FortiExtender - Admin Guide

Version 4.2.1

September 16, 2020
FortiExtender 4.2.1 Admin Guide

TABLE OF CONTENTS

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.

- This Admin Guide applies to FortiExtender OS version 4.2.1 and later.

Network topologies

FortiExtender FEX-201E and FEX-211E come with four LAN Ethernet ports and one WAN Ethernet port. 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.

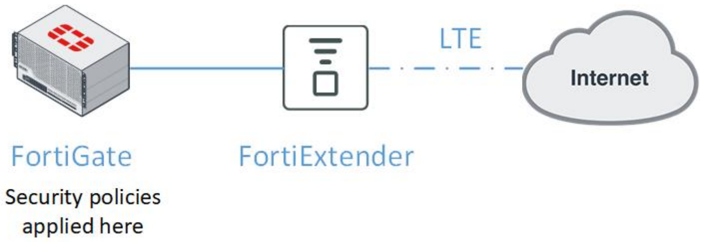
The following paragraphs highlight the network topologies for the three common use cases for FortiExtender:

- 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.

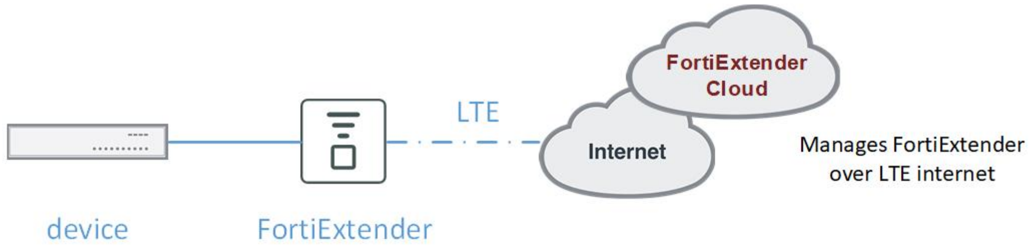
In this scenario, FortiGate manages FortiExtender over the Control and Provisioning of Wireless Access Points (CAPWAP) protocol in IP pass-through mode. Unlike a stand-alone 3G/4G wireless WAN extender, FortiExtender integrates directly into the FortiGate Connected UTM (Unified Threat Management) and 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 in Active-Passive, and two FortiExtenders to two FortiGate devices in Active-Active deployments, providing dual active redundancy for wireless WAN access as well.

Deployed on FortiExtender Cloud

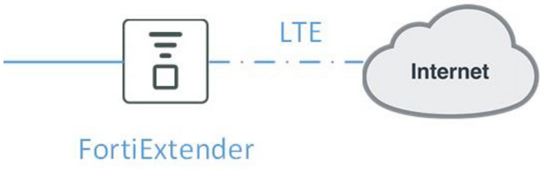
FortiExtender Cloud offers hosted management for an unlimited number of FortiExtender devices deployed anywhere around the globe in either IP pass-through or NAT mode.



FortiExtender Cloud provides hosted management of up to three FortiExtender devices free of charge to each of its registered customers on FortiCare. To take full advantage of this offering, you must purchase a FortiExtender Cloud license for every additional 10 FortiExtender devices to be hosted on FortiExtender Cloud. 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. You can configure locally on the device itself either from the Console or the GUI. A locally managed FortiExtender 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
- CAPWAP on multiple ports for broadcast discovery on page 14
- Stopping data traffic on overgaged LTE interface on page 15

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

Supported hardware models

Model	Market
FEX-201E	Americas and Europe
FEX-211E	Global coverage

FortiExtender 201E and 211E devices come with a Bluetooth button, which is off by default. However, when it is turned on, anyone can access the devices via Bluetooth. To safeguard your network, we strongly recommend setting passwords for all your devices before deploying them in your environment.

Cellular capabilities

FortiExtender 201E uses 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

FortiExtender 211E uses 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, including the following:

Region	Carrier
Europe	• A1MobilKom • Bouygues • O2 • Orange • SFR • Swisscom • T-Mobile • Vodafone
North America	• 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_02.32.11.00.cwe
   set pri SWI9X30C_02.32.11.00_GENERIC_002.064_000.nvu
next
```

FortiExtender also supports other wireless carriers in other parts of the world, depending on the technology and bands used, sometimes requiring specific configuration such as APN, but mostly using the generic modem firmware (see below). 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:

```
FX201E5919000035 # config lte simmap
FX201E5919000035 (simmap) # show
config lte simmap
end

FX201E5919000035 (simmap) # edit 1
FX201E5919000035 (1) <M> # set mcc 332
FX201E5919000035 (1) <M> # set mnc 321

FX201E5919000035 (1) <M> # set carrier

FX201E5919000035 (1) <M> # next
```

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, which is retrieved automatically at first connection from FortiExtender. 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 modem all
    set type by-default
    set apn <carrier apn>
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

SIM-switching can be configured by data plan, disconnect settings, signal strength, coupled with switch back by time or by timer. All these options are under the renamed “Auto switch” setting.

FortiExtender comes with two SIM-card slots per modem, with the first one (i.e., sim1) being the default. SIM-switch works only when you have two SIM cards installed on a FortiExtender device with the feature enabled on it. SIM-switch is disabled by default, you can enable it using the following commands:

```
config auto-switch
   set by-disconnect disable
   set by-signal disable
   set by-data-plan disable
   set switch-back
end
```

With SIM-switch enabled, 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
   config auto-switch
      set by-disconnect enable /*enable the switch by disconnect feature*/
      set disconnect-threshold <3> /*Number of disconnects for sim-switch*/
      set disconnect-period <600> /*Disconnect evaluation period for simswitch*/
   end
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 setting modem1
   config auto-switch
         set by-signal enable /*enable the switch by signal feature*/
         set by-data-plan enable /*enable the switch by data usage feature*/
   end
end
config lte plan
   edit <plan>
      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.

RSSI Values and LED State

RSSI	LED-1	LED-2	LED-3	LED-4
0, or N/A, or 'rssi<=-100'	OFF	OFF	OFF	OFF
-90~-81	ON	OFF	OFF	OFF
-80~-71	ON	ON	OFF	OFF
-70~-61	ON	ON	ON	OFF
rssi>=-60	ON	ON	ON	ON

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:

```
FX211E5919000006 (auto-switch) # show
      config lte setting modem1 auto-switch
         set switch-back [by-time | by-timer]
      end
```

Parameter	Description
`by-time`	Switch over to the preferred SIM card/carrier at a specified (UTC) time (in the format of HH:MM).
`by-timer`	Switch over to the preferred SIM/carrier after the given time (from 3600 to 2147483647 seconds).

Get modem status

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

```
X201E5919002499 # get modem status
Modem status:
```

```
modem             : Modem1
usb path          : 2-1.2 (sdk 0)
vender            : Sierra Wireless, Incorporated
product           : Sierra Wireless, Incorporated
model             : EM7455
SIM slot          : SIM1
revision          : SWI9X30C_02.32.11.00 r8042 CARMD-EV-FRMWR2 2019/05/15 21:52:20
imei              : 359073065340568
iccid             : 8933270100000296108
imsi              : 208270100029610
pin status        : enable
pin code          : 0000
carrier           : 436627|coriolis|EU
APN               : N/A
service           : LTE
sim pin (sim1)    : 3 attempts left
sim puk (sim1)    : 10 attempts left
rssi (dBm)        : -68
signal_strength   : 64
ca state          : ACTIVE
cell ID           : 00A25703
band              : B7
band width        : 20
sinr (dB )        : 7.4
rsrp (dBm)        : -99
rsrq (dB )        : -13.1
plan_name         : coriolis100G
connect_status    : CONN_STATE_CONNECTED
reconnect count   : 0
smart sim switch  : disabled
up time (sec)     : 26670
clock (UTC)       : 20/05/27,20:08:33+08
temperature       : 60
activation_status : N/A
roaming_status    : N/A
Latitude          : 37.376281
Longitude         : -122.010817
```

CAPWAP on multiple ports for broadcast discovery

Starting from Version 4.2.1, FortiExtender is able to discover FortiGate on multiple interfaces. It sends discovery messages on multiple ports (port1, port2, and port3, and port4), one at a time, until it has successfully connected with a FortiGate on a link.

```
config system management fortigate
  set ac-discovery-type broadcast
  set ac-ctl-port 5246
  set ac-data-port 25246
  set discovery-intf lan port4
  set ingress-intf
end
```

By default, it starts the discovery process with the LAN ports (from port1 through port3) first. If it fails to establish a connection after several attempts, it will move on to port4. If it fails on port4, it will go back to the LAN ports and start the process all over again.

A LAN interface has a static IP of 192.168.200.99 and a DHCP Server IP of 192.168.200.110~192.168.200.210. We recommend connecting to the WAN port on FortiGate for ZTP.

The port4 interface is set for DHCP mode, and must be connected to the internal port on FortiGate to obtain an IP address for the CAPWAP tunnel, which is the same as in previous versions.

Stopping data traffic on overgaged LTE interface

When an LTE interface has breached it data usage limit, FortiExtender will stop forwarding outgoing traffic (except for management traffic) to that interface. The following types of traffic are affected:

- NATted traffic
- VPN data traffic on IPsec Tunnel based on the overaged LTE interface
- VWAN traffic on a VWAN member based on the overaged LTE interface. (The VWAN member is marked as invalid, and traffic will be diverted to other valid VWAN members.)
- IP-passthrough traffic

Modes of operation

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

	Mode of operation	
Management scenario	**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 16
- NAT mode on page 18
- get extender status on page 18

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 with FortiGate management

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

```
FX201E5919000027 (fortigate) # show
config system management fortigate
    set ac-discovery-type broadcast
    set ac-ctl-port 5246
    set ac-data-port 25246
    set discovery-intf lan port4
    set ingress-intf
end
```

`ac-discovery-type` specifies the way in which FortiGate and FortiExtender discover each other. It can be static or broadcast. When it is static, the IP of FortiGate should be set as the value of static-ac-ip-addr.

`ac-ctl-port` and the `ac-data-port` define the UDP port used by the control channel and the data channel.

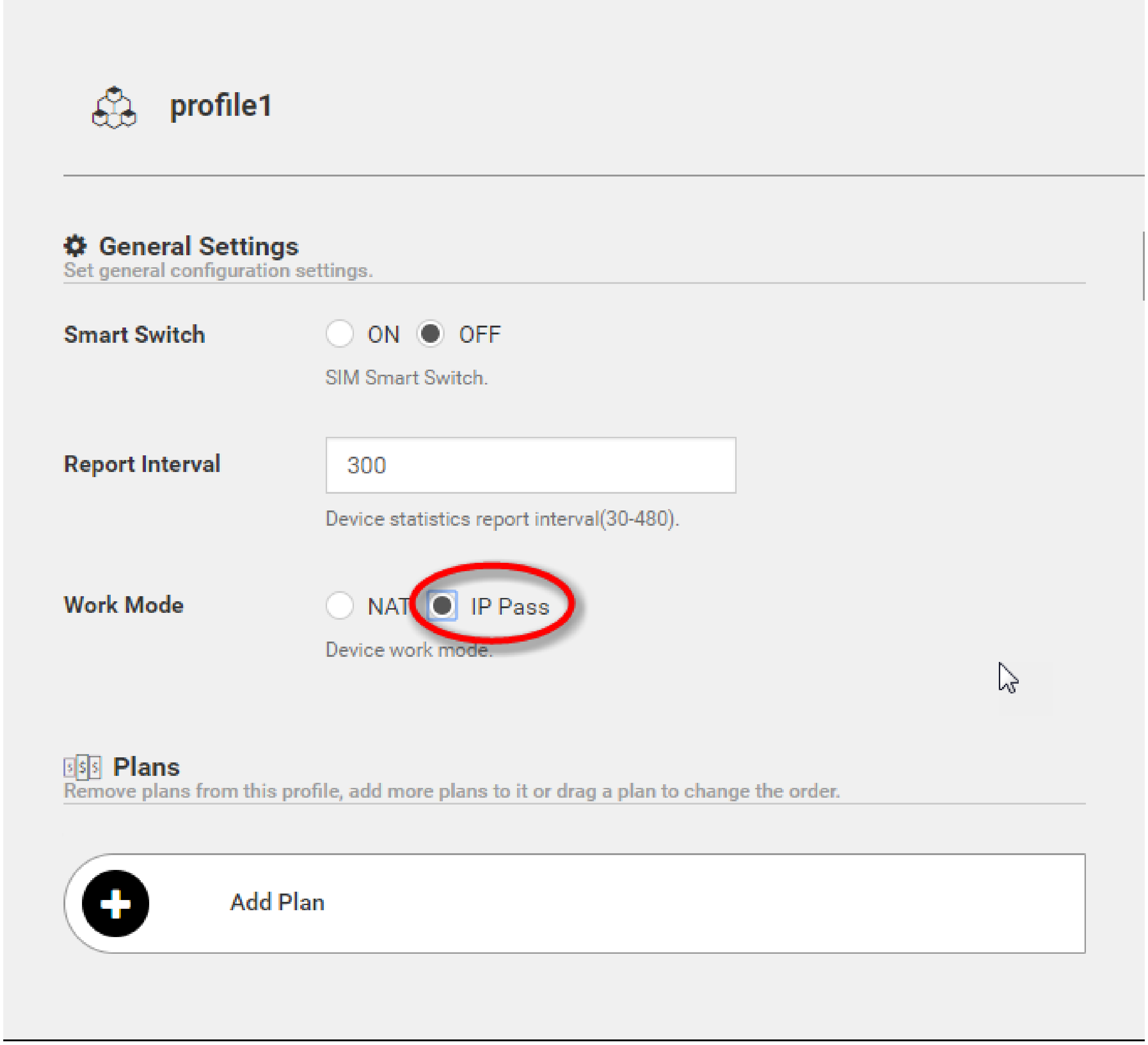
`discovery-intf` specifies the physical ports from which FortiExtender sends broadcast packets in search for FortiGate.

`ingress-intf` defines the interface connected to FortiGate.

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
#
```



profile1

General Settings

Set general configuration settings.

Smart Switch ○ ON ● OFF

SIM Smart Switch.

Report Interval 300

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.

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 20
- DHCP configurations
- System routing on page 30
- Configure PBR routing on page 31
- Firewalls on page 35
- VPN on page 39
- Low-cost SD-WAN strategy on page 48
- Health monitoring on page 53

get extender 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:

```
FX201E5919002499 # get extender status
Extender Status
    name                   : FX201E5919002499
    mode                   : CLOUD
    fext-addr              : 192.168.2.1
    fext-wan-addr          : 10.102.116.241
    controller-addr        : fortiextender-dispatch.forticloud.com:443
    deployed               : true
    management-state       : CWWS_RUN
    base-mac               : 04:D5:90:57:4F:77
    network-mode           : nat
    fgt-backup-mode        : backup
    discovery-type         : cloud
    discovery-interval     : 5
```

```
          echo-interval        : 30
          report-interval      : 30
          statistics-interval  : 120
          mdm-fw-server        : fortiextender-firmware.forticloud.com
          os-fw-server         : fortiextender-firmware.forticloud.com
```

Interface management

FortiExtender 201E and 211E each come with one WAN interface, one LTE interface, and four LAN interfaces. By default, FortiExtender 201E and 211E running on FortiExtender OS 4.2.1 come with the following network settings:

- port1, port2, and port3 are part of the LAN switch with the static IP address of 192.168.200.99/24; a DHCP server also runs on the LAN switch interface with an IP range from 192.168.200.110 to 192.168.200.210 and the default gateway IP of 192.168.200.99.
- port4/POE port is independent (as a DHCP client).

The table below describes the CLI commands used to configure the system interface.

CLI command	Description
`config system interface`	Enters system interface configuration mode.
`edit <interface_name>`	Specify or edit interface name (lan, lo, lte1 or wan).
`set type <type>`	Select the interface type: • `lan-switch`—LAN interface (Can be edited only). • `physical`—LAN interface (Can be edited only). • `lte`—LTE interface (Can be edited only). • `loopback`—Loopback interface (Can be edited only). • `tunnel`—Tunnel interface (Can be created, edited, or deleted). • `virtual-wan`—Virtual WAN interface (Can be created, edited, or deleted).
`set status {up | down}`	Specify the interface state: • `up`—Enabled. • `down`—Disabled.
`set mode {static | dhcp}`	Set the interface IP addressing mode: • `static`—If selected, FortiExtender will use a fixed IP address to connect to the Internet. See set `ip <ip>` below. • `dhcp`—If selected, FortiExtender will work in DHCP client mode.
`set ip <ip>`	(Applicable only when IP addressing mode is set to "static".) Specify an IPv4 address and subnet mask in the format: `x.x.x.x/24`
`set gateway <gateway>`	Set an IPv4 address for the router in the format: `x.x.x.x`
`set mtu <mtu>`	Set the interface's MTU value in the range of 0–4294967295.
`allowaccess {ping | http | https | telnet}`	Select the types of management traffic allowed to access the interface: • `ping`—PING access. • `http`—HTTP access. • `https`—HTTPS access. • `telnet`—TELNET 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.

LAN 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
```

WAN interface configuration example:

```
FX211E5919000009 # config system interface
FX211E5919000009 (interface) # edit wan
```

```
FX211E5919000009 (wan) # show
edit wan
    set type physical
    set status up
    set mode dhcp
    set mtu-override enable
    set mtu 1500
    set vrrp-virtual-mac enable
    config vrrp
        set status disable
    end
    set allowaccess
next

FX211E5919000009 (wan) # set allowaccess
ping
http
telnet
ssh
https

FX211E5919000009 (wan) #
```

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
- 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:

```
FX211E5919000011 # config system lan-switch
FX211E5919000011 (lan-switch) # config ports
FX211E5919000011 (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:

```
FX211E5919000011 (ports) # delete port4
FX211E5919000011 (ports) <M> # next
FX211E5919000011 (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:

```
FX211E5919000011 (ports) # show
config system lan-switch ports
    edit port1
    next
    edit port2
    next
    edit port3
    next
end
```

Example LAN switch configuration

```
FX211E5919000011 (ports) # edit port4
FX211E5919000011 (port4) <M> # next
FX211E5919000011 (ports) # show
config system lan-switch ports
    edit port1
    next
    edit port2
    next
    edit port3
    next
    edit port4
    next
end
```

DHCP configurations

FortiExtender supports DHCP server and DHCP relay. The following sections discuss how to configure the DHCP server and DHCP relay. respectively.

- Configure DHCP server
- Configure DHCP relay

Configure DHCP server

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

To configure 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
`config system dhcpserver`	Enters DHCP server configuration mode.
`edit <name>`	Specify the name of the DHCP server.
`set status {enable | disable | backup}`	Set the DHCP server status: • `enable`—Enable the DHCP server. • `disable`—Disable the DHCP server. • `backup`— Enable in VRRP backup mode. (**Note:** The DHCP server is launched only when the VRRP master goes down.)
`set lease-time <lease_time>`	Specify the DHCP address lease time in seconds. The valid range is 300–8640000. 0 means unlimited.
`set dns-service {local | default | specify | wan-dns}`	Select one of the options for assigning a DNS server to DHCP clients: • `local`—The IP address of the interface of the DHCP server that is added becomes clients' DNS server IP address. • `default`—Clients are assigned the FortiExtender configured DNS server. • `specify`—Specify up to three DNS servers in the DHCP server configuration. • `wan-dns`—The DNS of the WAN interface that is added becomes clients' DNS server IP address.
`set dns-server1 <dns_server1>`	Specify the IP address of DNS Server 1.
`set dns-server2 <dns_server2>`	Specify the IP address of DNS Server 2.
`set dns-server3 <dns_server3>`	Specify the IP address of DNS Server 3.

CLI command	Description
`set ntp-service {local | default | specify}`	Select an option for assigning a Network Time Protocol (NTP) server to DHCP clients: • `local`—The IP address of the interface of the DHCP server that is added becomes clients' NTP server IP address. • `default`—Clients are assigned the FortiExtender configured NTP servers. • `specify`—Specify up to three NTP servers.
`set ntp-server1 <ntp_server1>`	Specify the IP address of NTP Server 1.
`set ntp-server2 <ntp_server2>`	Specify the IP address of NTP Server 2.
`set ntp-server3 <ntp_server3>`	Specify the IP address of NTP Server 3.
`set default-gateway <gateway>`	Specify the default gateway IP address assigned by the DHCP server.
`set netmask <netmask>`	Specify the netmask assigned by the DHCP server.
`set interface <interface>`	Specify the interface on which the DHCP server is expected to run.
`set start-ip <start_ip>`	Specify the start IP address of the DHCP IP address range. For example, 192.168.1.100.
`set end-ip <end_ip>`	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
      set reserved-address enable
   next
end
```

FortiExtender LAN interface(s) can be configured in static IP address mode locally or from FortiExtender Cloud. By default, the LAN interface has 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.

FortiExtender supports DHCP server with reserved addresses. To take advantage of this feature, you must do the following:

1. Enable the `set reserved-address` option, as shown above.
2. Configure the system DHCP-reserved-address using the following commands:

```
edit 1
   set ip <preferred host IP>
   set mac <mac address of host>
   set action <reserved | blocked>
end
```

- `set action reserved` ensures that the same IP is assigned to the host with a matching MAC address.
- `set action disabled` ensures that the host with a given MAC address is not assigned an IP address.

Configure DHCP relay

FortiExtender supports DHCP relay agent which enables it to fetch DHCP leases from a remote server. It has to be configured per interface. Example below:

```
config system dhcprelay
   edit 1
      set status enable
      set client-interfaces <interface name on which relay agent services are
           offered>
      set server-interface <interface name through which DHCP server can be
           reachable>
      set server-ip <remote dhcp server IP>
```

Network utilities

You can define your network from the following aspects:

- Address on page 28
- Service on page 28
- Target on page 28

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
`config router target`	Enters target configuration mode.
`edit <name>`	Specify the target network.

CLI command	Description
`set interface <interface>`	Specify the outgoing interface of the gateway.
`set next-hop <next_hop>`	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 4.2.1 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

The table below describes the commands for configuring static routing.

CLI command	Description
`config router static`	Enters static route configuration mode.
`edit <name>`	Specify the name of the static route.
`set status {enable | disable}`	Set the status of the static route: • `enable`—Enable the static route. • `disable`—Disable the static route.
`set dst <dst>`	Specify the destination IP address and netmask of the static route in the format: `x.x.x.x/x`
`set gateway <gateway>`	Specify the IP address of the gateway.
`set distance <distance>`	Specify the administrative distance. The range is 1–255. The default is 1.
`set device <device>`	Specify the name of the outgoing interface.
`set comment [comment]`	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
`config router target`	Enters target configuration mode.
`edit <name>`	Specify the name of the target.
`set interface <interface>`	Specify the outgoing interface or tunnel.
`set next-hop <next_hop>`	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
```

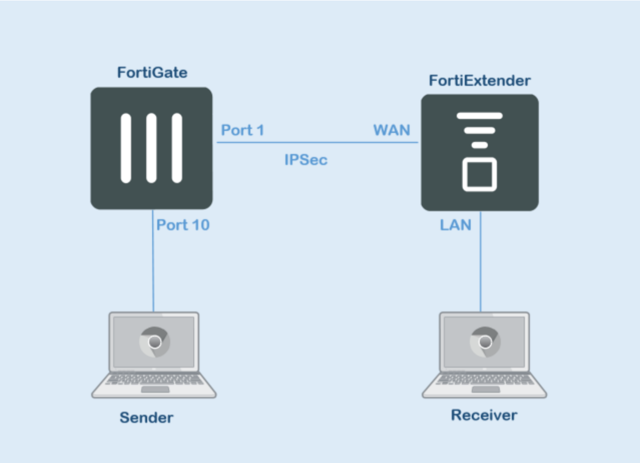
Configure multicast routing

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
        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 35
- Configure protocol/port range on page 35
- Configure firewall policies on page 36
- Move firewall policies on page 37

Configure address/subnet

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

CLI command	Description
`config network address`	Enters network IP address configuration mode.
`edit <name>`	Specify the name of the IP address configuration object.
`set type {ipmask | iprange}`	Select either address type: • `ipmask`—IPv4 address/mask in the format: `x.x.x.x/x` • `iprange`—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
`config network service service-custom`	Enters the network service configuration mode.
`edit <name>`	Specify the name of the service configuration object.
`set protocol <Protocol Type>`	Specify the protocol (service).
`set protocol number <0-255> *`	Specify the protocol number (if you are not sure of the name of the protocol).
`set protocol udp-portrange`	Specify the port range for UDP protocol.
`set protocol tcp-portrange`	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
`config firewall policy`	Enters firewall policy configuration mode.
`edit <name>`	Specify the name of the firewall configuration object.
`set srcintf`	Specify the ingress interface.
`set dstintf`	Specify the egress interface.

CLI command	Description
`set srcaddr`	Specify the source IP address, which can be either a single IP address or a range of IP addresses.
`set action {allow | deny}`	Select either of the following actions: - `allow`—Allow access. - `deny`—Deny access.
`set status {enable | disable}`	Set the status of the policy: - `enable`—Enable the policy. - `disable`—Disable the policy.
`set nat {enable | disable}`	Select an option for NAT: - `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.

An IPsec VPN is established in two phases: Phase 1 and Phase 2.

Several parameters determine how this is done, except for IP addresses, the settings simply need to match at both VPN gateways.

There are defaults that are applicable for most cases.

When a FortiExtender unit receives a connection request from a remote VPN peer, it uses IPsec Phase-1 parameters to establish a secure connection and authenticate that VPN peer. Then, the FortiExtender unit establishes the tunnel using IPsec Phase-2 parameters. Key management, authentication, and security services are negotiated dynamically through the IKE protocol.

To support these functions, the following general configuration steps must be performed on both units:

- Define the Phase-1 parameters that the FortiExtender unit needs to authenticate the remote peer and establish a secure connection.
- Define the Phase-2 parameters that the FortiExtender unit needs to create a VPN tunnel with the remote peer.
- Create firewall policies to control the permitted services and permitted direction of traffic between the IP source and destination addresses.
- Create a route to direct traffic to the tunnel interface.

Currently, FortiExtender only works in VPN client mode, be sure to keep the following limitations in mind when using this feature:

- If both ends of the VPN tunnel are FortiExtender devices, they must operate in NAT mode and use a static public IP address.
- If the remote device is not FortiExtender, it must have a static public IP address and can work in VPN server mode.

This section discusses the following topics:

- Configure VPN on page 39
- Check VPN tunnel status on page 45
- IPsec VPN support for third-party certificates on page 45

Configure VPN

VPN configurations include the following operations:

- Configure phase-1 parameters
- Configure phase-2 parameters
- Configure firewall policies
- Configure route

Configure phase-1 parameters

Use the following commands to configure a VPN tunnel.

CLI command	Description
`ike-version`	Specify the IKE protocol version, 1 or 2.
`keylife`	Specify the time (in seconds) to wait before the Phase-1 encryption key expires. The valid range is 20 –172800.
`proposal`	Specify Phase-1 proposal.
`Dhgrp`	Select one of the following DH groups: • `1` • `2` • `5` • `14`
`*interface`	Use either of the following: • `wan` • `eth1/lte1/lte2` **Note:** The WAN interface is only available on 2xxE devices. The names of the LTE interfaces vary depending on the hardware, as explained below: • `lte1` (for FEX-201E and 211E)
`type`	Select a remote gateway type: • `static` • `ddns`
`*remote-gw`	Specify the IPv4 address of the remote gateway’s external interface.
`*remotegw-ddns`	Specify the domain name of the remote gateway, e.g., xyz.DDNS.com.
`authmethod`	Select an authentication method: • `psk(pre-shared key)` • `signature`
`*psksecret`	Specify the pre-shared secret created when configuring the VPN client.
`*certificate`	`set certificate <local-cert-name>` Specify the name of local signed personal certificates. This entry is only available when authmethod is set to signature. You can enter the names of up to four signed personal certificates for the FortiExtender unit. The certificates must have already been installed on the FortiExtender before you are trying to enter them here.
`*peer`	`set peer <ca-cert-name>` This is the name of the CA certificate used to constrain that the peer certificate is issued by it or its sub-CA. This entry is available only when authmethod is set to signature. The certificates must have already been installed on the FortiExtender before you are trying to enter them here. **Note:** If no peer is set, the peer certificate can still be accepted as long as a CA certificate that can verify the peer certificate exists.

CLI command	Description
`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.

Configure phase-2 parameters

Parameter	Description
`phase1name`	The name of Phase-1 which determines the options required for Phase- 2.
`proposal`	Phase-2 proposal.
`pfs`	Select either of the following: • `enable` • `disable`
`Dhgrp`	Phase-2 DH group.
`keylife-type`	Key life type.
`keylifeseconds`	Phase-2 key life time in seconds. **Note:** The valid range is 120—172800.
`encapsulation`	ESP encapsulation mode
`protocol`	Quick mode protocol selector. **Note:** The valid range is 1—255. 0 means for all.
`src-addr-type`	Local proxy ID type. Select one of the following: • `subnet`— IPv4 subnet • `range` —IPv4 range • `ip` —IPv4 IP • `name` — IPv4 network address name
`src-subnet`	Local proxy ID subnet. **Note:** This field is only available when `src-addr-type` is set to `subnet.`

Parameter	Description
src-start-ip	Local proxy ID start. **Note:** This field is only available when src-addr-type is set to either range or ip.
src-end-ip	Local proxy ID end. **Note:** This field is only available when src-addr-type is set to range.
src-name	Local proxy ID name. **Note:** This field is only available when src-addr-type is set to name.
src-port	Quick mode source port. **Note:** The valid range is 1—65535. 0 means for all.
dst-addr-type	Remote proxy ID type. Select one of the following: subnet— IPv4 subnet range —IPv4 range ip —IPv4 IP name— IPv4 network address name
dst-subnet	Remote proxy ID subnet. **Note:** The field is only available when dst-addr-type is set to subnet.
dst-start-ip	Remote proxy ID start. **Note:** This field is only available when dst-addr-type is set to either range or ip.
dst-end-ip	Remote proxy ID end. **Note:** This field is only available when dst-addr-type is set to range.
dst-name	Remote proxy ID name. **Note:** This field is only available when dst-addr-type is set to name.
dst-port	Quick mode destination port. **Note:** The valid range is 1—65535. 0 means for all.

Example VPN configuration:

```
FX201E5919002631 # config vpn ipsec 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 34.207.95.79
        set authmethod psk
        set psksecret HG709!ppA#d
        set localid FX04DA5918004527
        set peerid
    next
end
FX201E5919002631 # config network address
FX201E5919002631 (address) # show
    config network address
        edit local_subnet
        set type ipmask
        set subnet 192.168.2.0/24
    next
    edit remote_subnet
        set type ipmask
        set subnet 192.168.10.0/24
    next
end
FX201E5919002631 # config vpn ipsec phase2-interface
FX201E5919002631 (phase2-interface) #
    edit fcs-0-phase-2
        set phase1name 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-type name
        set src-name local_subnet
        set src-port 0
        set dst-type name
        set dst-name remote_subnet
        set dst-port 0
    next
end
FX201E5919002631 # config firewall policy
FX201E5919002631 (policy) # show
config firewall policy
    edit to_remote
        set srcintf lan
        set dstintf fcs-0-phase-1
        set srcaddr local_subnet
        set dstaddr remote_subnet
        set action accept
        set status enable
        set service ALL
        set nat disable
    next
    edit from_remote
        set srcintf fcs-0-phase-1
        set dstintf lan
        set srcaddr remote_subnet
        set dstaddr local_subnet
        set action accept
        set status enable
        set service ALL
        set nat disable
next
end
FX201E5919002631 # config router static
FX201E5919002631 (static) # show
config router static
    edit to_remote
        set status enable
        set dst 192.168.10.0/24
        set gateway
        set distance 1
        set device fcs-0-phase-1
        set comment
    next
end
```

Configure firewall policies

You must define two ACCEPT firewall polices to permit communications between the source and destination addresses.

```
config firewall policy
     edit to_remote
         set srcaddr <The address name for the private network behind this FortiExtender
unit>
         set dstaddr <The address name that you defined for the private network behind
the remote peer>
         set service ALL
         set nat disable
         set srcintf <The interface that connects to the private network behind this
FortiExtender unit>
         set dstintf <The VPN Tunnel (IPsec Interface)>
         set status enable
     next
     edit from_remote
         set srcaddr <The address name that you defined for the private network behind
the remote peer>
         set dstaddr <The address name for the private network behind this FortiExtender
unit>
         set service ALL
         set nat disable
         set srcintf <The VPN Tunnel (IPsec Interface)>
         set dstintf <The interface that connects to the private network behind this
FortiExtender unit>
         set status enable
     next
end
```

Configure static routes

All network traffic must have a static route to direct its traffic to the proper destination. Without a route, traffic will not flow even if the firewall policies are configured properly. You may need to create a static route entry for both directions of VPN traffic if your firewall policies allow bi-directional tunnel initiation.

```
config router static
    edit to_remote
        set status enable
        set dst <The address name that you defined for the private network behind the
remote peer>
        set gateway <Leave as default: 0.0.0.0>
        set distance <Leave this at its default>
        set device <The VPN Tunnel (IPsec Interface)>
        set comment
    next
end
```

If there are other routes on the FortiExtender unit, you may need to set the distance on this route so the VPN traffic will use it as the default route. However, this normally happens by default because this route is typically a better match than the generic default route.

Check VPN tunnel status

Use the following command to check your VPN tunnel status:

```
FX201E5919002631 # get vpn IPSec tunnel details
fcs-0-phase-1: 0000002, 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-0-phase-2: 0000002, 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 192.168.10.0/24
```

IPsec VPN support for third-party certificates

FortiExtender now is able to use third-party CA certificates at phase 1 to verify identity of peers and to establish IPsec VPN tunnels.

Import third-party certificates

Import a third-party CA certificate:

- From the Console: `execute vpn certificate ca import tftp <remote_file> <local_name> <ip>`
- From the GUI: Chick **VPN>VPN Certificate>CA Certificate>Import New Certificate**.

Import a third-party Local certificate

- From the console: `execute vpn certificate local import tftp <remote_file> <local_name> <ip> <passwd>`
- From the GUI: Click **VPN>VPN Certificate>Entity Certificate>Import New Certificate.**

Use third-party certificates for IKE authentication

In 4.2.0, two new fields "certificate" and "peer" have been added to the phase1 interface entry. You can use them to reference the imported third-party certificates. It is important to know that these fields are available only when "authmethod" is set to signature.

Certificate

You can reference the datasource "vpn.certificate.local".

For the name of local signed personal certificates, you can enter the names of up to four signed personal certificates for the FortiExtender unit. You must have the certificated already installed on the FortiExtender beforehand to be able to enter them here.

Peer

You can reference the datasource "vpn.certificate.ca".

This is the name of the CA certificate used to constrain that the peer certificate is issued by it or its sub-CA. The certificates must have already been installed on the FortiExtender before you are able to enter them here.

If the peer is not set, the peer certificate can still be accepted as long as a CA certificate that can verify the peer certificate exists.

Example for using third-party certificates for IKE authentication

```
config vpn ipsec phase1-interface
    edit vpn1
        set ike-version 2
        set keylife 86400
        set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
```

```
3des-sha1
        set dhgrp 14 5
        set interface nas1
        set type static
        set remote-gw 192.168.137.106
        set authmethod signature
        set certificate <local_cert_name>   ==> new field
        set peer <ca_cert_name>             ==> new field
        set localid
        set peerid
    next
end
```

Low-cost SD-WAN strategy

FortiExtender supports Software-Defined Wide Area Network (SD-WAN) to provide link load-balancing (LLB) among different links. It provides the following features:

- Virtual interface in system for routing system and firewall.
- Adding targets as members and balancing traffic among them.
- Link Load-balancing (LLB) for WAN interfaces or VPN tunnels.
- LTE interface as members of SD-WAN, or combined with a physical interface as members of SD-WAN.
- Support for multiple LLB algorithms:
  - Redundant
  - Weighted Round Robin (WRR)
- Redundant algorithm using a SD-WAN member for data transmission based on:
  - Priority
  - Cost
- Two LTE interfaces as members of SD-WAN redundant by cost algorithm:
  - The lowest cost target works as primary. When primary fails, the next lowest cost target will take over the primary role (fail-over).
  - When a dead primary comes back to life, it will retake the primary role (fail-back).
  - The cost of LTE interface is calculated based on the capacity and monthly-fee of the LTE plan.
- When the LTE and physical interface(s) are members of SD-WAN redundant by cost algorithm:
  - The physical interface must always be selected as lowest cost target and works as the primary.

This section covers the following topics:

- Configure an SD-WAN on page 48
- Check SD-WAN health on page 49
- Define an SD-WAN member on page 51

Configure an SD-WAN

Use the following commands to configure an SD-WAN.

CLI command	Description
`config system interface`	Enters system interface configuration mode.
`edit <vwan_name>`	Specify the name of the SD-WAN interface.
`set type virtual-wan`	Set the interface type to virtual-wan.
`set status <status>`	Set the status of the interface: • `up`—Enable the interface. • `down`—Disable the interface.

CLI command	Description
`set persistence {source | dest | ip-pair | connection}`	Select a LLB metric to denote how to distribute traffic: • `source`—Traffic from the same source IP is forwarded to the same target. • `dest`—Traffic to the same destination IP is forwarded to the same target. • `ip-pair`—Traffic from the same source IP and to the same destination IP is forwarded to the same target. • `connection`—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
`set algorithm {redundant | WRR}`	Select the LLB algorithm: • `redundant`—Targets work in primary-slave mode. • `WRR`—Targets work in Weighted Round Robin mode.
`Set grace-period`	Specify the grace period in seconds to delay fail-back.
`set session-timeout 60`	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.
`set members`	Add VWAN members to the VWAN interface.

FortiExtender supports both redundant and Weighted Round Robin (WRR) load-balancing 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
set protocol {ping | http | dns}	The protocol to be used for status check.
set port	The port number used to communicate with the server. The valid range is 1–65535. The default is 80.
set http-get	The URL used to communicate with the server. The default is /.
set interval	Specify the monitoring interval in seconds. The valid range is 1–3600. The default is 5.
set probe_cnt	Specify the number of probes sent within the set interval. The valid range is 1–10. The default is 1.
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 confiuration:

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
`set target`	Specify the target to which traffic is forwarded.
`set health-check`	Specify the link health check of the VWAN.
`set priority`	Specify the priority of the link member. The valid range is 1–7.
`set weight`	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 53
- Perform link health check on page 54
- Configure health monitoring on page 56

Monitor interface status

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

CLI Command	Description
`*set interface <interface_name>`	Specify the interface to be monitored.
`set interval`	Specify the monitoring interval in seconds. The valid range is 1–3600. The default is 30.
`set filter {rx_bytes | tx_bytes | rx_packets | tx_packets | rx_dropped | tx_dropped | rx_bps | tx_bps | rx_pps | tx_pps}`	Set the monitor filters on the interface: • `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 internal 30
```

```
                    set interface lte1
                    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
lte1: 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.

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

Paramerter	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 • 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

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 intervalm default:1>
               set probe-tm <probe timeout, default:2>
               set probe-target <target to be probed>
               set interface <uplink interfaces on which probe has to be sent>
               set src-iface <interface whose source IP is to be used>
               set filter <rtt |loss>
       next
       end
end
```

To display interface statistics 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:

- FortiGate-FortiExtender zero-touch provisioning (ZTP) on page 57
- Get system version on page 57
- Upgrade OS firmware on page 58
- Upgrade modem firmware on page 59
- SMS notification on page 59
- Remote diagnostics via SMS on page 60
- Export system logs to remote syslog servers on page 61
- Support for SNMP (read-only) and traps on page 61

FortiGate-FortiExtender zero-touch provisioning (ZTP)

FortiExtender supports FortiGate-FortiExtender zero-touch provision (ZTP). The process is outlined stepwise as follows:

1. FortiExtender default discovery mode is set to auto with DHCP server enabled over the LAN interface. A SIM card without a PIN code is expected to be used for ZTP, and a default APN should be retrieved automatically at first connection.
2. Acting as a DHCP client, FortiGate connects to the FortiExtender LAN interface to obtain a private IP to reach FortiManager.
3. FortiGate reports the discovered FortiExtender to FortiManager to authorize it (FortiExtender).
4. Once authorized, FortiExtender switches to IP-passthrough mode and then reboots itself.
5. Upon booting up in IP-passthrough mode, FortiExtender serves as the FortiExtender-WAN interface of FortiGate, as it does in previous releases.

Get system version

Use the following command to find out your system version:

```
FX211E5919000011 # get system version
System version:
    image version    : FXT211E-v4.12-build400
    image type       : Interim
    model            : FortiExtender-211E
    MAC              : 04:d5:90:21:5f:c7
    SN               : FX211E5919000011
    license          : ae30e2902fc1fe8f
    OEM SN           : FX211E5919000011
    REV              : 24258-01
    VERSION          : 00020003
    ROM REV          : FX211E
```

```
Fallback image   : FXT211E-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 GUI, or any of the following CLI 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 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

FortiExtender-201E and 211E 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:

```
FX211E5919000011 # config system sms-remote-diag
FX211E5919000011 (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:

```
FX211E5919000011 # config system syslog
FX211E5919000011 (syslog) # show
config system syslog
    set remote-server
    set remote-port 514
end

FX211E5919000011 (syslog) # set
remote-server    Remote Syslog server IP address
remote-port      Remote Syslog server port
```

Support for SNMP (read-only) and traps

As an SNMP agent, FortiExtender responds to SNMP managers query on v1/v2c and v3 protocol. It supports the following SNMP trap events (which can be configured in both SNMP community and user events):

- system-reboot
- data-exhausted
- session-disconnect
- low-signal-strength
- os-image-fallback
- mode-switch
- fgt-backup-mode-switch

Typical SNMP commands

The following are commands commonly used to configure SNMP in FortiExtender.

```
FX201E5919000054 # config snmp
FX201E5919000054 (snmp) # show
config snmp
   config sysinfo
      set status enable
      set description
      set contact-info
      set location
   end
   config community
      edit fext
```

```
         set status enable
         set hosts lan
         set query-v1-status enable
         set query-v1-port 161
         set query-v2c-status enable
         set query-v2c-port 161
         set trap-v1-status enable
         set trap-v1-lport 162
         set trap-v1-rport 162
         set trap-v2c-status disable
         set trap-v2c-lport 162
         set trap-v2c-rport 162
         set events
      next
   end
   config user
   end
   config hosts
      edit lan
         set host-ip 172.30.0.0/16
         set host-type any
      next
   end
end
```

Sample SNMP commands

```
FX201E5919000054 # config snmp
FX201E5919000054 (snmp) # show
config snmp
   config sysinfo
      set status disable
      set description
      set contact-info
      set location
   end
   config community
   end
   config user
   end
   config hosts
   end
end

FX201E5919000054 (snmp) # config
sysinfo SNMP system info setting
community SNMP v1/v2c community setting
user SNMP v3 user setting
hosts SNMP hosts setting

FX201E5919000054 (snmp) # config sysinfo
FX201E5919000054 (sysinfo) # show
config snmp sysinfo
   set status disable
   set description
   set contact-info
   set location
end

FX201E5919000054 (sysinfo) # set
status Enable/disable SNMP
description System description. size[127]
contact-info Contact information
location System location. size[127]
FX201E5919000054 (sysinfo) # end

FX201E5919000054 # config snmp hosts
FX201E5919000054 (hosts) # edit lan
FX201E5919000054 (lan) <M> # set
*host-ip IPv4 address of the SNMP manager(host), syntax: X.X.X.X/24
host-type Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or
     both
FX201E5919000054 (hosts) # end

FX201E5919000054 # config snmp community
FX201E5919000054 (community) # edit fext
FX201E5919000054 (fext) <M> # set
status Enable/disable this SNMP community
hosts Configure IPv4 SNMP managers (hosts)
query-v1-status Enable/disable SNMP v1 queries
query-v1-port SNMP v1 query port (default = 161)
query-v2c-status Enable/disable SNMP v2c queries
query-v2c-port SNMP v2c query port (default = 161)
trap-v1-status Enable/disable SNMP v1 traps
trap-v1-lport SNMP v1 trap local port (default = 162)
trap-v1-rport SNMP v1 trap remote port (default = 162)
trap-v2c-status Enable/disable SNMP v2c traps
trap-v2c-lport SNMP v2c trap local port (default = 162)
trap-v2c-rport SNMP v2c trap remote port (default = 162)
events SNMP trap events
FX201E5919000054 (community) # end


FX201E5919000054 # config snmp user
FX201E5919000054 (user) # edit lan
FX201E5919000054 (lan) <M> # set
status Enable/disable this SNMP user
notify-hosts SNMP managers to send notifications (traps) to
trap-status Enable/disable traps for this SNMP user
trap-lport SNMPv3 local trap port (default = 162)
trap-rport SNMPv3 trap remote port (default = 162)
queries Enable/disable SNMP queries for this user
query-port SNMPv3 query port (default = 161)
events SNMP trap events
security-level Security level for message authentication and encryption
FX201E5919000054 (user) # end
```

Executable SNMP commands

```
FX201E5919000054 # execute snmpmibs
```

```
download Export SNMP MIBs to tftp server
FX201E5919000054 # execute snmpmibs download
tftp download through TFTP.
FX201E5919000054 # execute snmpmibs download tftp
FORTINET-CORE-MIB.mib download FORTINET-CORE-MIB.mib
FORTINET-FORTIEXTENDER-MIB.mib download FORTINET-FORTIEXTENDER-MIB.mib
FX201E5919000054 # execute snmpmibs download tftp FORTINET-CORE-MIB.mib
Usage: snmpmibs export mib_file tftp tftp_server
<mpmibs download tftp FORTINET-FORTIEXTENDER-MIB.mib
Usage: snmpmibs export mib_file tftp tftp_server
FX201E5919000054 #
```

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.

If you must configure the APN, you can do it on FortiGate, FortiExtender Cloud, or locally.

Add a new carrier profile

Default carrier profiles are included in modem firmware package. You can check the default carriers using the following commands:

```
config lte carrier
show
end
```

If your carrier is not in the list of profiles, you can create a customized carrier profile using the following commands:

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

Add a new operator/carrier

An SIM map entry is used to get the carrier from the PLMN. Most PLMNs are supported in the default configuration. You can always check if your SIM PLMN is supported using the following command:

```
get lte carrier <mcc> <mnc>
```

If you cannot find the carrier of your SIM card, you can add a customized SIM using the following commands:

```
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
```

The new operator/carrier requires at least one matched carrier profile entry from “`config lte carrier`” to take effect.

Create a data plan

```
edit verizon
   set modem modem1
   set type by-carrier
   set type by-iccid
   set carrier Verizon
   set type by-slot
   set apn WE01.VZWSTATIC
   set auth NONE
   set user
   set pwd
   set pdn ipv4-only
   set signal-threshold 0
   set signal-period 0
   set capacity 0
   set monthly-fee 0
   set billing-date 0
   set overage disable
   set preferred-subnet 32
   set private-network disable
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.

Parameter	Description
modem	Choose “modem1” or “modem2”.
type	Choose the way for the modem to select the SIM card: • by-iccid • by-slot • by-carrier • by-default
simid	The iccid of the SIM, mandatory for “set type by-iccid”.
carrier	The SIM card carrier, mandatory for “set type by-carrier”.
slot	The SIM card slot, mandatory for “set type by-slot”
apn	Set the APN of the SIM card.
auth	Choose the Authorization mode.
user	Set the username.
pwd	Set the password.
pdn	Choose the Packet Data Network (PDN) IP address family.

Parameter	Description
signal-threshold	Set the signal-strength threshold beyond which SIM switch will occur. (from -100 to -50 dBm)
signal-period	Set the length of time (from 600 to 18000 seconds) for SIM switch to occur when signal strength remains below the set signal threshold for more than half of the set period.
capacity	Set data capacity per month (from 0 to 102400000 MB).
monthly-fee	Set the monthly fee for the data plan (from 0 to 1000000).
billing-date	Set the billing date of the month.
preferred-subnet	DHCP subnet.
private-network	Enable/disable blocking all non-NAT'ed traffic.

Set the default SIM

When you install dual SIM cards in one modem, you can configure the default SIM to use.

You can set the default SIM by

- Set the default SIM by preferred carrier on page 67
- Set the default SIM by low cost on page 67
- Set the default SIM by SIM slot on page 68

Set the default SIM by preferred carrier

Use this option to set the default SIM if you have SIM cards from different carriers.

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

Set the default SIM by low cost

This option applies when you need to choose the low-cost SIM over a more expensive one.

You must configure two entries under "config lte plan" for the two SIM cards separately. The system will calculate the cost based on the "set capacity" and "monthly-fee".

```
config lte setting
   config modem1
      set default-sim by-cost
      set preferred-carrier <carrier name>
      end
   end
```

Set the default SIM by SIM slot

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

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

Enable SIM-switch

```
   config lte setting
      config modem1
         config auto-switch
            set by-disconnect enable
            set by-signal disable
            set by-data-plan disable
            set disconnect-threshold 1
            set disconnect-period 600
            set switch-back by-time by-timer
            set switch-back-by-time 00:01
            set switch-back-by-timer 3600
         end
      end
   end
```

SIM-switching can be configured by data plan, disconnect settings, signal strength, coupled with switch back by time or by timer. All these options are under the “Auto switch” setting.

Parameter	Description
by-disconnect	The SIM card switches by disconnect.
by-signal	The SIM card switches by signal strength.
by-data-plan	The SIM card switches by data plan.
disconnect-threshold	The number (1 - 100) of disconnects for SIM switch to take place.
disconnect-period	The evaluation period (600 - 18000) in seconds for SIM switch.
switch-back	Enables switching back to the preferred SIM card.
switch-back-by-time	Switches over to the preferred SIM /carrier at a specified (UTC) time (HH:MM).
switch-back-by-timer	Switches over to the preferred SIM/carrier after a given time (3600-

Parameter	Description
	2147483647) in seconds.

Report to controller

```
config lte setting
   config controller-report
      set status [enable | disable]
      set interval 300
      set signal-threshold 10
   end
end
```

Parameter	Description
`status`	Enable or disable periodic controller report.
`interval`	The interval at which to notify the controller (once every 30 to 86400 seconds; the default is 300).
`signal-threshold`	The signal strength threshold (10 - 50 dBm). FortiExtender notifies the controller once the RSSI change has exceeded the set threshold.

Use cases

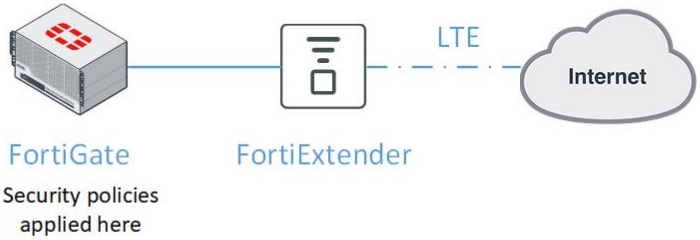
This section discuses some typical use cases to deploy FortiExtender.

- Extended cellular WAN of FortiGate on page 70
- Redundant with FGT in IP Pass-through mode on page 75
- Manage from FortiExtender Cloud on page 81
- FortiExtender 201E for FortiGate HA configuration

Extended cellular WAN of FortiGate

When setting up a FortiExtender out of box with FortiExtender OS version 4.2.1, you can connect FortiExtender to FortiGate in either of the following ways:

- Connect the FortiGate port in DHCP client mode (such as WAN1/WAN2) to the FortiExtender LAN port (1 , 2 or 3). In this option, the FortiGate interface acquires DHCP lease from the FortiExtender LAN DHCP server, and has a default gateway as the FortiExtender LAN interface IP address. An ZTP solution with FortiManager can be achieved through this mode.
- If the FortiGate internal /LAN is running a DHCP server, connect the FortiGate to port4 of FortiExtender 201E, which acquires DHCP lease from the FortiGate DHCP server.



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 allowacess capwap`" instead.

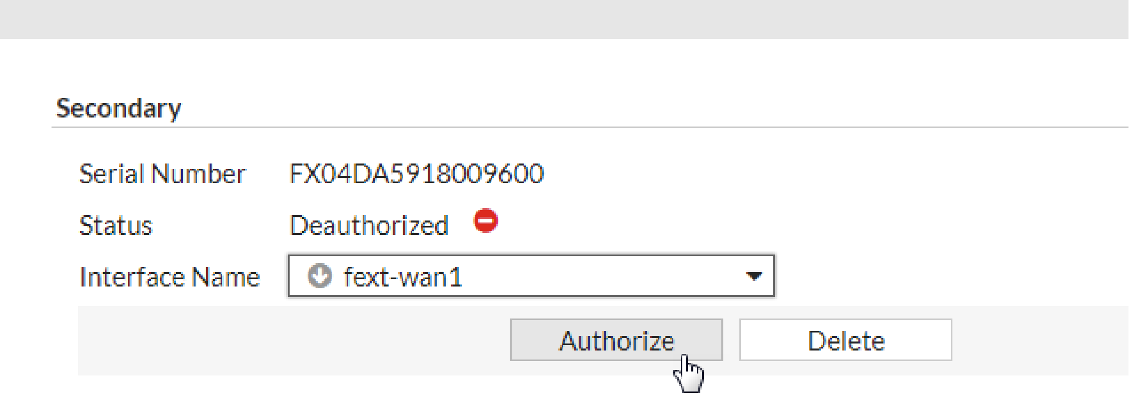
2. Authorize the FortiExtender device.

   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

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.)

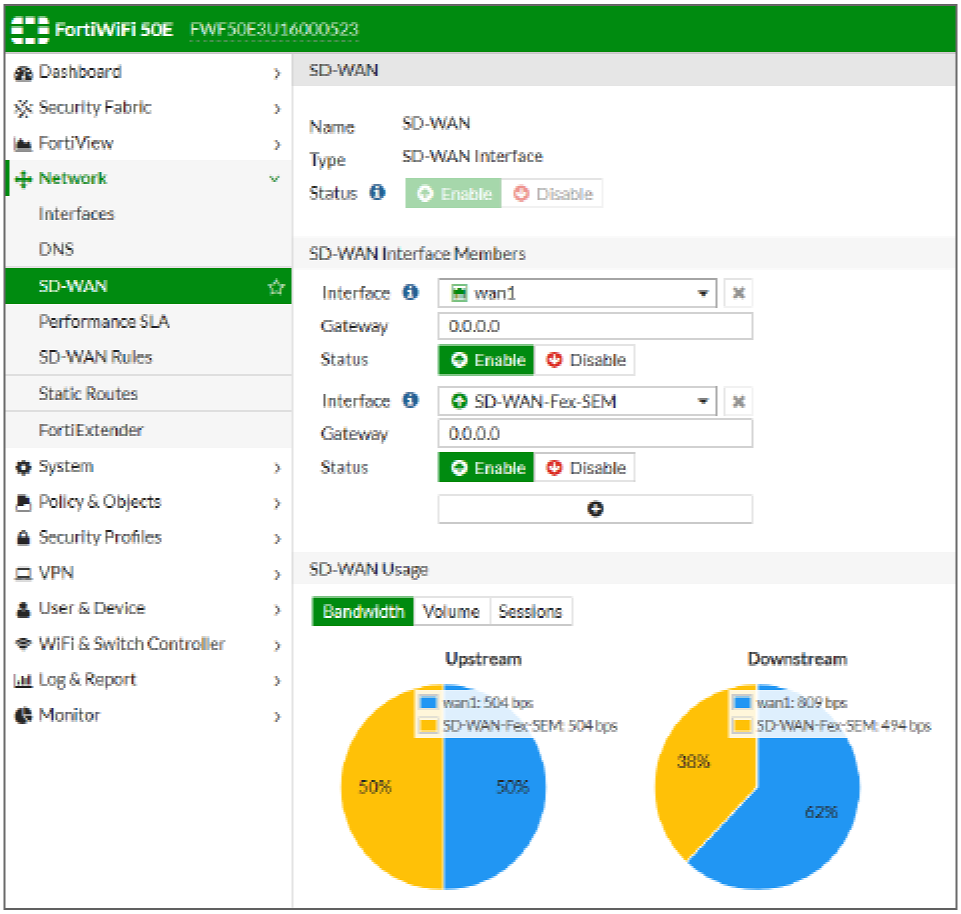
Now the traffic is shared between the wan1 and FEX-wan1 links according to the ECMP Load Balancing Method used. This deployment can be extrapolated for dual FortiExtender installation.

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.



SD-WAN

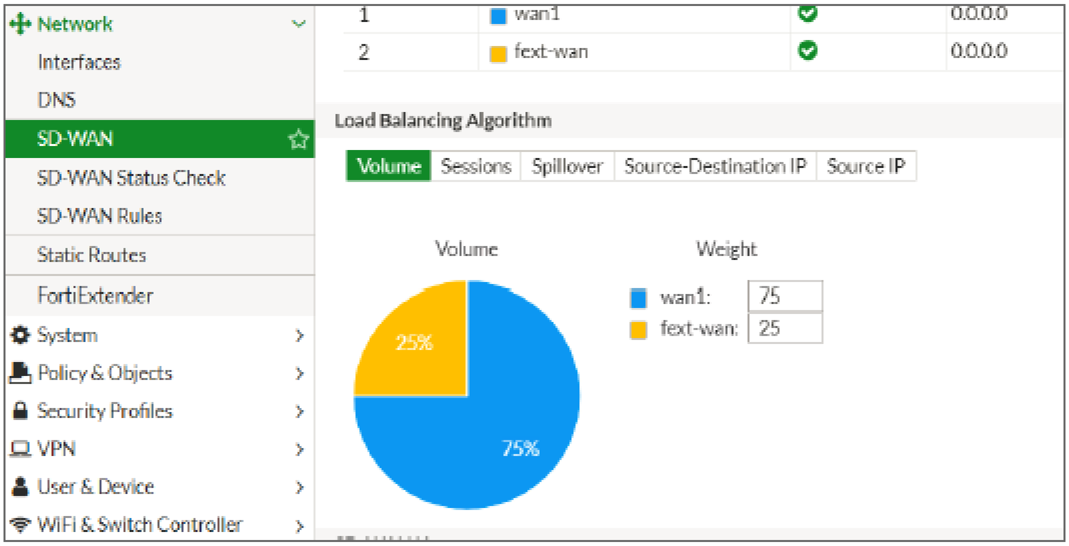
Name SD-WAN
Type SD-WAN Interface
Status Enable Disable

SD-WAN Interface Members

Interface wan1
Gateway 0.0.0.0
Status Enable Disable

Interface SD-WAN-Fex-SEM
Gateway 0.0.0.0
Status Enable Disable

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

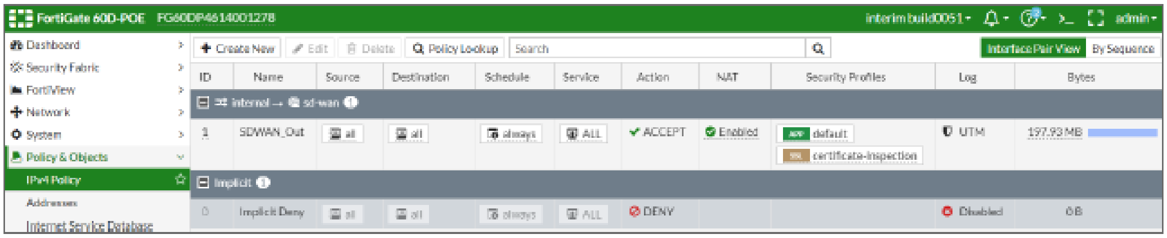


1	🟦 wan1	✓	0.0.0.0
2	🟨 fext-wan	✓	0.0.0.0

Load Balancing Algorithm: Volume

Weight
🟦 wan1: 75
🟨 fext-wan: 25

3. Define your policies as illustrated below.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
internal → sd-wan										
1	SDWAN_Out	all	all	always	ALL	✓ ACCEPT	Enabled	default certificate-inspection	UTM	197.93 MB
Implicit										
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

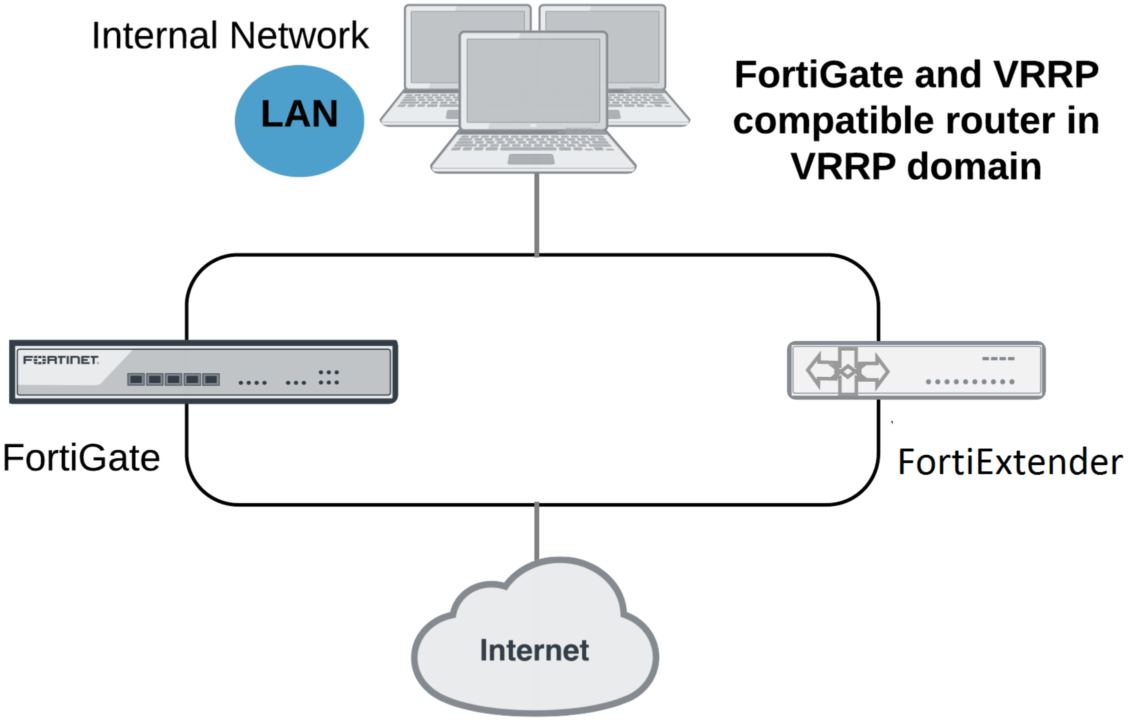
For more information about how to deploy SD-WAN in general, refer to FortiOS documentation.

Redundant with FGT in IP Pass-through mode

A Virtual Router Redundancy Protocol (VRRP) configuration can be used as a high-availability (HA) solution to ensure network connectivity in the event of a failing FortiGate router. With VRRP enabled on FortiExtender, all traffic will transparently fails over to FortiExtender when the FortiGate on your network fails. When the failed FortiGate is restored, it will take over the processing of traffic for the network.

For more information about VRRP, see RFC 3768.

Use Case 1: FortiExtender in VRRP mode while being managed from FortiGate.



General configuration procedures

1. The FortiExtender LAN interface consists of multiple ports by default. Be sure to separate out an individual port from the LAN-switch for VRRP purposes. (Refer to "Step 3: Verify the port settings on FortiExtender" in FEX-201E for FortiGate HA configuration on page 84.)
2. Continue managing FortiExtender from FortiGate over the LAN interface. (NOT the VRRP interface.)
3. Configure the VRRP gateway IP on the newly separated individual port on the FortiExtender and the corresponding VRRP port on the FortiGate.
4. Set the VRRP priority of the FortiExtender VRRP interface to a value lower than the FortiGate VRRP interface's priority.
5. Create a firewall policy on the FortiExtender to forward traffic from newly created VRRP interface to the LTE internet (Refer to Configure firewall policies on page 36.)
6. Ensure the VRRP ports on the FortiExtender and the FortiGate are connected by verifying that the FortiExtender is in backup mode and the FortiGate is in master mode by running command "get router info vrrp".

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

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
```

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:

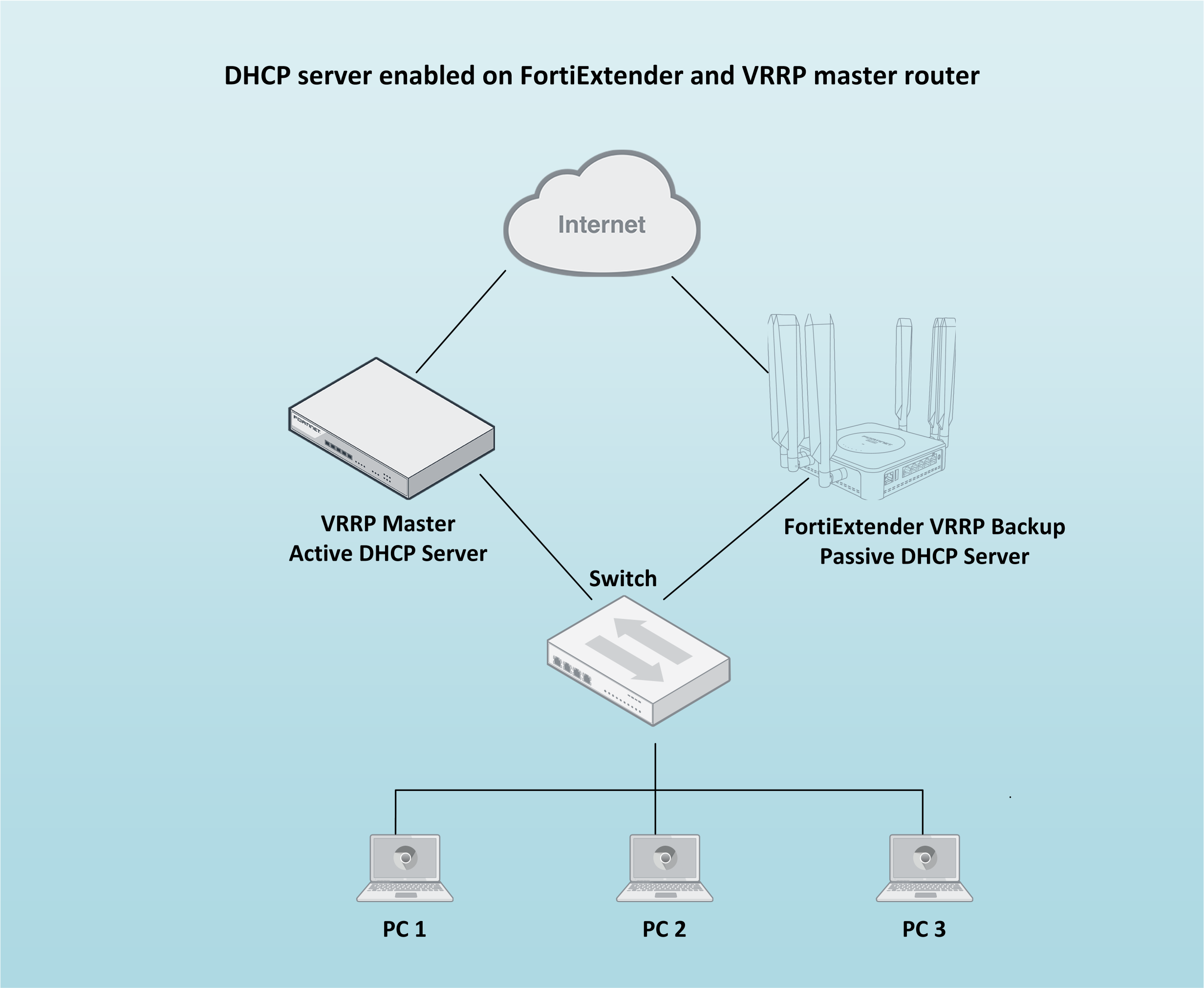
```
get router info vrrp
```

Enable DHCP server on FortiExtender and the VRRP master router

To ensure uninterrupted presence of a DHCP server when one of the VRRP-capable routers is down, you must ensure IP address availability all the time. Typically both the VRRP master and the backup routers are configured with DHCP servers with reserved IP addresses to their corresponding MAC addresses.

FortiExtender configured in VRRP backup mode will not launch the replicated copy of the DHCP server until and unless the VRRP master router goes down; FortiExtender will also terminate the DHCP server when the VRRP master router comes back up.This ability ensures that the hosts in the VRRP domain always gets the same IP address, irrespective of which VRRP router is in operation, without causing any IP address conflicts.

For information on DHCP server configuration, refer to Configure DHCP server on page 25.


DHCP server enabled on FortiExtender and VRRP master router
Internet
VRRP Master
Active DHCP Server
FortiExtender VRRP Backup
Passive DHCP Server
Switch
PC 1
PC 2
PC 3

Enable DHCP relay on both FortiExtender and the VRRP master router

You must guarantee IP address availability to ensure access to the DHCP server at any time. The hosts must be able to access a DHCP server locally or remotely on an uninterrupted basis. In the event that the DHCP server is not present locally, a DHCP relay agent service is needed to receive DHCP requests from DHCP hosts and forwards the requests to the remote DHCP server, receive responses from the server, and cater to the needs of DHCP clients. In this configuration, the FortiExtender which acts in VRRP backup mode will be running a DHCP relay agent on a VRRP interface; the VRRP master router is also running a DHCP relay agent on the respective VRRP interface. This ability ensures that the hosts in the VRRP domain always gets the same IP address, irrespective of which VRRP router is in operation, without causing any IP address conflicts because the requests are catered to by the same remote DHCP server.

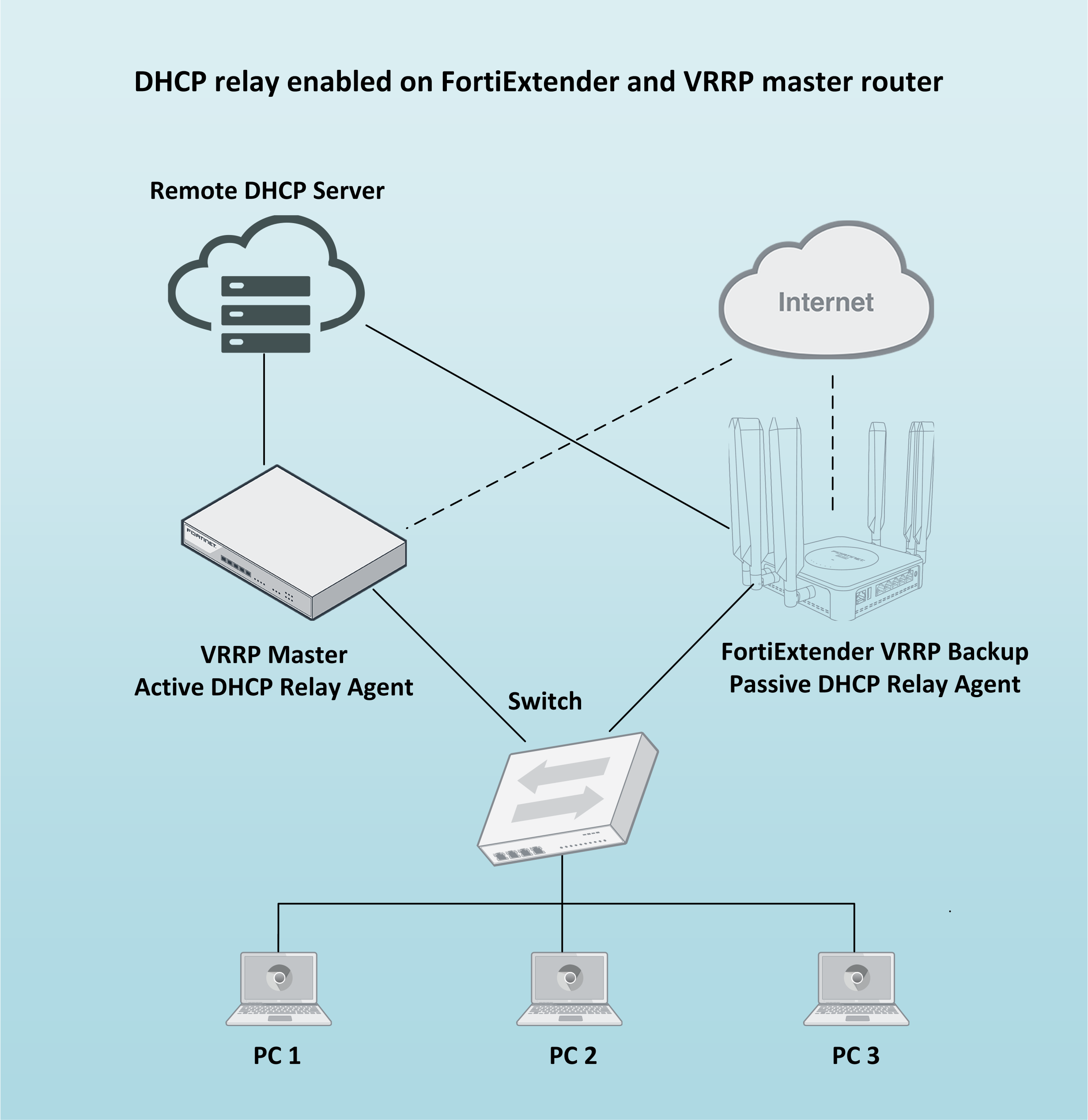
For information on DHCP relay configuration, refer to Configure DHCP relay on page 27DHCP configurations on page 25

DHCP relay

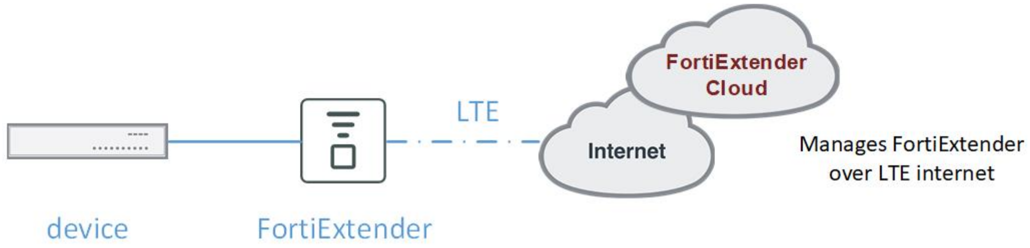
FortiExtender now supports DHCP relay agent which enables it to fetch DHCP leases from a remote server. It has to be configured per interface. Example below:

```
config system dhcprelay
   edit 1
   set status enable
   set client-interfaces <vrrp interface name on which relay agent services are
         offered>
   set server-interface <interface name through which DHCP server can be reachable>
   set server-ip <remote dhcp server IP>
end
```

The DHCP relay and DHCP server services can be run on any VRRP interface, which could be either a separate port or a VLAN interface.


DHCP relay enabled on FortiExtender and VRRP master router
Remote DHCP Server
Internet
VRRP Master
Active DHCP Relay Agent
FortiExtender VRRP Backup
Passive DHCP Relay Agent
Switch
PC 1
PC 2
PC 3

Manage from FortiExtender Cloud



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

- A FortiCare account
- A FortiExtender Cloud license (The current SKU: FC-10-X0CME-608-02-DD)

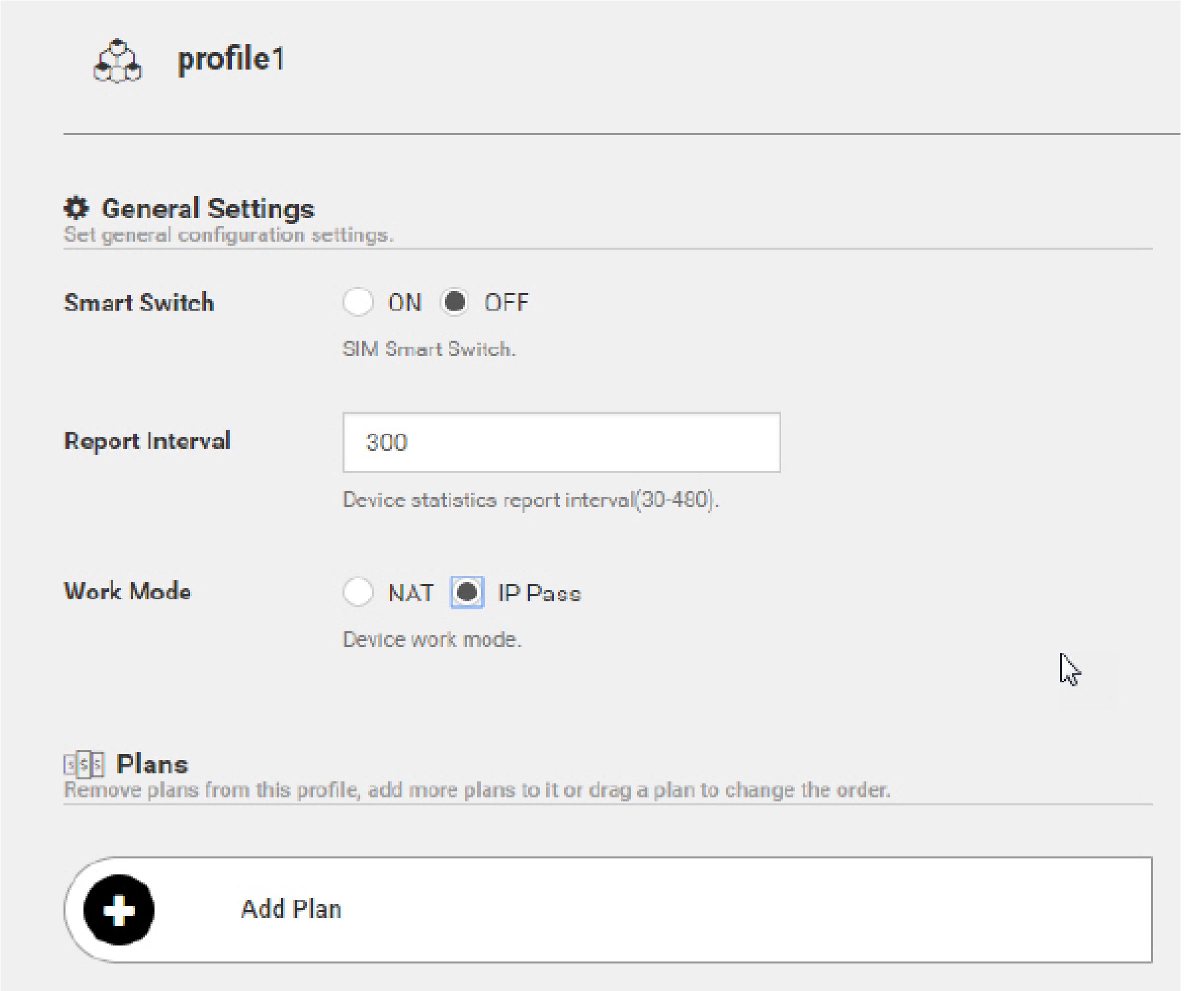
Configure with FortiExtender Cloud

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 300

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.

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 client 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/adapter. 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/adapter is used, execute the following command:

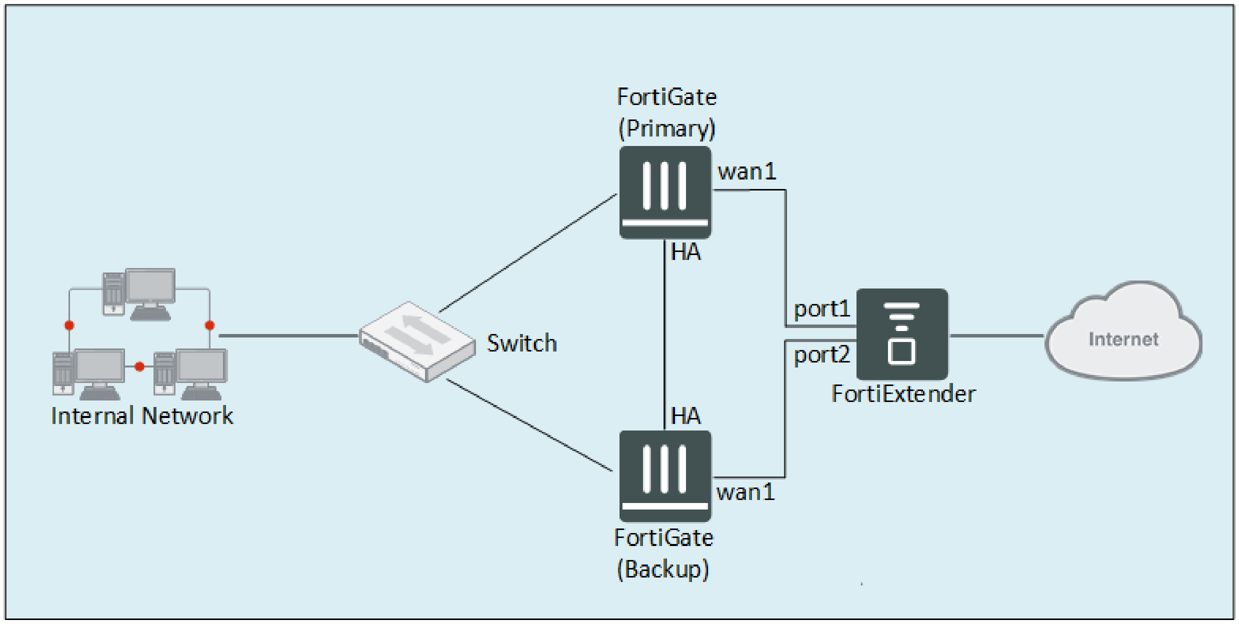
```
# execute obm-console
Welcome to OBM Console - Serial Redirector.
There are 2 devices/ports connected.
Please choose one from list below:
1. ttyUSB0
2. ttyUSB1
Please choose the baudrate from list below:
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
6. 921600
7. Other baudrate
Enter to continue &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

```
FX211E5919000011 # config system interface
FX211E5919000011 (interface) # edit lan
FX211E5919000011 (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
next

FX211E5919000011 # config system lan-switch
FX211E5919000011 (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

Below are some common error situations with their suggested solutions.

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?`
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	`get extender status`
Check connectivity to FortiExtenderCloud	`get cpm status`
Check the status of modems	`get modem status`
Perform health checks and monitoring	`get hmon hchk vwan.<vwan_member name>` (The member can be tunnel0 or tunnel1.)
Logs on telnet/ssh	`execute debug log-to-console on`
Perform modularized debugging	1. Select the module. 2. Turn the log level on/off as needed.
Debug	`execute debug <module> <log level> on/off`
	`SYSTEM,MONITORD, EXTD, MDMD, CONNMGR,NETD,CLI,GUI CPM,CONFIG,JCLI,HMON,IPSecD,FIREWALLD`
Applicable log levels	`error, info, dbg, fatal, warning, trace`

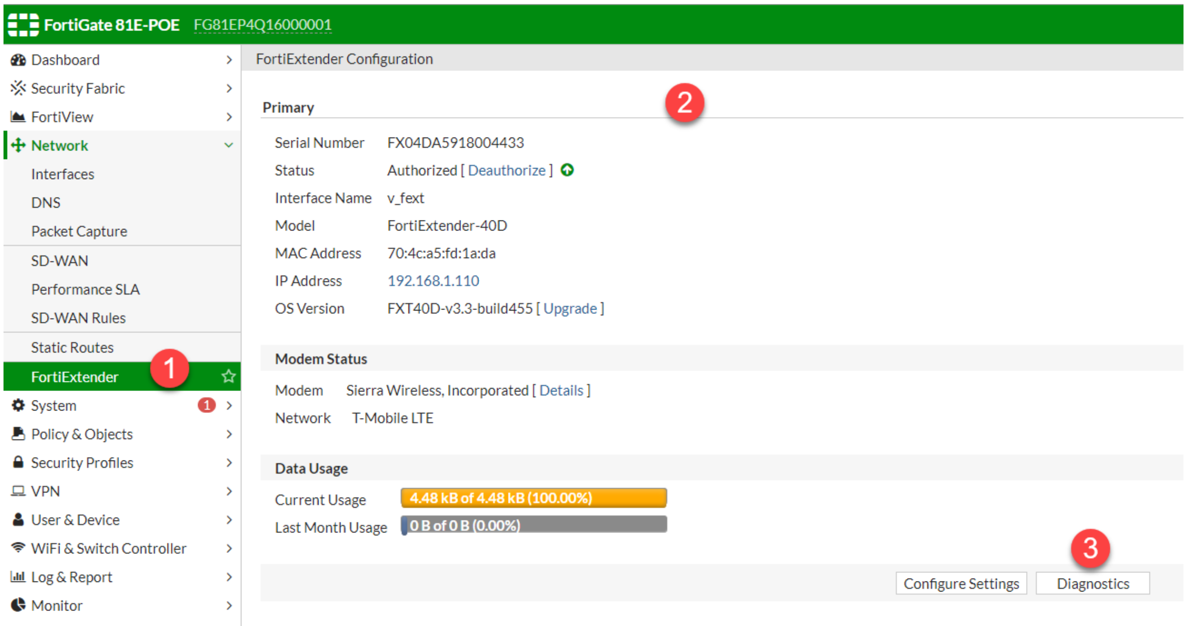
Diagnose FortiExtender

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

- From FortiGate
- From FortiExtender Cloud
- From Telnet.

Diagnose from FortiGate

1. Open a browser to access the FortiGate GUI.
2. From the main FortiGate window, go to **Network > FortiExtender**, as illustrated below.



FortiExtender Configuration

Primary

Serial Number	FX04DA5918004433
Status	Authorized [Deauthorize]
Interface Name	v_fext
Model	FortiExtender-40D
MAC Address	70:4c:a5:fd:1a:da
IP Address	192.168.1.110
OS Version	FXT40D-v3.3-build455 [Upgrade]

Modem Status

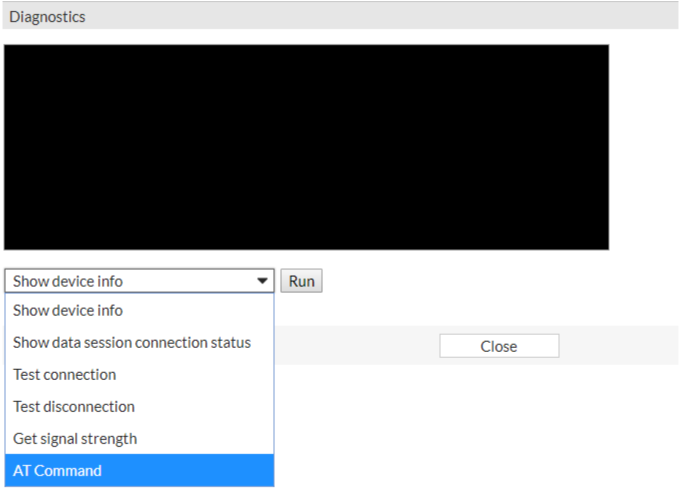
Modem	Sierra Wireless, Incorporated [Details]
Network	T-Mobile LTE

Data Usage

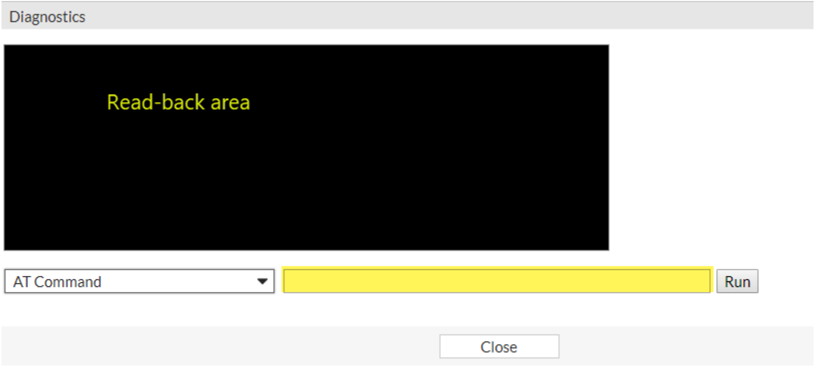
Current Usage	4.48 kB of 4.48 kB (100.00%)
Last Month Usage	0 B of 0 B (0.00%)

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

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



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

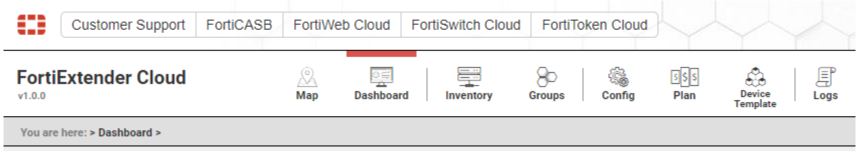


5. Type a command into the text box, and click **Run**.
   The output shows in the read-back area.

For a complete list of diagnostic commands, refer to Status, diagnostics, and debugging commands on page 90.

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 90.

Diagnose from Telnet

1. From the Windows Command prompt, type `cmd`.
2. Type `telnet [modem ip address]`. (The default IP address is 192.168.100.20/24.)
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 90.

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	First update, replacing the content in "OBM management".
August 3, 2020	FortiExtender 4.2.1 Admin Guide, initial release.