
    set status enable
    set service service1 service2 service3 service4
    set nat disable
next
end
```

If you want to move policy one after two, you can use either of the following commands:

```
move filter1 after filter2
```

or

```
move filter2 before filter1
```

VPN

FortiExtender uses IPsec VPN to connect branch offices to each other. It only supports the site-to-site VPN tunnel mode.

This section discusses the following topics:

- [Configure VPN on page 36](#)
- [Check VPN tunnel status on page 38](#)

Configure VPN

Use the following commands to configure a VPN tunnel.

CLI command	Description
<code>ike-version</code>	Specify the IKE protocol version, 1 or 2.
<code>keylife</code>	Specify the time (in seconds) to wait before the Phase-1 encryption key expires. The valid range is 20 –172800.
<code>proposal</code>	Specify Phase-1 proposal.
<code>Dhgrp</code>	Select one of the following DH groups: <ul style="list-style-type: none">• 1• 2• 5• 14
<code>*interface</code>	Use either of the following: <ul style="list-style-type: none">• <code>lo</code>• <code>eth1/lte1/lte2</code> Note: The names of the LTE interfaces vary depending on the hardware, as explained below: <ul style="list-style-type: none">• <code>eth1</code> (for FEX 40D-AMEU)• <code>lte1</code> (for FEX 201E and 211E)• <code>lte1</code> or <code>lte2</code> (for FEX 212E)
<code>type</code>	Select a remote gateway type: <ul style="list-style-type: none">• <code>static</code>• <code>ddns</code>
<code>*remote-gw</code>	Specify the IPv4 address of the remote gateway's external interface.
<code>*remotegw-ddns</code>	Specify the domain name of the remote gateway, e.g., <code>xyz.DDNS.com</code> .
<code>authmethod</code>	Select an authentication method: <ul style="list-style-type: none">• <code>psk</code> (pre-shared key)

CLI command	Description
	<ul style="list-style-type: none"> signature
*psksecret	Specify the pre-shared secret created when configuring the VPN client.
Localid	Specify the local ID.
peerid	Accept the peer ID.

A Phase-1 interface can be of two categories:

- A static remote VPN gateway with a fixed IP address.
- A DDNS with a dynamic IP address functioning as a dynamic DNS client.

A Phase-1 interface can support the following two authentication methods:

- psk (pre-shared key)
- signature

When a psk is configured, the psksecret must be configured as well. When signature is chosen, it uses the default Fortinet certs for authentication. Signature mode only supports FortiGate or FortiExtender as a remote gateway.

A tunnel interface is created in the system interface list when an IPsec Phase-1 is successfully created.

Parameter	Description
*phasename	The name of Phase-1 which determines the options required for Phase- 2.
proposal	Phase-2 proposal.
pfs	Select the option for the PFS feature: <ul style="list-style-type: none"> • enable • disable
Dhgrp	Phase-2 DH group.
keylife-type	Key life type.
keylifeseconds	Phase-2 key life time in seconds. The valid range is 120–172800.
encapsulation	ESP encapsulation mode
protocol	Quick mode protocol selector. The valid range is 1–255. 0 means for all.
src-subnet	Local proxy ID subnet.
src-port	Quick mode source port. The valid range is 1–65535. 0 means for all.
dst-subnet	Remote proxy ID subnet.
dst-port	Quick mode destination port. The valid range is 1–65535. 0 means for all.

Example VPN configuration:

```
FX201E5919002631 # config vpn
FX201E5919002631 (vpn) # config ipsec
FX201E5919002631 (ipsec) # config phase1-interface
FX201E5919002631 (phase1-interface) #
```

```

config phase1-interface
edit fcs-0-phase-1
    set ike-version 2
    set keylife 8000
    set proposal aes128-sha256 aes256-sha256 3des-sha256
    aes128-sha1 aes256-sha1 3des-sha1
    set dhgrp 14 5
    set interface eth1
    set type static
    set remote-gw 35.182.249.145
    set authmethod psk
    set psksecret HG709!ppA#d
    set localid FX04DA5918004527
    set peerid
next
edit fcs-1-phase-2
set phasename fcs-0-phase-1
    set proposal aes128-sha1 aes256-sha1 3des-sha1
    aes128-sha256 aes256-sha256 3des-sha256
    set pfs enable
    set dhgrp 14 5
    set keylife-type seconds
    set keylifeseconds 86400
    set encapsulation tunnel-mode
    set protocol 0
    set src-subnet 192.168.2.0/24
    set src-port 0
    set dst-subnet 0.0.0.0/0
    set dst-port 0
next
end

```

Check VPN tunnel status

Use the following command to check your VPN tunnel status:

```

get vpn IPSec tunnel details
fcs-1-phase-1: #2, ESTABLISHED, IKEv2, 94e21ce630f449a4_i*
07ca3af8b5fb4697_r
    local 'FX04DA5918004433' @ 100.64.126.36[4500]
    remote 'strongswan' @ 34.207.95.79[4500]
    AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_
    2048
    established 6850s ago, rekeying in 681s, reauth in
    78404s
fcs-1-phase-2: #2, reqid 2, INSTALLED, TUNNEL-in-UDP,
ESP:AES_CBC-128/HMAC_SHA1_96
    installed 6850s ago, rekeying in 72384s,
    expires in 88190s
    in cc6b72b7 (0x00000002), 704506 bytes, 6034
    packets
    out c3e9cb25 (0x00000002), 673016 bytes, 7407
    packets, 0s ago
    local 192.168.2.0/24

```

```
remote 0.0.0.0/0

fcs-0-phase-1: #1, ESTABLISHED, IKEv2, 89cdc38a8086b21c_i*
1b2ce8ba7f8d81b9_r
  local 'FX04DA5918004433' @ 100.64.126.36[4500]
  remote 'strongswan' @ 35.183.127.212[4500]
  AES_CBC-128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048
    established 6851s ago, rekeying in 1080s, reauth in 78536s
  fcs-0-phase-2: #1, reqid 1, INSTALLED, TUNNEL-in-UDP,
  ESP:AES_CBC-128/HMAC_SHA1_96
    installed 6851s ago, rekeying in 76423s, expires in
    88189s
    in c2b594fd (0x00000001), 6254187 bytes, 11489
    packets
    out c8a71b91 (0x00000001), 1015712 bytes, 10003
    packets, 0s ago
  local 192.168.2.0/24
  remote 0.0.0.0/0
```

SD-WAN

A Virtual-WAN interface is a virtual interface that aggregates multiple up-links. Traffic routed to it is load-balanced among all designated link members.

When operating with FortiExtender Cloud, you can add multiple member tunnels. The SD-WAN system interface is of the type of Virtual-WAN (vwan1) and can do link load-balancing (LLB) on top of the member interfaces. The SD-WAN function can be achieved by defining the health checks for the WAN interface, adding them to the Virtual-WAN interface, and then defining the attributes of the Virtual-WAN interface.

This section covers the following topics:

- [Configure an SD-WAN on page 40](#)
- [Check SD-WAN health on page 41](#)
- [Define an SD-WAN member on page 43](#)

Configure an SD-WAN

Use the following commands to configure an SD-WAN.

CLI command	Description
<code>config system interface</code>	Enters system interface configuration mode.
<code>edit <vwan_name></code>	Specify the name of the SD-WAN interface.
<code>set type virtual-wan</code>	Set the interface type to virtual-wan.
<code>set status <status></code>	Set the status of the interface: <ul style="list-style-type: none"> • <code>up</code>—Enable the interface. • <code>down</code>—Disable the interface.
<code>set persistence {source dest ip-pair connection}</code>	Select a LLB metric to denote how to distribute traffic: <ul style="list-style-type: none"> • <code>source</code>—Traffic from the same source IP is forwarded to the same target. • <code>dest</code>—Traffic to the same destination IP is forwarded to the same target. • <code>ip-pair</code>—Traffic from the same source IP and to the same destination IP is forwarded to the same target. • <code>connection</code>—Traffic with the same 5 tuples (i.e., a source IP address/port number, destination IP address/port number and the protocol) is forwarded to the same target
<code>set algorithm {redundant WRR}</code>	Select the LLB algorithm: <ul style="list-style-type: none"> • <code>redundant</code>—Targets work in primary-slave mode. • <code>WRR</code>—Targets work in Weighted Round Robin mode.
<code>Set grace-period</code>	Specify the grace period in seconds to delay fail-back.

CLI command	Description
<code>set session-timeout 60</code>	Specify the session timeout threshold in seconds. The default is 60. This is used to time out a VWAN session. A LLB session is created for each traffic stream. However, when a session times out, it is deleted.
<code>set members</code>	Add VWAN members to the VWAN interface.

FortiExtender supports both redundant and Weighted Round Robin (WRR) load-balanceing algorithms.

In redundant mode, the link member with the highest priority is selected as the primary member to forward packets. When the primary member is down, the member with the next highest priority is selected.

In WRR mode, traffic is sent to each link member in a round-robin fashion based on the weight assigned to it.

- **Weighted Round Robin (WRR)**—Traffic is load-balanced based on the weight configured on the underlying link member. The weight value should be based on the available bandwidth of the link member.
- **Redundant**—If the primary link (determined by priority) goes down, traffic is steered to the secondary link. In the above example, if the algorithm were set to redundant mode, the priorities of the member interfaces (i.e., tunnel0 and tunnel1) must be different. A link with the lowest priority setting gains the primary link status.

Unreliable links can cause bouncing between the primary and the secondary links. Therefore, a grace-period option is provided.

Use persistence to guarantee a specific traffic stream always goes through the same link member. This is useful for a group of traffic streams related to the same application, and there is a time sequence and dependency among them. In this case, a proper persistence should be configured. Current available options are `source_ip`, `dest_ip`, `source_dest_ip_pair`, and `connection`.

Check SD-WAN health

A `vwan_health_check` is for VWAN member status checking or health checking. Identify a server on the Internet and determine how the VWAN verifies that FortiExtender can communicate with it.

Parameter	Description
<code>set protocol {ping http dns}</code>	The protocol to be used for status check.
<code>set port</code>	The port number used to communicate with the server. The valid range is 1–65535. The default is 80.
<code>set http-get</code>	The URL used to communicate with the server. The default is /.
<code>set interval</code>	Specify the monitoring interval in seconds. The valid range is 1–3600. The default is 5.
<code>set probe_cnt</code>	Specify the number of probes sent within the set interval. The valid range is 1–10. The default is 1.

Parameter	Description
set probe_tm	Specify the timeout for a probe in seconds. The valid range is 1–10. The default is 2.
set probe_target	Specify the target to which probes are sent.
set src_iface	Specify the number of failures before the probe_target is considered lost. The valid range is 1–10. The default is 5.
recovery_cnt	Specify the number of successful responses received before the probe_target is considered recovered. The valid range is 1–10. The default is 5.

Example SD-WAN health check configuration:

The following commands are used to define a vwan_health_check and use it to perform health check for the VWAN member, member1.

```
config system
    config vwan_health_check
        edit vwchk1
            set protocol http
            set port 80
            set http-get /
            set interval 5
            set probe_cnt 1
            set probe_tm 2
            set probe_target www.google.com
            set src_iface nas1
            set fail_cnt 5
            set recovery_cnt 5
        next
    end
    config vwan_member
        edit member1
            set target target.member1
            set priority 1
            set weight 1
            set in-bandwidth-threshold 0
            set out-bandwidth-threshold 0
            set total-bandwidth-threshold 0
            set health-check vwchk1
        next
    end
end
```

You can use the “get hmon hchk vwan.<vwan_member_name>” command to show the latest statistics the system has captured.

For every round of measurement, HMON first sends several packets. It then sorts the different round-trip times, and selects the median.

The output shows the following values:

- avg, max, min, now—average, maximum, minimum, current median
- sd—standard deviation of the median
- am/s—ratio of the average median vs. the standard deviation

Example health check output

```
FX04DA5918000098 # get hmon hchk vwan.member1
median rtt:      avg      max      min      now      sd      am/s
eth1:  182.82ms  182.92ms  182.80ms  182.82ms  0.03ms  5414.7
packet loss:      avg      max      min      now
eth1:             0%      0%      0%      0%
```

Define an SD-WAN member

An SD-WAN link member is a target with a priority and weight clearly specified.

Use the following commands to define a link member.

CLI command	Description
<code>set target</code>	Specify the target to which traffic is forwarded.
<code>set health-check</code>	Specify the link health check of the VWAN.
<code>set priority</code>	Specify the priority of the link member. The valid range is 1–7.
<code>set weight</code>	Specify the weight of the member.

Example SD-WAN member configurations:

The following example shows the configuration for two members (`tunnel0` and `tunnel1`) on top of interfaces `fcs-0-phase-1` and `fcs-1-phase-1`, respectively, and prefixed with a target. The same can be attained over any available interface type.

```
config system vwan_member
edit tunnel0
set target target.fcs-0-phase-1
set priority 1
set weight 1
set in-bandwidth-threshold 0
set out-bandwidth-threshold 0
set total-bandwidth-threshold 0
set health-check vwchk1
next
edit tunnel1
set target target.fcs-1-phase-1
set priority 1
set weight 1
set in-bandwidth-threshold 0
set out-bandwidth-threshold 0
set total-bandwidth-threshold 0
set health-check vwchk1
next
end
```

Health monitoring

This section discusses how to monitor network interface status and perform health check on links. It covers the following topics:

- [Monitor interface status on page 44](#)
- [Perform link health check on page 45](#)
- [Configure health monitoring on page 47](#)

Monitor interface status

Use the following commands to configure traffic monitoring on an interface.

CLI Command	Description
<code>*set interface <interface_name></code>	Specify the interface to be monitored.
<code>set interval</code>	Specify the monitoring interval in seconds. The valid range is 1–3600. The default is 30.
<code>set filter {rx_bytes tx_bytes rx_packets tx_packets rx_dropped tx_dropped rx_bps tx_bps rx_pps tx_pps}</code>	Set the monitor filters on the interface: <ul style="list-style-type: none"> • rx_bytes—The number of bytes received. • tx_bytes—The number of bytes transmitted . • rx_packets—The number of packets received. • tx_packets—The number of packets transmitted. • rx_dropped—The number of incoming packets dropped. • tx_dropped—The number of outgoing packets dropped. • rx_bps—The number of bytes received per second. • tx_bps—The number of bytes transmitted per second. • rx_pps—The number of packets received per second. • tx_pps—The number of packets transmitted per second.

Example interface monitoring configuration:

```
config hmon interface-monitoring
  edit fcs-0-phase-1-mon
    set interval 30
    set interface fcs-0-phase-1
    set filter rx_bytes tx_bytes
  next
  edit fcs-1-phase-1-mon
    set interval 30
    set interface fcs-1-phase-1
    set filter rx_bytes tx_bytes
  next
  edit ifmon
    set interval 30
```

```

        set interface ltel
        set filter rx_bytes tx_bytes
    next
end

```

You can monitor the aforementioned configuration using the following commands:

```

X04DA5918004433 # get hmon interface-monitoring fcs-0-phase-1-
mon
                rx_bytes tx_bytes rx_packets tx_
packets rx_dropped tx_dropped rx_bps tx_bps
rx_pps tx_pps
fcs-0-phase-1: 12.76MB 3.40MB 24878 21032
0 0 488b 968b 0 0

X04DA5918004433 # get hmon interface-monitoring ifmon
                rx_bytes tx_bytes rx_packets tx_
packets rx_dropped tx_dropped rx_bps tx_bps
rx_pps tx_pps
ltel: 22.20MB 11.50MB 83137 72281
0 0 101.85Kb 21.14Kb 15 14
0

```

Perform link health check

Health checks can be performed on all types of links. The following example shows a health check configuration on top of two IPsec VPN links, “fcs-0-phase-1” and “fcs-1- phase-1”, respectively.

Use `hmon hchk` to send probes to a specific target to measure:

- The maximum, minimum, or average latency for a given period.
- The maximum, minimum, or average packet loss rate for a given period.
- The latency variation (jitter) for a given period.

Parameter	Descriptions
<code>set protocol {ping http dns}</code>	The protocol used for status check.
<code>set port</code>	The port number used to communicate with the server. Valid range is 1 - 65535. The default is 80.
<code>set http-get</code>	The URL used to communicate with the server. The default is /.
<code>*interface <interface_name></code>	The name of the interface.
<code>interval</code>	The monitoring interval in seconds. The valid range is 1–3600. The default is 5.
<code>probe_cnt</code>	The number of probes sent within the interval. The valid range is 1–10. The default is 1.

Parameter	Descriptions
probe_tm	The timeout for a probe in seconds. The valid range is 1–10. The default is 2.
*probe_target	The target to which a probe is sent.
src_iface	The source address derived from the specified interface.
filter {rtt loss}	Filter by <ul style="list-style-type: none"> rtt—Round Trip Time. loss—Packet loss.

Example health monitor health check configurations:

```

config hmon hchk
edit fcs-0-phase-1-chk
    set protocol ping
    set interval 10
    set probe_cnt 5
    set probe_tm 2
    set probe_target 34.207.95.79
    set interface fcs-0-phase-1
    set src_iface lan
    set filter loss rtt
next
edit fcs-1-phase-1-chk
    set protocol ping
    set interval 10
    set probe_cnt 5
    set probe_tm 2
    set probe_target 34.207.95.79
    set interface fcs-1-phase-1
    set src_iface lan
    set filter loss rtt
next
end

```

You can get the health check status for the above configurations using the following command:

```

FX04DA5918004433 # get hmon hchk fcs-0-phase-1
median rtt:      avg      max      min      now      sd      am/s
fcs-0-phase-1:  141.00ms 151.62ms 127.73ms 132.06ms 7.28ms  19.4
packet loss:      avg      max      min      now
fcs-0-phase-1:    0%      0%      0%      0%

FX04DA5918004433 # get hmon hchk fcs-1-phase-1
median rtt:      avg      max      min      now      sd      am/s
fcs-1-phase-1:  121.27ms 133.56ms 108.98ms 115.86ms 8.49ms  14.3
packet loss:      avg      max      min      now
fcs-1-phase-1:    0%      0%      0%      0%

```

Configure health monitoring



This feature applies to FEX-201E, FEX-202E, FEX-211E, and FEX-212E only.

Health Monitoring or HMON is commonly used for monitoring network and system health status, in addition to notifying subscribers of certain conditions which result in reporting collected statistics to FortiExtender cloud or FortiGate, respectively. One instance could involve data overage, another could be probing targets via ping or HTTP, and another could be checking link usability based on RTT or packet loss.

To configure interface monitoring:

```
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
```

To configure health check (which can be via ping, http,etc with specific intervals, timeouts and filters on any specific interface or interfaces):

```
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 interval 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
```

To display interface statistics with a pre-configured filter of choice:

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

To display health check statistics:

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

To run health check monitor to display all the interface statistics:

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

To run health check instance on a specific interface:

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


System management

This section discusses system management tasks. It covers the following topics:

- [Get system version on page 49](#)
- [Upgrade OS firmware on page 49](#)
- [Upgrade modem firmware on page 50](#)
- [SMS notification on page 51](#)

Get system version

Use the following command to find out your system version:

```
FX202E5919000011 # get system version
System version:
  image version      : FXT202E-v4.12-build400
  image type         : Interim
  model              : FortiExtender-202E
  MAC                : 04:d5:90:21:5f:c7
  SN                 : FX202E5919000011
  license            : ae30e2902fc1fe8f
  OEM SN             : FX202E5919000011
  REV                : 24258-01
  VERSION            : 00020003
  ROM REV            : FX202E
  Fallback image     : FXT202E-v4.12-build400
  Image type         : Interim
```

Upgrade OS firmware

You can upgrade FortiExtender OS firmware from FortiGate or FortiExtender Cloud. You can also upgrade the OS image directly using the FortiExtender CLI, or any of the following commands, depending on your circumstances:

TFTP

```
execute restore os-image tftp <image name> <tftp server IP address>
```

FTP

```
execute restore os-image ftp <image name> <ftp server IP address> <username>
<password>
```

USB

1. Configure the OS image name.

```
config system
    set hostname
    set auto-install-image enable
    set default-image-file <OS image name>
end
```

2. Insert the USB and reboot FortiExtender.

FortiExtender Cloud

Whether a FortiExtender is managed via FortiExtender Cloud, through FortiGate, or locally, you can always pull the OS image from the cloud to upgrade it.

1. Enter this command:

```
execute restore os-image cloud
```

The available OS images show on FortiExtender Cloud.

2. Select the appropriate option offered in the CLI.
FortiExtender automatically downloads the images.

GUI

1. From the navigation bar, click **Settings**.
2. On top of the page, click **Firmware**.
3. Select the desired OS firmware to upgrade.

Upgrade modem firmware

The FortiExtender modem firmware can't be upgraded from FortiGate. It must be upgraded from FortiExtender Cloud. The modem firmware is available as a downloadable package from the support site and can be upgraded directly from the FortiExtender CLI or by using the following commands, depending on your circumstances.

TFTP

```
execute restore modem-fw tftp <package name> <tftp server IP address>
```

FTP

```
execute restore modem-fw ftp <package name> <ftp server IP address>
<username> <password>
```

USB

```
execute restore modem-fw usb <modem package name>
```

FortiExtender Cloud

Whether your FortiExtender is managed via FortiExtender Cloud, through FortiGate, or locally, you can always pull the modem image from the FortiExtender Cloud onto the device.

1. Enter this command:

```
execute restore modem-fw cloud
```

The available modem images show on FortiExtender Cloud.
2. Select the appropriate option in the CLI.
FortiExtender automatically downloads the images.

GUI

1. From the navigation bar, click **Settings**.
2. On top of the page, click **Firmware**.
3. Select the desired modem firmware to upgrade.

SMS notification

All FEX-40D-AMEU, FEX-201E, FEX-202E, FEX-211E, and FEX-212 support Simple Message Service (SMS). This enables you to configure multiple mobile phone numbers on the FortiExtender to received SMS 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, format: +(country code) (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, format: +(country code) (phone number)>
        set alert <type of alerts i.e system-reboot,data-exhausted,session-disconnect,etc >
    next
end
```



The following are the types of alerts that are supported.

```
config system sms-notification alert
    set system-reboot system will reboot
    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 networking mode switched
    set fgt-backup-mode-switch FortiGate backup work mode switched
end
```

Remote diagnostics via SMS

FortiExtender supports remote diagnostics by SMS.

To enable remote diagnostics by SMS:

```
FX202E5919000011 # config system sms-remote-diag
FX202E5919000011 (sms-remote-diag) # show
config system sms-remote-diag
    set remote-diag enable
    config allowed-user
        edit user
            set sender disable
            set phone-number 5714515627
            set allowed-command-type factory-reset reboot get-system-status
        next
        edit user2
            set sender enable
            set phone-number 5714515627
            set allowed-command-type reboot get-modem-status get-extender-status
        next
    end
end
```

Export system logs to remote syslog servers



In order for FortiExtender to forward system logs to a remote syslog server, the syslog server and FortiExtender's LAN port must be part of the same subnet.

FortiExtender is able to forward system logs to remote syslog servers based on user configuration.

To enable exporting system logs to a remote syslog server:

```
FX202E5919000011 # config system syslog
FX202E5919000011 (syslog) # show
config system syslog
    set remote-server
    set remote-port 514
end
```

```
FX202E5919000011 (syslog) # set
remote-server      Remote Syslog server IP address
remote-port        Remote Syslog server port
```

Configure LTE settings

Typically, when deployed in the Cloud, FortiExtender is able to download its configuration from FortiExtender Cloud. However, you can still configure the device locally, using the commands below.



You must configure the APN, which can be done on FortiGate, FortiExtender Cloud, or locally.

Add a new carrier profile

To add a new carrier profile

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

Add a new operator/carrier

To add new operator/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
```

Set preferred carrier

To select a preferred carrier

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

Add a private network

To add a private network

```
edit Telus-plan
  set simid
  set carrier Telus
  set slot
  set apn sp.telus.com
  set mode
  set auth none
  set user
  set pwd
  set signal -100;600
  set capacity 6000
  set billing-date 1
  set overage disable
  set private-network enable
next
```



When "private network" is enabled, FortiExtender allows the flow of non-NAT'ed IP traffic on to an LTE interface. Otherwise, it does not.

Change default SIM

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

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

Enable SIM-switch

To enable SIM-switch

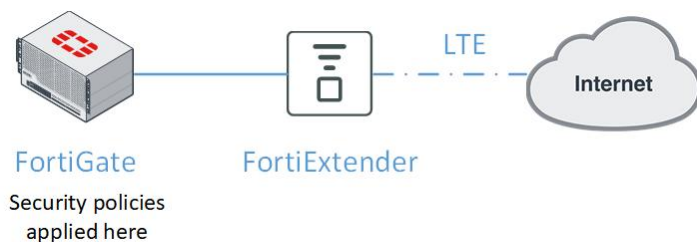
```
config lte setting
  set smart-switch enable
end
```

Use cases

This section discusses some typical use cases to deploy FortiExtender.

- [Extended cellular WAN of FortiGate on page 56](#)
- [Redundant with FGT in IP Pass-through mode on page 61](#)
- [Manage from FortiExtender Cloud on page 63](#)
- [FortiExtender 201E for FortiGate HA configuration](#)

Extended cellular WAN of FortiGate



Connect to FortiGate

1. Connect your FortiExtender LAN port to the POE-enabled port of FortiGate.
 - a. Enable the FortiExtender Controller on FortiGate.


```
# config system global
(global) # set fortiextender enable
(global) # end
```
 - b. Make sure that your FortiGate enables FortiExtender Controller.

The FortiExtender-related GUI is hidden by default. To enable it, go to **System > Feature Visibility**.
 - c. Enable the CAPWAP access to use the FortiGate interface to which FortiExtender is connected.

```
config system interface
edit lan
    append allowaccess fabric
end
```



The "append allowaccess fabric" command is introduced in FOS 6.2.3, and applies to FortiGate devices running FOS 6.2.3 and later. If you are connecting your FortiExtender to a pre-FortiOS 6.2.3 FortiGate device, you **MUST** use "append allowaccess capwap" instead.


2. Authorize the FortiExtender device.



Once the FortiExtender is discovered, you must authorize it by associating it either with a virtual WAN interface or a VLAN interface.

- a. Go to **Network > FortiExtender**, and wait for the FortiExtender device to be discovered by FortiGate.
- b. Bind the device to an interface and authorize it.
In FortiGate 5.4 and higher releases, you must manually create either a virtual WAN interface of type FEX-WAN or a VLAN sub-interface, and link it to FortiExtender as part of the authorization process, as illustrated below.

Secondary

Serial Number FX04DA5918009600

Status Deauthorized 

Interface Name  fext-wan1 

Authorize

Delete



Make sure that FortiExtender and FortiGate are connected on Layer 2 by default. If they are not connected via Layer 2 but can reach each other via Layer-3 networking, configure your FortiExtender with static discovery using the following FortiExtender CLI commands:

```
config system management fortigate
    set ac-discovery-type static
    set static-ac-ip-addr 192.168.1.99
    set ac-ctl-port 5246
    set ac-data-port 25246
end
```

VLAN mode and performance

While using the FEX-WAN type interface, all the traffic to/from FortiGate is encapsulated in the CAPWAP data channel, whereas for VLAN type interface, the traffic is sent/received on the VLAN interface. Due to absence of encapsulation overheads, VLAN mode delivers better speeds with the requirement that the VLAN interface be directly created on top of the port on which FortiExtender is connected to FortiGate.



Note that VLAN mode must be explicitly enabled, as it is disabled by default on FortiGate, and that all the FEX-WAN interfaces must be deleted before VLAN mode is enabled.

```
#config system global
(global) # set fortiextender-vlan-mode enable
(global) # end
```

Ensure that the VLAN interface is created based on the physical interface of your connected FortiExtender.

Modem connectivity

FortiExtender allows for multiple modes of operation of the modem from FortiGate.

- **Always Connect**—By default, this feature is enabled when a FortiExtender is authorized. In this mode, the modem is always connected to the Internet, meaning that the FortiExtender is readily available for Internet access from the FortiGate. If there are multiple active WAN interfaces on the FortiGate, care must be taken to ensure that the distances of the FortiExtender interface and other WAN interfaces are configured appropriately. The FortiExtender's modem is always connected to the Internet. It can be a primary or backup method of connecting to the Internet for the FortiGate.
- **On Demand**—In this mode, FortiExtender instructs the modem to connect to an ISP for Internet access only upon executing the dial-up command and disconnects only upon a subsequent hang-up command from the FortiGate CLI.

To connect

```
execute extender dial <SN>
// <SN> is the FortiExtender's serial number.
```

To disconnect

```
execute extender hangup <SN>
// <SN> is the FortiExtender's serial number.
```

Dual FortiExtender operations

Active/Passive mode

By default, each FortiGate device can support up to two FortiExtenders at a time. Typically, the first FortiExtender that it has authorized takes the primary role and the second one takes the secondary role. The primary FortiExtender always provides Internet access and the secondary FortiExtender stays in passive mode. If the primary FortiExtender goes down, the secondary FortiExtender gets activated, and vice versa.

Active/Active mode

To have access to active Internet sessions on both FortiExtenders simultaneously, the role of the secondary FortiExtender needs to be changed to primary.

```
config extender-controller extender
  edit < fext serial no > /* FortiExtender with secondary
    role */
    set role primary
end
```

Cellular as backup of Ethernet WAN

In this redundant mode of operation, the FortiExtender daemon running on FortiGate monitors a given WAN link on the FortiGate, and brings up FortiExtender's cellular Internet access when the WAN link is down and brings down the FortiExtender cellular Internet when the WAN link comes up. For example:

```
config extender-controller extender
    edit <FEXT serial number>
        set admin enable
        set ifname <fext interface>
        set mode redundant
        set redundant-intf < wan interface I,e wan1>
    end
```

In this mode of operation, the FortiExtender interface comes up if the WAN interface goes down and goes down if the WAN interface comes up.

ECMP across FEX-wan1 and wan1

To set up Equal-cost multi-path routing (ECMP) to automatically find the best path:

1. On the FortiGate UI, go to **Router > Static > Settings**, and do the following:
 - a. Configure ECMP Load Balancing Method.
 - b. Choose among Source IP based, Weighted Load Balance, Spillover, Source-Destination IP based, and
 - c. Configure your settings as required.
2. Go to **System > Network > Interfaces** and edit FEX-wan1, setting the distance to the same distance as the wan1 interface under **Router > Static > Static Routes**. (In this example, the distance is 10.)

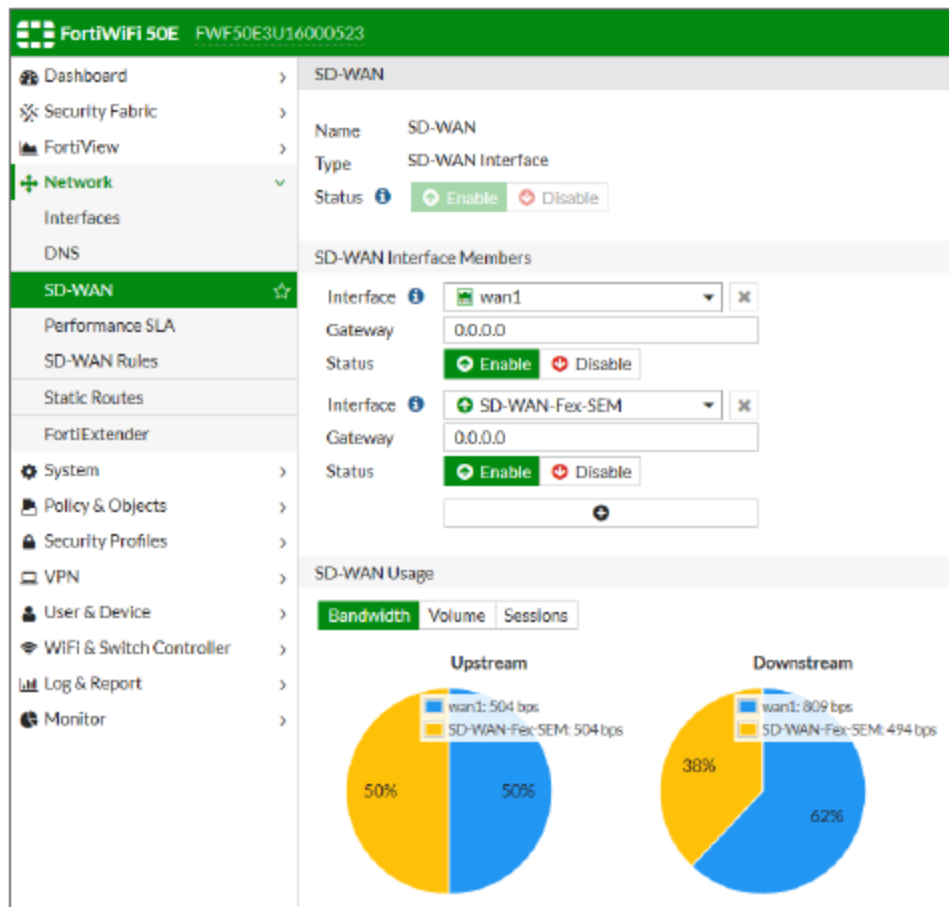
Now the traffic is shared between the wan1 and FEX-wan1 links according to the ECMP Load Balancing Method used. This deployment can be extrapolated for dual FortiExtender installation.

SD-WAN in FortiOS 5.6 and higher

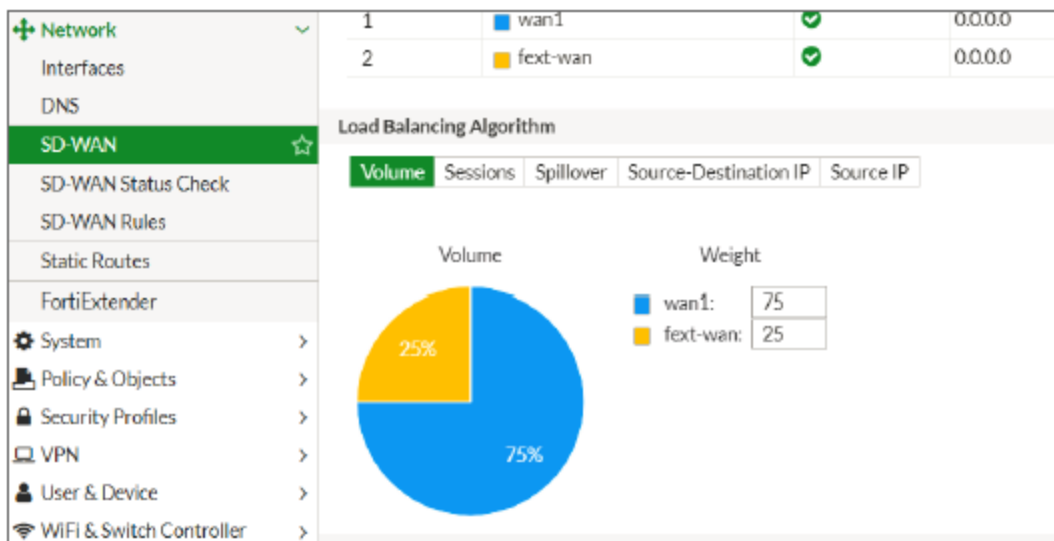
FortiOS now recognizes and uses FEX as a valid interface within an SD-WAN interface bundle. Using SD-WAN, FortiGate becomes a WAN path controller and supports diverse connectivity methods. With FEX, 3G/4G can be used as a primary connection, a backup interface, or a load-balanced WAN access method with Application-Aware WAN path control selection. It provides high availability and QoS for business-critical applications by using the best effort access for low-priority applications through low-cost links, and backs up service through associations with an FEX link. This enables aggregation of multiple interfaces into a single SD-WAN interface using a single policy.

To accomplish this:

1. Add the FortiExtender interface as a member of the SD-WAN interface, as illustrated below.



2. Define a load-balancing algorithm, as shown in the following example of volume-based distribution.



3. Define your policies for the whole bundle (but not per interface) as illustrated below.

The screenshot shows the FortiGate configuration interface for a FortiGate 600-POE. The 'Policy & Objects' tab is selected, and a policy named 'SDWAN_Out' is being configured. The policy is set to 'ACCEPT' and 'Enabled'. The source is 'all' and the destination is 'all'. The action is 'ACCEPT' and the security profile is 'UTM'. The policy is associated with the 'SD-WAN' interface pair. The table below shows the policy configuration details.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	SDWAN_Out	all	all	always	ALL	ACCEPT	Enabled	UTM		197.93 MB
	Implicit	all	all	always	ALL	DENY	Disabled			0B

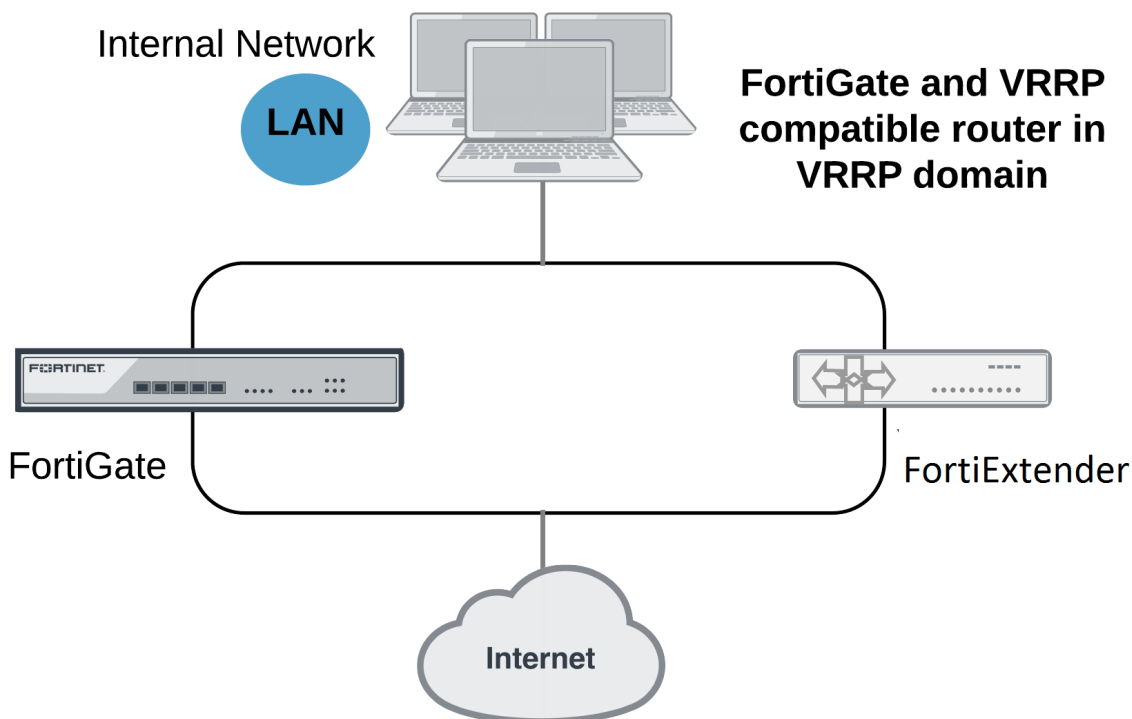
For more information about how to deploy SD-WAN in general, refer to FortiOS documentation.

Redundant with FGT in IP Pass-through mode



This feature applies to FEX-201E, FEX-202E, FEX-211E, and FEX-212E only.

A Virtual Router Redundancy Protocol (VRRP) configuration can be used as a high-availability (HA) solution to ensure network connectivity in the event the default router for the network fails. With VRRP, If a router or FortiGate on your network fails, all traffic will transparently fail over to another router or FortiGate. When the failed router or FortiGate is restored, it will once again take over processing traffic for the network. For more information about VRRP, see [RFC 3768](#).



The most common application of VRRP is to provide redundant default routers between an internal network and the internet. The default routers can be FortiGates and or any routers like FortiExtenders that support VRRP.

General configuration procedures

1. Add a virtual VRRP router to the internal interface of each of the FortiGates and FortiExtender. This adds the FortiGate and FortiExtender to the same VRRP domain.
2. Set the VRRP IP address of the domain to the internal network default gateway IP address.
3. Give one of the VRRP domain members the highest priority so it becomes the primary (or master) router and give the others lower priorities (such as FortiExtender) so they become backup routers.

In normal operations, all traffic from the internal network to the internet passes through the primary VRRP router, i.e., FortiGate. The primary router also sends VRRP advertisement messages to the backup router, i.e., FortiExtender. The backup FortiExtender will not attempt to become a primary router while receiving these messages. If the primary router fails, the backup FortiExtender with the highest priority becomes the new primary router after a brief delay, during which the new primary router sends gratuitous ARP packets to the network to map the default route IP address of the network to the MAC address of the new primary router. All packets sent to the default route are now being sent to the new primary router, i.e., FortiExtender. If the new primary router is a FortiGate, the network will continue to benefit from FortiOS security features. If it is a regular router, traffic will continue to flow, but the FortiOS security features will not be available until the FortiGate is back online.

During a VRRP failover with a FortiGate as the backup router, the FortiGate will not have session information for all of the failed-over in-progress sessions. So it would normally not be able to forward in-progress session traffic. To solve this issue, the FortiGate acting as the new primary router will operate with asymmetric routing enabled immediately after a failover and for a short time (called the start time). This enables the FortiGate to re-create all of the in-progress sessions and add them to its session table.

While operating with asymmetric routing enabled, the FortiGate cannot apply security functions. When the start time ends, the FortiGate disables asymmetric routing and returns to normal operation (including applying security functions).

To enable VRRP on the interface attached to the LAN port on FortiGate:

```
FortiOS# config system interface
FortiOS (interface) # edit <port num>
    edit <port num>
        set vdom "root"
        set ip <ip> <subnet mask>
        set allowaccess ping
        set type physical
        set vrrp-virtual-mac enable
        config vrrp
            edit <vrrp id>
                set vrip <vrrp IP>
                set priority <priority>
            next
        end
    end
end
```

To enable VRRP on FortiExtender:

```

config system management
set discovery-type fortigate
    config fortigate-backup
        vrrp-interface <vrrp interface i.e por1>
        status enable
    end
end

config system interface wan vrrp
set status enable
set version 2 <only 2 is supported currently>
set ip <IP of virtual router>
set id <vrrp id>
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)
end

```

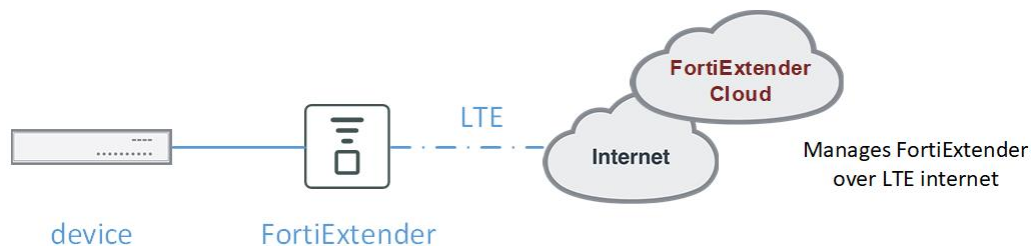


The VRRP interfaces on FortiGate and FortiExtender must be individual ports, and must not be part of a LAN switch with static IP address configuration. Devices reliant on the Internet from FortiGate or FortiExtender must also have a static IP configured.

To display the status of virtual router on FortiExtender:

```
get router info vrrp
```

Manage from FortiExtender Cloud



To manage FortiExtender from FortiExtender Cloud, you must have the following:

- A FortiCare or FortiGate account
- A FortiCloud key



You can find your FortiCloud key on the sticker on the front of your FortiExtender device.

Configure with FortiExtender Cloud

Refer to the FortiExtender Cloud [Admin Guide](#) for instructions on how to

- Access FortiExtender Cloud.
- Deploy FortiExtender devices.
- Synchronize devices.

IP Pass-through mode with Cloud management

1. On FortiExtender Cloud, configure a profile in IP pass-through mode.

profile1

General Settings
Set general configuration settings.

Smart Switch ☐ ON ☒ OFF
SIM Smart Switch.

Report Interval
Device statistics report interval(30-480).

Work Mode ☐ NAT ☒ IP Pass
Device work mode.

Plans
Remove plans from this profile, add more plans to it or drag a plan to change the order.

Add Plan

2. Connect the FortiExtender LAN port to the WAN port of FortiGate or a third-party appliance.



If the WAN port is not POE-enabled, use a power injector (12V/1A) to power the FortiExtender device.

3. Set the WAN port of FortiGate or a third-party appliance to DHCP mode. The device will get an IP address from the ISP and connect to the Internet.

NAT mode with Cloud management

1. Configure a profile in NAT mode. Refer to Step 1 in the preceding section.
2. Use the following commands to complete the configurations:

Address

```
config network address
  edit all
    set type ipmask
    set subnet 0.0.0.0/0
  next
  edit none
    set type ipmask
    set subnet 0.0.0.0/32
  next
  edit src
    set type ipmask
    set subnet 192.168.2.0/24
  next
end
```

Firewall policies

```
config firewall policy
  edit all-pass
    set srcintf
    set dstintf
    set srcaddr src
    set dstaddr all
    set action accept
    set status enable
    set service
    set nat enable
  next
end
```

Policy-based routing (PBR)

```
config router
  config policy
    edit eth1-pbr
      set input-device
      set src 192.168.2.0/24
      set srcaddr
      set dst
```

```
        set dstaddr
        set service
        set target target.eth1
        set status enable
        set comment
    next
end
```

OBM management

FortiExtender can be connected to the console port of any device behind it via its USB port, thereby enabling out-of-band management (OBM). This mode requires access to FortiExtender over its WAN interface.

This feature supports multiple OBM console connections with USB to multiple serial console cable/adaptor. Once you've logged into FortiExtender, you can access its console port using the following procedures:

1. Log into the FortiExtender device.
2. Connect to the console port of the device.
3. Execute the command:

```
# execute obm-console
Welcome to OBM Console - Serial Redirector.
One device connected with ttyUSB0.
Please choose the baudrate from list below:
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
6. 921600
7. Other baudrate
Enter to continue & CTRL+X to go back to FortiExtender Console.
```

When USB to multiple serial console cable/adaptor is used, execute the following command:

```
# execute obm-console
Welcome to OBM Console - Serial Redirector.
There are 2 devices/ports connected.
Please choose one from list below:
1. ttyUSB0
2. ttyUSB1
Please choose the baudrate from list below:
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
6. 921600
7. Other baudrate
Enter to continue & CTRL+X to go back to FortiExtender Console.
```

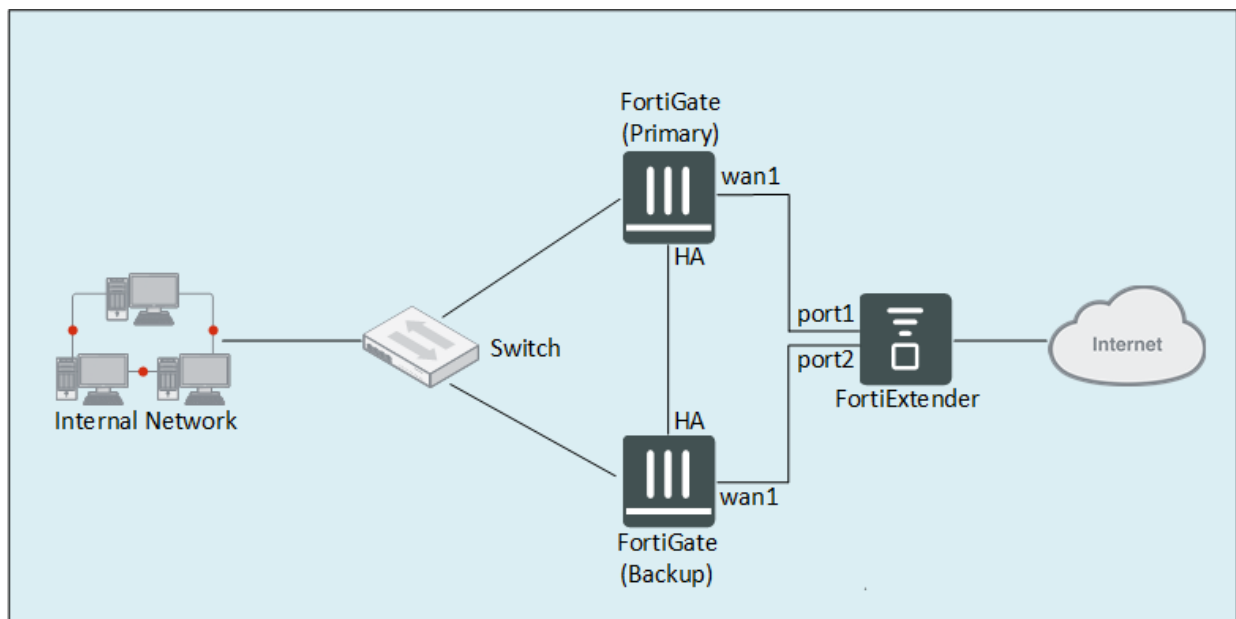


Make sure that the baud rate you select matches the baud rate of the router which is connected to the serial console via the USB port.

FEX-201E for FortiGate HA configuration

This use case discusses how to use a FortiExtender 201E to support two FortiGate devices in HA configuration to ensure uninterrupted network connectivity and business continuity. It provides step-by-step instructions on how to configure the FortiGate HA cluster from the FortiGate GUI. It also provides the FortiExtender CLI commands to verify the port configuration of FortiExtender 201E as a WAN switch to support the FortiGate HA configuration.

Network topology



Prerequisites

- The FortiExtender 201E device must be physically networked with the two FortiGate devices, with its Port 1 connected to wan1 on the primary FortiGate and Port 2 connected to wan1 on the backup FortiGate, as illustrated in the Network topology.
- The two FortiGate devices must be physically connected via the HA port on both of them, as illustrated in the Network topology.
- The two FortiGate devices must be running the same version of FOS.



The FortiGate devices used in this sample configuration are both running FOS 6.2.1.

Configuration procedures

This configuration involves the following major steps:

Step 1: Configure the primary FortiGate

1. Log in to the GUI of the primary FortiGate device.
2. From the menu, go to **Dashboard > Status**.
The **Status** page opens.
3. Locate the **System Information** widget, click the **Hostname**, and (from the drop-down menu) select the **Configure settings in System > Settings** link.
The **System Settings** page opens.
4. Change the **Host name** to something that identifies the FortiGate as the primary device, and click **Apply**.
5. Then, select **System > HA**, click the top part of the page to highlight it, and click **Edit**.
The **High Availability** page opens.



The **Edit** button will not be available until the top part of the Status page is highlighted.

6. Make the following required entries and/or selections:
 - a. Change **Mode** to **Active-Passive**.
 - b. Set **Device Priority** to a value greater than the one set on the backup FortiGate.
 - c. Specify a **Group name**.
 - d. Set the **Password**.
 - e. Select two **Heartbeat interfaces** (one at a time) by doing the following:
 - i. Click **+** (plus sign), and (from the pop-up list of interfaces) select **ha**.
 - ii. Set **Heartbeat Interface Priority** to 50.
 - iii. Click **OK**.
 - iv. Click **+** (plus sign) again, and (from the pop-up list of interfaces) select **wan1**.
 - v. Set **Heartbeat Interface Priority** to 50.
 - vi. Click **OK**.

Step 2: Configure the backup FortiGate

1. Log in to the GUI of the backup FortiGate device.
2. From the menu, go to **Dashboard > Status**.
The **Status** page opens.
3. Locate the **System Information** widget, click the **Hostname**, and (from the drop-down menu) select the **Configure settings in System > Settings** link.
The **System Settings** page opens.
4. Change the **Host name** to something that identifies the FortiGate as the backup device, and click **Apply**.
5. Then, select **System > HA**, click the top part of the page to highlight it, and click **Edit**.
The **High Availability** page opens.



The **Edit** button will not be available until the top part of the Status page is highlighted.

6. Make the following required entries and/or selections:
 - a. Change **Mode** to **Active-Passive**.
 - b. Set the **Device Priority** value smaller than the one set for the primary FortiGate.
 - c. Set the **Group name** to be the same as the one set on the primary FortiGate.
 - d. Set the **Password** to be the same as the one set on the primary FortiGate.
 - e. Select two **Heartbeat interfaces** (one at a time) by doing the following:
 - i. Click **+** (plus sign), and (from the pop-up list of interfaces) select **ha**.
 - ii. Set **Heartbeat Interface Priority** to 50.
 - iii. Click **OK**.
 - iv. Click **+** (plus sign) again, and (from the pop-up list of interfaces) select **wan1**.
 - v. Set **Heartbeat Interface Priority** to 50.
 - vi. Click **OK**.



- Ensure that the Device Priority value on the primary FortiGate is higher than the one for the backup FortiGate.
- Ensure that two heartbeat interfaces are selected and the Heartbeat Interface Priority are both set to 50 on both.

Step 3: Verify the port settings on FortiExtender

1. Ensure that Port 1 on the back of the FortiExtender is connected to the WAN1 port on the primary FortiGate. Refer to the Network topology.
2. Ensure that Port 2 on the back of the FortiExtender is connected to the WAN1 port on the backup FortiGate. Refer to the Network topology.
3. Run the following commands to verify and ensure that the physical Ports 1 and 2 are aggregated in the LAN switch port.

```
FX202E5919000011 # config system interface
FX202E5919000011 (interface) # edit lan
FX202E5919000011 (lan) # show
edit lan
    set type lan-switch
    set status up
    set mode dhcp
    set mtu 1500
    set vrrp-virtual-mac enable
    config vrrp
        set status disable
    end
    set allowaccess http https ssh ping telnet capwap
next

FX202E5919000011 # config system lan-switch
FX202E5919000011 (lan-switch) # show
config system lan-switch
    config ports
        edit port1
        next
        edit port2
```

```
    next
    edit port3
    next
    edit port4
    next
end
end
```



The "show" commands above yield the default settings of FortiExtender 201E as a LAN switch, which can be used out of the box to support FortiGate HA configurations. We recommend using these settings without change unless you are confident in your ability to configure custom settings of your own. If you prefer to configure your own LAN switch, be sure to use the aforementioned commands to double-check its configuration before putting FortiExtender to work.

Troubleshooting, diagnostics, and debugging

This section discusses system troubleshooting, diagnostics, and debugging. It covers the following topics:

- [Troubleshooting on page 71](#)
- [Status, diagnostics, and debugging commands on page 72](#)
- [Diagnose FortiExtender on page 72](#)

Troubleshooting

Below are some common error situations with their suggested solutions.

Can't detect FortiExtender on FortiGate

If you can't detect FortiExtender on a FortiGate with OS versions 5.6.3 or higher, upgrade the FortiExtender to OS version 3.2.2 or higher. (FortiExtender-40D-AMEU only.)

Can't manage the FortiExtender from FortiExtender Cloud

Upgrade the FortiExtender to OS version 3.3.0 or higher.

Can't start an Internet session

1. Type `execute debug-mode ati` to enter debug mode.
2. Troubleshoot in the following sequence:

Step	Task	CLI command to use
1	Check the SIM card If the SIM is accessible, output the SIM IMSI number, for example, 311480420284429. If the SIM can't be read, reinsert it into the SIM slot until it clicks into place.	AT+CIMI
2	Check the modem firmware compatibility The current firmware and the preferred firmware for the inserted SIM card must be the same, or else the output will indicate a mismatch error.	AT!IMPREF? AT!GOBIIMPREF?
3	Check the signal availability Ensure that the FortiExtender has good signal strength to derive good speeds and prevent time-outs.	AT!GSTATUS?

Step	Task	CLI command to use
4	Check Internet connectivity Check to see if the APN is configured correctly. Although the modem in FortiExtender can negotiate the APN, it might run into issues with some wireless providers.	AT+CGDCONT?

Status, diagnostics, and debugging commands

FortiExtender supports the following CLI commands for system status checking, diagnostics, and debugging.

Task	CLI command/action
Check connectivity to FortiGate	<code>get extender status</code>
Check connectivity to FortiExtenderCloud	<code>get cpm status</code>
Check the status of modems	<code>get modem status</code>
Perform health checks and monitoring	<code>get hmon hchk vwan.<vwan_member name></code> (The member can be tunnel0 or tunnel1.)
Perform modularized debugging	<ol style="list-style-type: none"> 1. Select the module. 2. Turn the log level on/off as needed.
Debug	<code>execute debug <module> <log level> on/off</code>
Logs on telnet/ssh	<code>execute debug log-to-console on</code>
	SYSTEM, MONITOR, EXTD, MDMD, CONNMGR, NETD, CLI, GUI, CPM, CONFIG, JCLI, HMON, IPSEC, FIREWALLD
Applicable log levels	<code>error, info, dbg, fatal, warning, trace</code>
Packet tracing	Start the tcpdump utility from the shell prompt using the command <code>execute shell</code> .

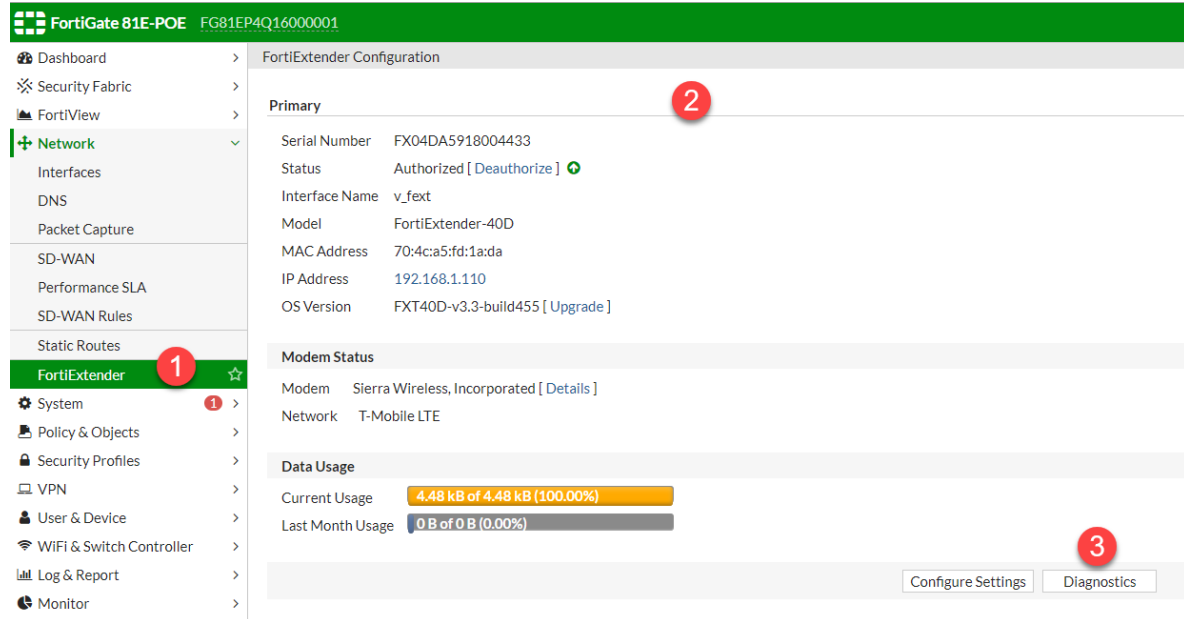
Diagnose FortiExtender

You can diagnose your FortiExtender device using any of the following methods:

- From FortiGate
- From FortiExtender Cloud
- From Telnet.

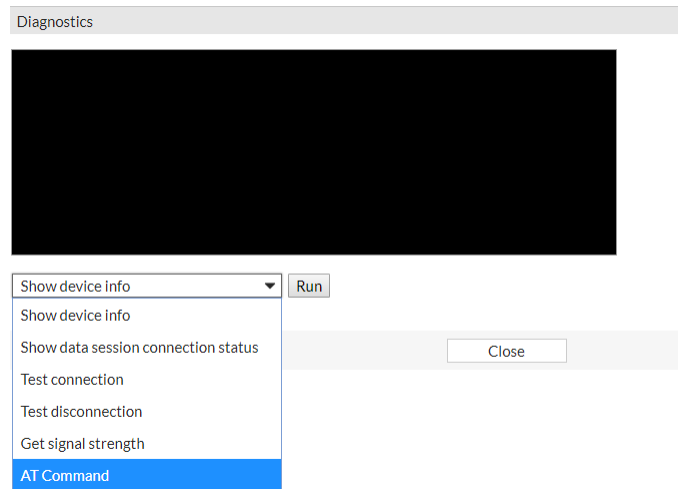
Diagnose from FortiGate

1. Connect your computer directly to the FortiGate's console port.
2. Open a browser to access the FortiGate GUI.
3. From the main FortiGate window, go to **Network > FortiExtender**, as illustrated below.

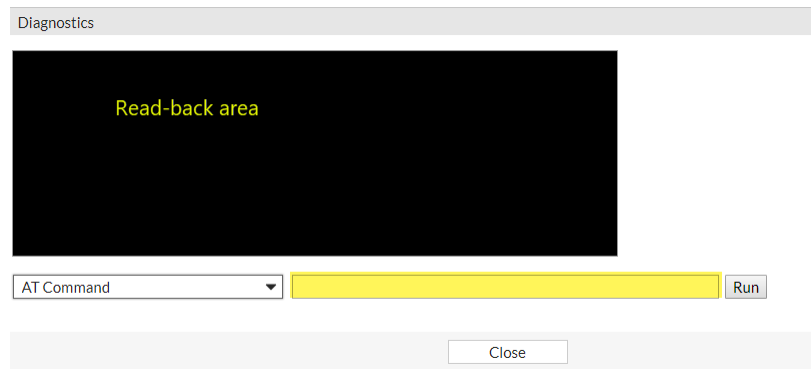


If the FortiExtender is running correctly, the modem status and data usage statistics appear.

4. Click **Diagnostics** to open the Diagnostics window.



5. Click the down arrow, and from the drop-down menu, click **AT Command**. The command text box opens.



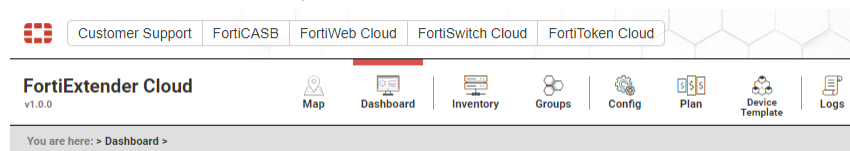
6. Type a command into the text box, and click **Run**.
The output shows in the read-back area.



For a complete list of diagnostic commands, refer to [Status, diagnostics, and debugging commands on page 72](#).

Diagnose from FortiExtender Cloud

1. From FortiExtender Cloud, click **Dashboard**.



2. On the Dashboard page, click the FortiExtender device of interest.
The device page opens.
3. Click **Console**.
The Console Editor opens. You are now communicating directly with the modem.
4. Type `execute debug-mode ati` to enter debug mode.
5. Type a debug command.
A message is returned showing the status of the modem.



For a complete list of diagnostic commands, refer to [Status, diagnostics, and debugging commands on page 72](#).

Diagnose from Telnet

1. From the Windows Command prompt, type `cmd`.
2. Type `telnet [modem ip address]`. (The default IP address is 192.168.1.2.)
3. Enter your user name and password as required.
4. Enter the command you want.



For a complete list of diagnostic commands, refer to [Status, diagnostics, and debugging commands on page 72](#).

Collect complete diagnostics information

FortiExtender now supports collecting all diagnostics information in a compressed package. The package contains all details, including system software, hardware, configuration, CPU usage, memory usage, modem status, interfaces, routing tables, IP tables, VPN, session tables, and kernel logs.

Use the following command to collect all diagnostics information:

```
execute debuginfo export tftp <filename.tgz> <tftp server ip address>
```

Change Log

Date	Change Description
September 16, 2020	Third update, replacing the content in "OBM Management".
March 26, 2020	Second update, correcting errors in the VPN configuration section.
February 12, 2020	First update, adding "FortiExtender 201E for FortiGate HA configuration" to "Use Cases".
October 31, 2019	Initial release.



Copyright© 2021 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.