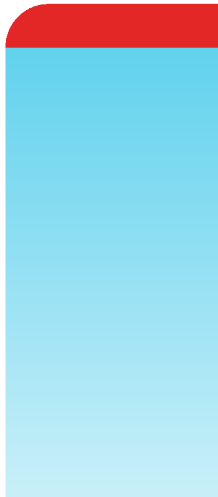
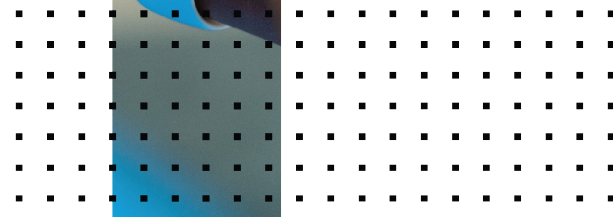


Admin Guide

FortiExtender (Standalone) 7.4.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



July 14, 2023

FortiExtender (Standalone) 7.4.1 Admin Guide

TABLE OF CONTENTS

Introduction	7
Supported hardware models	8
Getting started	9
Check current manage mode	9
Main LTE/5G features	10
Cellular capabilities	10
Supported wireless carriers	11
SIM mapping	12
Add a data plan and APN	12
Global SIM with roaming on	13
SIM-switch	13
SIM switch-back	14
Configure SIM-switch based on link health	14
Get modem status	16
Stopping data traffic on overaged LTE interface	17
OBM management	17
Unlock SIM pin	18
Modes of operation	19
IP pass-through mode	19
Enable IP pass-through mode	19
Configure a virtual wire pair	19
NAT mode	20
Destination Network Address Translation (DNAT)	20
Interface management	22
Interface configuration guideline	23
Physical interface(s)	23
LTE interface	23
Tunnel interface	23
Virtual-WAN interface	23
Access allowance	24
Get interface status	25
Configure LAN switch	26
Configure switch interface	27
Configure VXLAN interface	28
SFP DSL support	28
Aggregate interface support with load-balancing	29
Configure a private network	30
Configure Virtual-WAN interface	31
DHCP configurations	34
Configure DHCP server	34
Configure DHCP relay	36

DHCP relay over VPN	37
DHCP client optimization	37
Network utilities	38
Address	38
Service	38
System routing	39
Configure static routing	39
Configure dynamic routing — OSPF	40
Configure OSPF from Console (CLI)	40
Verify OSPF configurations	45
Configure OSPF GUI	47
Complete OSPF configuration code example	48
Configure PBR routing	50
View routing configurations	51
Move PBR rules	52
Configure multicast routing	53
Target	53
Firewall	55
Configure address/subnet	55
Configure protocol/port range	55
Configure firewall policies	56
Move firewall policies	57
VPN	59
Configure VPN	59
Configure phase-1 parameters	60
Configure phase-2 parameters	61
Configure firewall policies	64
Check VPN tunnel status	65
IPsec VPN support for third-party certificates	65
Import third-party certificates	65
Use third-party certificates for IKE authentication	66
DNS Service	67
Enable DNS service	67
Set up DNS database	68
Check DNS statistics	70
Dump the DNS cache	70
Clear the DNS cache	70
Dump the DNS database	70
Force DNS request to go through DNSPROXY	71
SD-WAN	74
Configure an SD-WAN	74
Check SD-WAN health	75
Define an SD-WAN member	76
Health monitoring	78
Monitor interface status	78

Perform link health check	79
Configure health monitoring	81
System management	82
API handling of error messages	82
Add trusted hosts	83
Activate the default admin account	84
Multiple static access controller addresses or FQDN	84
Get system version	85
Get user session status and force log-out	85
Upgrade OS firmware	86
TFTP	86
FTP	86
USB	86
FortiExtender Cloud	87
GUI	87
Upgrade modem firmware	87
TFTP	87
FTP	87
USB	87
FortiExtender Cloud	87
GUI	88
SMS notification	88
Remote diagnostics via SMS	88
Export system logs to remote syslog servers	89
Configure syslog database array	89
Support for SNMP (read-only) and traps	90
Typical SNMP commands	90
Sample SNMP commands	91
Executable SNMP commands	92
Get MIB2 interface statistics via SNMP	93
Access other devices via SSH	93
Dual modems	94
Dual modems in NAT mode	94
Troubleshooting, diagnostics, and debugging	95
Troubleshooting	95
Can't manage the FortiExtender (Standalone) from FortiExtender (Standalone) Cloud	95
Can't start an Internet session	95
Status, diagnostics, and debugging commands	96
Diagnose from Telnet	96
Collect complete diagnostics information	96
Appendix A: Configure LTE settings	98
Add a new carrier profile	98
Add a new operator/carrier	98
Create a data plan	99
Activate a SIM card	100

Configure start session timeout	101
Check the recorded SIM card IMSI number	102
Delete the recorded SIM card IMSI number	102
Set the default SIM	102
Set the default SIM by preferred carrier	103
Set the default SIM by low cost	103
Set the default SIM by SIM slot	103
Enable SIM-switch	103
Unlock SIM pin	104
Dual modems	105
Dual-modem in IP pass-through mode	105
Dual modems in NAT mode	106
Change Log	107

Introduction

FortiExtender is a plug-and-play customer premises equipment (CPE) device. As a 3G/4G LTE and 5G 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. You can deploy it both indoors and outdoors by choosing the right model and appropriate enclosures.

FortiExtender can be deployed in standalone mode as a wireless router, managed individually or centrally from FortiExtender Cloud, or managed by FortiGate as part of the integrated Fortinet Fabric Solutions.

This *Guide* is for standalone locally managed FortiExtender only. For information about FortiExtender managed by FortiGate or by FortiExtender Cloud, refer to their respective Admin Guides.

Supported hardware models

FortiExtender 7.4.1 supports the following hardware models:

Model	Market
FortiExtender 201E	North and South Americas, EMEA, and some APAC carriers
FortiExtender 211E	Global
FortiExtender 101F-AM	North America
FortiExtender 101F-EA	EMEA, Brazil, and some APAC carriers
FortiExtender 200F	Global
FortiExtender 201F-AM	North America
FortiExtender 201F-EA	EMEA, Brazil, and some APAC carriers
FortiExtender 202F-AM	North America
FortiExtender 202F-EA	EMEA, Brazil, and some APAC carriers
FortiExtender 212F	Global
FortiExtender 311F	Global
FortiExtender 511F	Global
FortiExtenderVehicle 211F	Global
FortiExtenderVehicle 211F-AM	North America

For more information about FortiExtender OS and hardware compatibility, see [FortiExtender OS & Hardware Platform Compatibility Matrix](#).



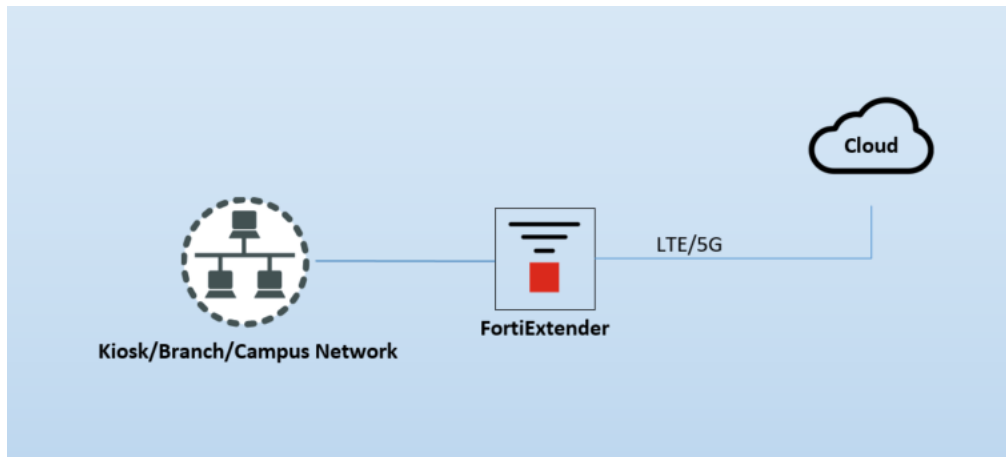
All built-in modems can be upgraded with compatible, wireless service provider-specific modem firmware.



FortiExtender 201E, 211E, 101F, 201F, 202F, 212F, 311F, 511F and FortiExtenderVehicle 211F devices come with a Bluetooth button, which is turned off by default. 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.

Getting started

FortiExtender works as a standalone device when it is not managed by FortiGate or FortiExtender Cloud. A standalone FortiExtender can work in either IP pass-through or NAT mode. You can configure a standalone FortiExtender device from its CLI (Console/SSH) or GUI.



Check current manage mode

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

```
FX511F5921000053 # get extender status
Extender Status
  name           : FX511F5921000053
  mode           : CLOUD
  fext-addr      : 192.168.237.1
  fext-wan-addr  : 25.75.193.57
  controller-addr : fortiextender-dispatch.forticloud.com:443
  deployed       : true
  account-id     : 343849
  uptime         : 5 days, 17 hours, 2 minutes, 45 seconds
  management-state : CWS_RUN
  base-mac       : E8:ED:D6:03:D2:58
  network-mode   : ip-passthrough
  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
```

Main LTE/5G features

FortiExtender (Standalone) offers the following main LTE/5G features:

- [Cellular capabilities on page 10](#)
- [Supported wireless carriers on page 11](#)
- [SIM mapping on page 12](#)
- [Add a data plan and APN on page 12](#)
- [Global SIM with roaming on on page 13](#)
- [SIM-switch on page 13](#)
- [Get modem status on page 16](#)
- [Stopping data traffic on overaged LTE interface on page 17](#)
- [OBM management on page 17](#)
- [Unlock SIM pin on page 104](#)



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

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

FortiExtender 511F supports 5G using the following frequencies:

- **5G NR:** n1, n3, n5, n7, n8, n20, n28, n38, n40, n41, n77, n78, and n79,
- **LTE-FDD Bands:** 1, 3, 5, 7, 8, 18, 19, 20, 26, 28, and 32
- **LTE-TDD Bands:** 34, 38, 39, 40, 41, 42, and 43
- **WCDMA Bands:** 1, 3, 5, 6, 8, and 19

Supported wireless carriers

By default, FortiExtender (Standalone) supports all major wireless carriers in Europe and North America, including the following:

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



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

```
config lte carrier
edit free
    set firmware SWI9X30C_02.32.11.00.cwe
    set pri SWI9X30C_02.32.11.00_GENERIC_002.064_000.nvu
next
```



FortiExtender (Standalone) 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 (Standalone) 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 (Standalone) 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 <carrier name>
FX201E5919000035 (1) <M> # next
```



FortiExtender (Standalone) 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 (Standalone) 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 may need an Access Point Name (APN) to establish a Packet Data Network (PDN) connection with a wireless carrier. An APN may be required for a cellular 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 sometimes may not be established without a valid APN. Always be aware of the APN of the SIM card that you are using. If you are not sure, contact your network service provider (NSP) for assistance.

Global SIM with roaming on

FortiExtender (Standalone) must always run on the modem firmware compatible with the native wireless operator's SIM. Most of the providers in the world can work with the "generic" modem firmware included with the FortiExtender (standalone) image. 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 "Auto switch" setting.

FortiExtender (Standalone) 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 (Standalone) 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 (Standalone) 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 (Standalone) 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 or locally from the FortiExtender GUI. All the aforementioned parameters can be configured from the FortiExtender (Standalone) 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) #
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).

Configure SIM-switch based on link health

FortiExtender enables you to configure automatic SIM switch based on the link health.



For more information, refer to the CLI Reference Guide.

To use this feature:

1. Configure an hmon hchk instance:

```
config hmon hchk
  edit sim-health
    set protocol ping
    set interval 10
    set probe-cnt 1
    set probe-tm 2
    set probe-target 166.253.42.211
    set interface lte1
    set src-type none
    set filter loss
  next
end
```

2. Link the auto-switch instance to the config hmon hchk instance:

```
FX511FTQ21001152 # config lte setting modem1 auto-switch
FX511FTQ21001152 (auto-switch) # show
config lte setting modem1 auto-switch
  set by-disconnect disable
  set by-signal disable
  set by-data-plan disable
  set by-health-monitor enable
  config health-monitor
    set event sim-health
    set fail-cnt 3
    set recovery-cnt 2
    set by-latency enable
    set latency-threshold 150
    set by-jitter enable
    set jitter-threshold 150
    set recover-by-reboot enable
    set max-switches-allowed 4
    set max-switches-interval 1800
  end
```

Parameter	Description
event sim-health	"sim-health" refers to the config hmon hchk instance above.
fail-cnt 3	The link is deemed unusable if three pings have failed.
recovery-cnt 2	The link is considered usable if two pings have succeeded.
by-latency	Enable/Disable latency monitoring on the active SIM card.
latency-threshold	Latency in milliseconds for SLA to make decisions.
by-jitter	Enable/Disable jitter monitoring on the active SIM card.

Parameter	Description
jitter-threshold	Jitter in milliseconds for SLA to make decisions.
recover-by-reboot [disable enable]	Enable/Disable. If enabled, the system will reboot if the following two conditions are met: <ul style="list-style-type: none"> max-switches-allowed max-switches-interval See below.
max-switches-allowed 5	5 switches
max-switches-interval 1800	Within 1,800 seconds

Get modem status

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

```
FX201E5919002499 # 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
```

Stopping data traffic on overaged LTE interface

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

- NATed traffic
- VPN data traffic on IPsec Tunnel based on the overaged LTE interface
- IP-passthrough traffic

OBM management

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

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

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

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

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

```
# execute obm-console
Welcome to OBM Console - Serial Redirector.
There are 2 devices/ports connected.
Please choose one from list below:
1. ttyUSB0
2. ttyUSB1
Please choose the baudrate from list below:
1. 9600
2. 19200
```

```
3. 38400
4. 57600
5. 115200
6. 921600
7. Other baudrate
Enter to continue & CTRL+X to go back to FortiExtender Console.
```

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

Unlock SIM pin

A SIM card is automatically locked following three incorrect pin uses. You can unlock a locked SIM card with PUK code using AT commands.



This feature applies to FEX-511F only.

To unlock a SIM card with PUK code:

1. Pause the modem manager to prevent SIM switching:

```
config lte setting
  config modem1
    set pause-modem-manager enable
  end
```

2. Run the following command with the appropriate PUK code and new SIM pin.

```
execute modem modem1 sim1 puk unlock 12345678 1111
```

Note: In the sample code above, the PUK is 12345678 and the new SIM pin is 1111.

3. Disable pause-modem-manager in Step 1 above.

```
set pause-modem-manager disable
```

4. Configure the newly configured SIM pin, i.e., 1111 in the example above, to activate the session.

Modes of operation

This section covers the following topics:

- [IP pass-through mode on page 19](#)
- [NAT mode on page 20](#)

IP pass-through mode

In IP pass-through mode, FortiExtender (Standalone) distributes the WAN IP address provided by the NSP to the device behind it.

Enable IP pass-through mode

FortiExtender (Standalone) can be used as a stand-alone device, without integration with FortiGate or FortiExtender (Standalone) Cloud. In this scenario, all configuration is done locally on the FortiExtender (Standalone) 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
```

There can be only a single device behind FortiExtender (standalone) when in IP-passthrough mode. That device can be either a router that NATs the traffic behind or a PC, but it cannot be a switch (L2 or L3) without NAT.

Configure a virtual wire pair

A virtual wire pair configuration is necessary to enable IP pass-through forwarding between two ports. Configuration of ip-pass-through mode differs, depending the port on which the DHCP server is configured. There are two scenarios:

If a LAN port (port1 through port3) is being used, we recommend that you disable the DHCP server before setting FortiExtender in IP pass-through mode:

```
config system virtual-wire-pair
    set ltel-mapping lan
end
```

If port4 is being used, no such action is required:

```
config system virtual-wire-pair
    set ltel-mapping port4
end
```



For best practice, plug in port4 when setting FortiExtender in IP pass-through mode.

NAT mode

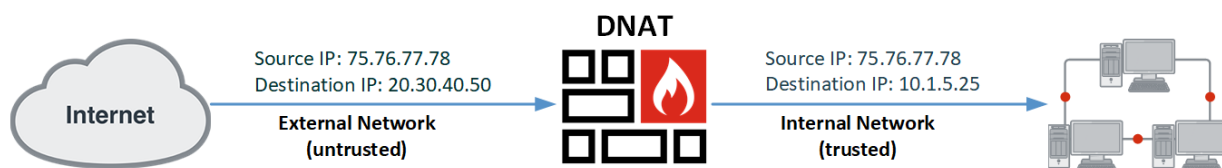
The LAN port on FortiExtender (Standalone) can support multiple devices (e.g., PCs, printers, etc.) in NAT mode. In this mode, FortiExtender (Standalone) works as a gateway of the subnet behind it to forward traffic between the LAN and the LTE WAN.

The following features are supported in NAT mode:

- [Interface management on page 22](#)
- [DHCP configurations on page 34](#)
- [System routing on page 39](#)
- [Configure PBR routing on page 50](#)
- [Firewall on page 55](#)
- [VPN on page 59](#)
- [SD-WAN on page 74](#)
- [Health monitoring on page 78](#)

Destination Network Address Translation (DNAT)

Destination Network Address Translation (DNAT) is used by an external host to initiate connection with a private network. It translates the public IP address of an external host to the private IP of an internal host. DNAT can also translate the destination port in TCP/UDP headers. The mapping can include all TCP/UDP ports or only refers to specific configured ports if port forwarding is enabled.



DNAT comes into play when an external untrusted network initiates communication with an internal secured network. It allows any host on the internet to reach a single host on the LAN.

DNAT changes the destination address in the IP header of a packet, and may also alter the destination port in TCP/UDP headers. It is commonly used to redirect incoming packets with a destination of a public address/port to a private IP address/port inside an internal network. For example, DNAT is used to allow external internet users to access a web service hosted inside a data center behind a firewall.

In essence, DNAT changes the destination address of packets passing through the router. The translation happens before the routing decision is made.

Interface management

FortiExtender (Standalone) 201E and 211E each come with four LAN Ethernet ports and one WAN Ethernet port. FortiExtender 511F adds another WAN port with 1GigE SFP fiber 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 functions as a router when in NAT mode.

- 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
<code>config system interface</code>	Enters system interface configuration mode.
<code>edit <interface_name></code>	Specify or edit interface name (lan, lo, lte1 or wan).
<code>set type <type></code>	Select the interface type: <ul style="list-style-type: none"> • <code>lan-switch</code>—LAN interface (Can be edited only). • <code>physical</code>—LAN interface (Can be edited only). • <code>lte</code>—LTE interface (Can be edited only). • <code>loopback</code>—Loopback interface (Can be edited only). • <code>tunnel</code>—Tunnel interface (Can be created, edited, or deleted). • <code>virtual-wan</code>—Virtual WAN interface (Can be created, edited, or deleted). • <code>vlan</code>—Vlan interface (Can be created, edited, or deleted) • <code>dummy</code>—Dummy interface (Can be created, edited, or deleted) • <code>capwap</code>—Capwap interface (Can edited only) • <code>vxlan</code>—Vxlan interface (Can edited only) • <code>aggregate</code>—Aggregate interface (Can edited only) • <code>switch</code>—Switch interface (Can edited only)
<code>set status {up down}</code>	Specify the interface state: <ul style="list-style-type: none"> • <code>up</code>—Enabled. • <code>down</code>—Disabled.
<code>set mode {static dhcp}</code>	Set the interface IP addressing mode: <ul style="list-style-type: none"> • <code>static</code>—If selected, FortiExtender (Standalone) will use a fixed IP address. See <code>set ip <ip></code> below. • <code>dhcp</code>—If selected, FortiExtender (Standalone) will work in DHCP client mode.
<code>set ip <ip></code>	(Applicable only when IP addressing mode is set to "static".) Specify an IPv4 address and subnet mask in the format: <code>x.x.x.x/24</code>
<code>set gateway <gateway></code>	Set an IPv4 address for the router in the format: <code>x.x.x.x</code>

CLI command	Description
<code>set mtu <mtu></code>	Set the interface's MTU value in the range of 512—1500.
<code>allowaccess {ping http https telnet}</code>	Select the types of management traffic allowed to access the interface: <ul style="list-style-type: none">• ping—PING access.• http—HTTP access.• https—HTTPS access.• telnet—TELNET access.• ssh—Secure Shell access.• snmp—SNMP access.

Interface configuration guideline

The following are the general guidelines regarding system interface configurations.

Physical interface(s)

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

FortiExtender (Standalone) 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 10](#).

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
  edit lan
    set type lan-switch
    set status up
    set mode static
    set ip 192.168.180.45/24
    set gateway
    set mtu-override disable
    set distance 50
    set vrrp-virtual-mac disable
    config vrrp
      set status disable
    end
  set allowaccess
```

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

snmp

FX211E5919000009 (wan) #
```

Access allowance

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

- SSH
- Telnet

- ping
- HTTP
- HTTPS
- SNMP



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 (Standalone) via LTE, you must use FortiExtender (Standalone) Cloud.

Get interface status

Use the following command to get system interface status:

```
FX511FTQ21001262 # get system interface
== [ port4 ]
name: port4                status: online/up/link up      type: physical      mac:
94:ff:3c:0d:1e:30          mode: static                   ip: 0.0.0.0/0        mtu: 1500
                           gateway: 0.0.0.0
== [ wan ]
name: wan                  status: online/up/link up      type: physical      mac:
94:ff:3c:0d:1e:34          mode: static                   ip: 10.107.41.45/24   mtu: 1500
                           gateway: 0.0.0.0
== [ sfp ]
name: sfp                  status: online/up/link down    type: physical      mac:
94:ff:3c:0d:1e:35          mode: dhcp                    ip: 0.0.0.0/0        mtu: 1500
                           gateway: 0.0.0.0
== [ lan ]
name: lan                  status: online/up/link up      type: lan-switch     mac:
94:ff:3c:0e:1e:30          mode: static                   ip: 192.168.180.45/24 mtu: 1500
                           gateway: 0.0.0.0
== [ 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
== [ ltel ]
name: ltel                 status: online/up/link up      type: lte            mac:
ca:45:59:b1:5f:db          mode: dhcp                    ip: 192.0.0.2/27      mtu: 1472
                           gateway: 192.0.0.1            dns: 192.0.0.1
== [ vwan ]
name: vwan                 status: online/up/link up      type: virtual-wan     mac:
fe:f3:55:af:53:fa          mode: static                   ip: 0.0.0.0/0         mtu: 1472
                           gateway: 0.0.0.0
== [ test511 ]
name: test511              status: online/up/link down    type: tunnel         mac:
00:00:00:00:00:00          mode: static                   ip: 0.0.0.0/0         mtu: 1332
                           gateway: 0.0.0.0
```

Configure LAN switch

FortiExtender (Standalone) comes with four LAN ports (i.e., Ports 1—4) which can be part of the same LAN switch. These ports can also 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 in the example above:

```
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 from the state above:

```
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
```

Configure switch interface

A software switch is a virtual switch that is implemented at the software or firmware level. It can be used to simplify communication between devices connected to different FortiExtender interfaces. For example, using a software switch, you can place the FortiExtender interface connected to an internal network on the same subnet as your other virtual interfaces, such as VXLAN, aggregate interfaces, and so on.

Similar to a hardware switch, a software switch functions like a single interface. It has an IP address, and all the interfaces in the software switch are on the same subnet. Traffic between devices connected to each interface is not regulated by security policies, while traffic passing in and out of the switch is controlled by the same policy.

When setting up a software switch, consider the following:

- Ensure that you have a backup of your configuration.
- Ensure that you have at least one port or connection, such as the console port, to connect to the FortiExtender unit. This ensures that, if you accidentally combine too many ports, you have a way to undo the error.
- The ports that you include must not have any link or relation to any other aspect of the FortiExtender unit, such as DHCP servers, security policies, and so on.

To create a software switch on the GUI:

1. Go to **Networking > Switch Interface**.
2. Click **Create Switch-Interface**.
3. Configure the name, interface members, and all the other required fields.
4. Click **Save**.

To create a software switch in the CLI:

```
FX511FTQ21001152 (switch-interface) # show
config system switch-interface
    edit switch1
        set members 1 2
        set stp enable
    next
end

FX511FTQ21001152 (switch1) # set
members Interfaces within the virtual switch.
stp Enable/disable spanning tree protocol.
```

Upon execution of the above commands, the following configuration will be automatically generated:

```
config system interface
    edit <interface>
        set type switch
        set status down
    next
end
```

You can update the IP, allowaccess, and the other configurations based on the switch interface. And this interface can also be used in configuring the DHCP server, firewall policies, routes, and some other modules.

Configure VXLAN interface

VXLAN encapsulates OSI Layer-2 Ethernet frames within Layer-3 IP packets using the standard destination Port 4789. VXLAN endpoints, known as VXLAN tunnel endpoints (VTEPs), terminate VXLAN tunnels which can be virtual or physical switch ports.

To add a VXLAN interface from GUI:

1. Go to **Networking>VXLAN**.
2. Click **Create VXLAN**.
3. Configure the name, VNI, remote IP, local IP, and dstport.
4. Click **Save**.



- The local IP must be an IP address of one of your system interfaces.
- The VNI must be unique on every single local IP.
- The destination port is 4789 by default. The valid range is 1—16777215.

To configure VXLAN from the CLI:

```
config system vxlan
  edit <vxlan>
    set vni <vni>
    set remote-ip <remote ip>
    set local-ip <local ip>
    set dstport 4789
  next
end
```

Upon execution of the above commands, the following configuration will be automatically generated:

```
edit vxlan1
  set type vxlan
  set status down
  set mode static
end
```

You can change the IP, allowaccess, mode, and some other configurations based on this VXLAN interface.

SFP DSL support

FortiExtender 7.2.2 sees the implement of the SFP DSL feature in FortiExtender 311F and 511F.

On these two platforms, the GUI offers an SFP interface that you can edit.

All interfaces can have the SFP feature. When SFP feature is enabled, you will have access to multiple options consecutively. FortiExtender follows the edit feature of the SFP on the interface, depending on user requirement

Aggregate interface support with load-balancing

Interfaces of the same type can be aggregated into a virtual aggregate interface as its members. A member of an aggregate interface can be monitored by HMON. A member is considered as healthy if its link is up and marked as ALIVE by HMON. Only a healthy member could be considered as a candidate for sending and receiving packets.

Interfaces are aggregated in either of the following ways:

- **Active backup**—Only one member of the aggregate interface is active to send and receive packets at a time. One member should be designated as the primary and the others as secondary. If the primary member is healthy, it should be chosen as the active member. Otherwise, another healthy member must be chosen instead. Once the primary member becomes healthy again, it will take over the traffic.
- **Load balance**—All healthy members are active for sending and receiving packets. Packets are sent over active members based on the round-robin algorithm at the same time. Packets originated from the same source follow the same path.

Once an interface becomes a member of an aggregate interface, it must not be used for firewall and PBR. The aggregate interface must be used instead.

To create an aggregate interface in the GUI:

1. Go to **Networking>Aggregate Interface**.
2. Click **Create Aggregate Interface**.
3. Configure the ID, Mode, and Mapping timeout if mode is set to load balance.
4. Click **Create Member**.
5. Configure the Name, Interface, Weight/Role, HealthCheck, HealthCheckFailCount, and HealthCheckRecoveryCount of each member.

To create an aggregate interface in the CLI:

A table is added to `/config/system` to represent interface aggregations. Each table entry indicates an aggregate interface to be created and one or more interfaces can be aggregated under this aggregate interface.

The following configuration shows two aggregate interfaces in active backup and load-balance mode:

```
config system aggregate-interface
  edit aggl
    set mode loadbalance
    set mapping-timeout 60
    config members
      edit 1
        set interface vx2
        set health-check-event vxlan
        set health-check-fail-cnt 5
        set health-check-recovery-cnt 5
      next
      edit 2
        set interface vx3
        set health-check-event
        set health-check-fail-cnt 5
        set health-check-recovery-cnt 5
      next
    next
  next
```

```
        end
    next
    edit agg2
        set mode activebackup
        config members
            edit 1
                set interface wan
                set role primary
                set health-check-event
                set health-check-fail-cnt 5
                set health-check-recovery-cnt 5
            next
            edit 2
                set interface port4
                set role secondary
                set health-check-event
                set health-check-fail-cnt 5
                set health-check-recovery-cnt 5
            next
        end
    next
end
```

Following configuration will be automatically generated:

```
config system interface
    edit agg1
        set type aggregate
        set status down
    next
    edit agg2
        set type aggregate
        set status down
    next
end
```

You can update the IP, allowaccess, and other configurations based on the aggregate interface. And this interface can also be used in configuring the DHCP server, firewall policies, routes, and some other modules.

To get the aggregate interface status:

```
# get system aggregate-interface status
agg2:
    2(port4): linkdown UNKNOWN aggregated
    1(wan): linkup UNKNOWN aggregated active
agg1:
    2(vx3): linkup UNKNOWN aggregated active
    1(vx2): linkup ALIVE aggregated active
```

Configure a private network

Private network wireless solutions provide seamless, secure access to your corporate network. You can enable private network on your FortiExtender using the following commands:

```
config lte plan
```

```
edit test
set private-network enable
end
end
```

Configure Virtual-WAN interface

Step 1: Config VWAN health check

```
config hmon hchk
edit vw_mb1_hc
set protocol ping
set interval 5
set probe-cnt 1
set probe-tm 2
set probe-target 8.8.8.8
set interface wan
set src-type none
set filter rtt loss
next
edit vw_mb2_hc
set protocol ping
set interval 5
set probe-cnt 1
set probe-tm 2
set probe-target 8.8.8.8
set interface ltel
set src-type none
set filter rtt loss
next
end
```

Step 2: Configure VWAN members

```
config system vwan-member
edit mb1
set target target.wan
set priority 1
set weight 1
set in-bandwidth-threshold 0
set out-bandwidth-threshold 0
set total-bandwidth-threshold 0
set health-check vw_mb1_hc
set health-check-fail-threshold 5
set health-check-success-threshold 5
set link-cost-factor packet-loss latency jitter
set latency-threshold 5
set jitter-threshold 5
set packetloss-threshold 100
next
edit mb2
set target target.ltel
set priority 10
set weight 1
set in-bandwidth-threshold 0
```

```
set out-bandwidth-threshold 0
set total-bandwidth-threshold 0
set health-check vw_mb2_hc
set health-check-fail-threshold 5
set link-cost-factor packet-loss latency jitter
set latency-threshold 5
set jitter-threshold 5
set packetloss-threshold 100
```

Step 3: Configure VWAN interface

```
config system interface
edit vwan1
set type virtual-wan
set status up
set algorithm redundant
set redundant-by priority
set FEC source_dest_ip_pair
set session-timeout 60
set grace-period 0
set members mb1 mb2
next
end
```

Step 4: Confirm the subnet of LAN, and configure a network address instance

```
config network address
edit lan
set type ipmask
set subnet 192.168.2.0/24
next
end
```

Step 5: Configure firewall policies

```
config firewall policy
edit vwan_permit_out
set srcintf any
set dstintf vwan1
set srcaddr lan
set dstaddr all
set action accept
set status enable
set service ALL
set nat disable
next
edit vw_mb1_nat
set srcintf any
set dstintf wan
set srcaddr lan
set dstaddr all
set action accept
set status enable
set service ALL
set nat enable
next
```

```
edit vw_mb2_nat
    set srcintf any
    set dstintf ltel
    set srcaddr lan
    set dstaddr all
    set action accept
    set status enable
    set service ALL
    set nat enable
next
end
```

Step 6: Configure router policy

```
config router policy
    edit to_vwan
        set input-device
        set srcaddr lan
        set dstaddr all
        set service ALL
        set target target.vwan1
        set status enable
        set comment
    next
end
```

DHCP configurations

FortiExtender (Standalone) 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 (Standalone) 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
<code>config system dhcpserver</code>	Enters DHCP server configuration mode.
<code>edit <name></code>	Specify the name of the DHCP server.
<code>set status {enable disable backup}</code>	Set the DHCP server status: <ul style="list-style-type: none"> • <code>enable</code>—Enable the DHCP server. • <code>disable</code>—Disable the DHCP server. • <code>backup</code>—Enable in VRRP backup mode. (Note: The DHCP server is launched only when the VRRP primary goes down.)
<code>set lease-time <lease_ time></code>	Specify the DHCP address lease time in seconds. The valid range is 300–8640000. 0 means unlimited.
<code>set dns-service {default specify wan-dns}</code>	Select one of the options for assigning a DNS server to DHCP clients: <ul style="list-style-type: none"> • <code>local</code>—The IP address of the interface of the DHCP server that is added becomes clients' DNS server IP address. • <code>default</code>—Clients are assigned the FortiExtender (Standalone) configured DNS server. • <code>specify</code>—Specify up to three DNS servers in the DHCP server configuration. • <code>wan-dns</code>—The DNS of the WAN interface that is added becomes clients' DNS server IP address.
<code>set dns-server1 <dns_ server1></code>	Specify the IP address of DNS Server 1.
<code>set dns-server2 <dns_ server2></code>	Specify the IP address of DNS Server 2.

CLI command	Description
<code>set dns-server3 <dns_server3></code>	Specify the IP address of DNS Server 3.
<code>set ntp-service {default specify}</code>	Select an option for assigning a Network Time Protocol (NTP) server to DHCP clients: <ul style="list-style-type: none"> <code>local</code>—The IP address of the interface of the DHCP server that is added becomes clients' NTP server IP address. <code>default</code>—Clients are assigned the FortiExtender (Standalone) configured NTP servers. <code>specify</code>—Specify up to three NTP servers.
<code>set ntp-server1 <ntp_server1></code>	Specify the IP address of NTP Server 1.
<code>set ntp-server2 <ntp_server2></code>	Specify the IP address of NTP Server 2.
<code>set ntp-server3 <ntp_server3></code>	Specify the IP address of NTP Server 3.
<code>set default-gateway <gateway></code>	Specify the default gateway IP address assigned by the DHCP server.
<code>set netmask <netmask></code>	Specify the netmask assigned by the DHCP server.
<code>set interface <interface></code>	Specify the interface on which the DHCP server is expected to run.
<code>set start-ip <start_ip></code>	Specify the start IP address of the DHCP IP address range. For example, 192.168.1.100.
<code>set end-ip <end_ip></code>	Specify the end IP address of the DHCP IP address range. For example, 192.168.1.120.
<code>Set mtu <mtu size></code>	Specify the MTU size. The default value is 1500.
<code>Set reserved-address <enable/disable></code>	Set the reserved address enable or disable: <ul style="list-style-type: none"> <code>enable</code>—enable reserved address option by configuring ip, mac and action as reserved or block. <code>disable</code>—Disable reserved address option.

Example DHCP server configuration:

```

FX201E5919000222 (1) <M> # show
edit 1
    set status enable
    set lease-time 86400
    set dns-service default
    set ntp-service specify
    set ntp-server1
    set ntp-server2
    set ntp-server3
    set default-gateway 192.168.200.99
    set netmask 255.255.255.0
    set interface lan
    set start-ip 192.168.200.100

```

```
set end-ip 192.168.200.150
set mtu 1500
set reserved-address enable
config reserved-addresses
  edit 1
    set ip 192.168.200.101
    set mac 45:59:b1:5f:db:ca
    set action reserved
  next
end
next
```

FortiExtender (Standalone) 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 192.168.200.99/24 and runs a DHCP server serving addresses from 192.168.200.110. You can enable the management of LAN-side capabilities from FortiExtender (Standalone) 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>
```

DHCP relay over VPN

FortiExtender supports DHCP relay agent which enables it to fetch DHCP leases from a remote server. The configuration must be done by interface. In FortiExtender OS 7.2.3, DHCP relay can go over VPN without setting IP address on the tunnel interface.

```
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>
```

DHCP client optimization

In 7.2.2, FortiExtender (Standalone) has optimized its DHCP client module by introducing the renew DHCP lease command in its CLI, and checking and renewing DHCP lease information on its GUI. The following two new options have also been introduced under interface configuration:

- **defaultgw** — Enable/Disable using the gateway IP acquired from DHCP server. This option is enabled by default.
- **dns-server-override** — Enable/disable using the DNS servers acquired from DHCP server. This option is enabled by default.

```
### execute interface dhcpclient-renew [interface name]
"manually renew dhcp lease on certain interface"
e.g. renew WAN port DHCP lease
# execute interface dhcpclient-renew wan
    renewing dhcp lease on wan
```

```
### config system interface
"defaultgw and dns-server-override are shown when the interface mode is dhcp"
edit <name>
    set mode dhcp
    .....
        set defaultgw enable
        set dns-server-override enable
    next
```

Network utilities

You can define your network from the following aspects:

- [Address on page 38](#)
- [Service on page 38](#)
- [Target on page 53](#)

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
```

System routing

FortiExtender (Standalone) 7.4.1 supports [static routing](#) and [Policy Based Routing \(PBR\)](#). Dynamic routing, such as ISIS and EIGRP, is not supported in this release.



Both static routing and PBR apply to NAT mode only.

This section covers the following topics:

- [Configure static routing on page 39](#)
- [Configure PBR routing on page 50](#)
- [View routing configurations on page 51](#)
- [Move PBR rules on page 52](#)

Configure static routing

The table below describes the commands for configuring static routing.

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

Example static route configuration:

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

```

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

```

Configure dynamic routing — OSPF

Open Shortest Path First (OSPF) is a link state routing protocol and uses the shortest-path-first algorithm to find the best Layer 3 path. It is an Interior Gateway Protocol (IGP) and IP routing information is distributed throughout a single Autonomous System (AS) in an IP network. You can configure OSPF using both the FortiExtender Console (CLI) and GUI.

The current release only supports basic features for point-to-point network type over IPSEC tunnel and Area 0, and static routes and connected routes are allowed to be redistributed into the OSPF routing domain. Other features such as the network type, authentication type, multiple areas, stub areas, and summary-address, etc. are not supported in this release.



- Other dynamic routing protocols such as ISIS, EIGRP, and BGP are not supported in this release.
- Static routing, PBR, and OSPF apply to NAT mode only.

Configure OSPF from Console (CLI)

Below are the general steps you need to follow when configuring OSPF. You can click the topics for more information and instructions for each of the steps:

1. [Configure OSPF status on page 40](#)
2. [Configure OSPF router-id on page 41](#)
3. [Configure OSPF area on page 41](#)
4. [Configure OSPF network on page 41](#)
5. [Configure OSPF interface on page 42](#)
6. [Configure OSPF redistribution on page 42](#)

Configure OSPF status

CLI Command	Description
<code>set status [enable disable]</code>	Set the status of the OSPF: <ul style="list-style-type: none"> • enable—Enable OSPF • disable—Disable OSPF

Example configuration:

```

FortiExtender# config router ospf
    set status enable | disable

```

Configure OSPF router-id

CLI Command	Description
<code>set router-id [x.x.x.x]</code>	The router-id is a unique identity to the OSPF router. If no router-id is specified, the system will automatically choose the highest IP address as the router-id.

Example configuration:

```
ForitExtender# config router ospf
set router-id 192.168.100.127
```

Configure OSPF area

CLI Command	Description
<code>config area</code> <code>edit 0.0.0.0</code>	An area is a logical grouping of contiguous networks and routers in the same area with the same link-state database and topology. Note: The current release only supports Area 0 called the backbone area, and does not support multiple areas. All routers inside an area must have the same area ID to become OSPF neighbors. You can add Area 0 by editing Area 0.0.0.0

Example configuration:

```
ForitExtender# config router ospf
config area
edit 0.0.0.0
```

Configure OSPF network

CLI Command	Description
<code>config network</code> <code>edit [id]</code> <code>set prefix</code> <code>[X.X.X.X/Y]</code> <code>set area 0.0.0.</code> <code>Prefix</code>	Prefix is used to identify network/subnet address for advertising to the OSPF domain. <ul style="list-style-type: none"> id—string X.X.X.X—Network prefix Y—Netmask

Example configuration:

```
ForitExtender# config router ospf
config network
edit 1
set prefix 192.168.100.127/32
set area 0.0.0.0
next
edit 2
set prefix 192.168.100.0/30
set area 0.0.0.0
```

```

    next
End

```

Configure OSPF interface

CLI Command	Description
<pre> config ospf-interface edit [id] set status [enable disable] set interface <ospf- interface name> set mtu-ignore [enable disbale] set cost <0-65535> </pre>	<p>Configure the OSPF interface.</p> <ul style="list-style-type: none"> id—string status—enable/disable OSPF processing on the said interface. interface—must be the VPN tunnel interface as OSPF is built over IPSEC VPN. mtu-ignore—enable/disable. mtu-ignore prevents OSPF neighbor adjacency failure caused by mismatched MTUs. When mtu-ignore is enabled, OSPF will stop detecting mismatched MTUs before forming OSPF adjacency. When mtu-ignore is disabled, OSPF will detect mismatched MTUs, and OSPF adjacency is not established if MTU is mismatched. cost—Interface cost used to calculate the best path to reach other routers in the same area.

Example configuration:

```

FortiExtender# config router ospf
config ospf-interface
    edit 1
        set status enable
        set interface opaq
        set mtu-ignore enable
        set cost 5
    end
end

```

Configure OSPF redistribution

The current release allows both connected routes and static routes redistributed into the OSPF Domain.

The following are the summary steps for configuring OSPF redistribution:

1. Configuring prefix-list
2. Configuring route-map
3. Configuring redistribute

Step 1: Configuring redistribute

CLI Command	Description
<pre> config prefix-list edit <prefix-name> config rule edit <id> set action [permit deny] set prefix <X.X.X.X/Y> set ge 0 set le 0 next next </pre>	<p>Configure the <code>prefix-list</code> which defines the prefix (IP address and netmask) for the filter of redistribution.</p> <ul style="list-style-type: none"> <code>prefix-name</code>— for either static routes or connected routes <code>id</code>—rule-id (1-65535) <code>action</code>—permit/deny. Permit if it matches prefix network; deny if it does not match the exact prefix network. <code>le</code>—(less than or equal to). The <code>le</code> parameter can be included to match all more-specific prefixes within a parent prefix up to a certain length. For example, <code>10.0.0.0/24 le 30</code> will match <code>10.0.0.0/24</code> and all prefixes contained within a length of 30 or less. <code>ge</code>— (greater than or equal to) The length specified should be longer than the length of the initial prefix.

Example configuration:

```

ForitExtender# config router
  config prefix-list
    edit local-nets
      config rule
        edit 10
          set action permit
          set prefix 192.168.201.0/24 set ge 0
          set le 0
        next
      end
    next
  edit static-routes
    config rule
      edit 10
        set action deny
        set prefix 192.168.203.0/24 set ge 0
        set le 0
      next
      edit 20
        set action permit
        set prefix 192.168.202.0/24 set ge 0
        set le 0 next
    end
  
```

Step 2: Configuring route-map

CLI Command	Description
<pre> config route-map edit <route-map name> config rule edit <id> </pre>	<p>Configure <code>route-map</code> which defines the redistributed routes.</p> <ul style="list-style-type: none"> <code>route-map name</code>—defines the route-map name <code>rule</code>—routing rule

CLI Command	Description
<pre> set action [permit deny] set match-ip- address <prefix- list> </pre>	<ul style="list-style-type: none"> • id—rule-id (1—65535) • action—permit/deny. If set to permit, the system redistributes the permitted prefix-list; if set to deny, the system does not redistribute the permitted prefix-list. • match-ip-address—Configure the prefix-list and identifies the prefix list defined in the prefix-list section. <p>Note: Route-maps are numbered with edit IDs, which are sequential numbers such as 10, 20, etc. We recommend starting with Number 10 to reserve numbering space in case you need to insert new matched/denied condition in the future.</p>

Example configuration:

```

ForitExtender# config router
config route-map
    edit redist-local-connected
        config rule
            edit 10
                set action permit
                set match-ip-address local-nets
        end
    edit redist-static
        config rule
            edit 10
                set action permit
                set match-ip-address static-routes

```

Step 3: Configuring redistribution

CLI Command	Description
<pre> config router ospf config redistribute config [connected static] set status [enable disable] set metric-type [1 2] set metric <value> set route-map <route-map name> </pre>	<p>Configure router OSPF redistribute.</p> <ul style="list-style-type: none"> • status—enable/disable redistributing routes. • metric-type—specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default). • metric value—used for the redistributed routes. The value range is from 1 to 16777214. The default is 10. • routemap—defined and configured on the route-map, see Configure route-map for details.

Example configuration:

```

ForitExtender# config router ospf
config redistribute
    config connected
        set status enable

```

```

        set metric-type 2
        set metric 10
        set routemap redist-local-connected
    end
    config static
        set status enable
        set metric-type 2
        set metric 10
        set routemap redist-static

```

Verify OSPF configurations

Upon completing the OSPF configurations, you may want to double-check to ensure that it works as expected.

- [Verify OSPF status on page 45](#)
- [Verify OSPF interface on page 46](#)
- [Verify OSPF neighbor adjacency on page 46](#)
- [Verify OSPF database on page 46](#)
- [Verify OSPF routes on page 46](#)
- [Verify routing table on page 47](#)

Verify OSPF status

```

FortiExtender# get router info ospf status
OSPF Routing Process, Router ID: 169.254.254.127
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 0 millisec(s)
Minimum hold time between consecutive SPF's 50 millisec(s)
Maximum hold time between consecutive SPF's 5000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 4h47m24s ago
Last SPF duration 75 usecs
SPF timer is inactive
Refresh timer 10 secsArea ID: 0.0.0.0 (Backbone)
Number of interfaces in this area: Total: 1, Active: 1
Number of fully adjacent neighbors in this area: 1

Area has no authentication
SPF algorithm executed 7 times
Number of LSA 2
Number of router LSA 2. Checksum Sum 0x0000e273
Number of network LSA 0. Checksum Sum 0x00000000 Number of summary LSA 0.
Checksum Sum
0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
Number of opaque link LSA 0. Checksum Sum 0x00000000
Number of opaque area LSA 0. Checksum Sum 0x00000000
This router is an ASBR (injecting external routing information)
Number of external LSA 6. Checksum Sum 0x0001faea

```

```
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
```

Verify OSPF interface

```
FortiExtender# get router info ospf interface
vtil is up
ifindex 14, MTU 1332 bytes, BW 0 Kbit <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
Internet Address 169.254.254.2/30, Area 0.0.0.0
MTU mismatch detection:disabled
Router ID 169.254.254.127, Network Type POINTOPOINT, Cost: 5
Transmit Delay is 1 sec, State Point-To-Point, Priority 1
No designated router on this network
No backup designated router on this network
Multicast group memberships: OSPFAllRouters
Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
Hello due in 3.348s
Neighbor Count is 1, Adjacent neighbor count is 1
```

Verify OSPF neighbor adjacency

```
FortiExtender# get router info ospf neighbor
Neighbor ID Pri State Dead Time Address Interface RXmtL RqstL
DBsmL
10.8.8.1 1 Full/DROther 32.647s 169.254.254.1 vtil:169.254.254.2 0 0 0
```

Verify OSPF database

```
FortiExtender # get router info ospf database
OSPF Router with ID (169.254.254.127)
Router Link States (Area 0.0.0.0)
Link ID ADV Router Age Seq# CkSum Link count
10.8.8.1 10.8.8.1 1061 0x80000155 0x05da 3
169.254.254.127 169.254.254.127 1076 0x8000000c 0xdc99 2
AS External Link States
Link ID ADV Router Age Seq# CkSum Route
0.0.0.0 10.8.8.1 321 0x800000e9 0x9c28 E2 0.0.0.0/0 [0x0]
1.1.1.0 169.254.254.127 226 0x8000000b 0x2a6a E2 1.1.1.0/24 [0x0]
2.2.2.0 10.8.8.1 1591 0x80000087 0x1908 E2 2.2.2.0/24 [0x0]
2.2.2.0 169.254.254.127 156 0x8000000b 0x068b E2 2.2.2.0/24 [0x0]
10.7.7.0 10.8.8.1 1121 0x800000e9 0x7834 E2 10.7.7.0/24 [0x0]
192.168.0.0 169.254.254.127 1206 0x8000000b 0x9c91 E2 192.168.0.0/24 [0x0]
```

Verify OSPF routes

```
FortiExtender# get router info ospf route
===== OSPF network routing table =====
N 169.254.254.0/30 [5] area: 0.0.0.0
directly attached to vtil
N 169.254.254.126/32 [105] area: 0.0.0.0
via 169.254.254.1, vtil
===== OSPF router routing table =====
R 10.8.8.1 [5] area: 0.0.0.0, ASBR
```

```

via 169.254.254.1, vti1
===== OSPF external routing table =====
N E2 0.0.0.0/0 [5/10] tag: 0
via 169.254.254.1, vti1
N E2 2.2.2.0/24 [5/10] tag: 0
via 169.254.254.1, vti1
N E2 10.7.7.0/24 [5/10] tag: 0
via 169.254.254.1, vti1

```

Verify routing table

```

FortiExtender# get router info routing-table all
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
> - selected route, * - FIB route
O>* 0.0.0.0/0 [110/10] via 169.254.254.1, vti1, 04:47:49
S 0.0.0.0/0 [253/0] is directly connected, lte1
S 0.0.0.0/0 [255/0] is directly connected, lte2
S>* 1.1.1.0/24 [1/0] via 10.8.8.1, port1
O 2.2.2.0/24 [110/10] via 169.254.254.1, vti1, 04:47:49
S>* 2.2.2.0/24 [1/0] via 10.8.8.1, port1
S>* 3.3.3.0/24 [1/0] is directly connected, port1
O>* 10.7.7.0/24 [110/10] via 169.254.254.1, vti1, 04:47:49
C>* 10.8.8.0/24 is directly connected, port1
C>* 10.10.10.0/24 is directly connected, wan
C>* 10.38.24.43/32 is directly connected, lte2
C>* 10.224.207.185/32 is directly connected, lte1
C>* 127.0.0.0/8 is directly connected, lo
O 169.254.254.0/30 [110/5] is directly connected, vti1, 05:07:40
C>* 169.254.254.0/30 is directly connected, vti1
O>* 169.254.254.126/32 [110/105] via 169.254.254.1, vti1, 04:47:50
C>* 192.168.0.0/24 is directly connected, port2
C>* 192.168.200.0/24 is directly connected, lan

```

Configure OSPF GUI

Take the following general steps to configure OSPF from the FortiExtender GUI:

1. Go to Router page.
2. Create prefix list.
3. Create route-map.
4. Go to OSPF page:
 - For OSPF settings, enable status and add the router-id.
 - For OSPF Area, create Area "0.0.0.0".
 - For OSPF Network, create the network to add the network prefix.
 - For OSPF Interface, create the interface.
 - For OSPF Redistribute, add created the route-maps for redistributing the connected and static routes to the OSPF domain.

Refer to the illustrations below.

The image displays three screenshots of the FortiExtender web interface, showing the configuration of OSPF (Open Shortest Path First) routing.

Prefix List Screenshot: The 'Prefix List' tab is active. It shows a table with columns: Name, ID, Action, Prefix, GE, and LE. A single entry is visible:

Name	ID	Action	Prefix	GE	LE
local-net	1	permit	192.168.100.0/30	0	0

Route Map Screenshot: The 'Route Map' tab is active. It shows a table with columns: Name, ID, Action, and Match IP Address. A single entry is visible:

Name	ID	Action	Match IP Address
local-net	1	permit	local-net

OSPF Screenshot: The 'OSPF' tab is active. It shows the 'OSPF Settings' section with 'Status' set to 'enable' and 'Router-Id' set to '192.168.200.27'. Below this, there are sections for 'OSPF Areas' and 'OSPF Redistribute'. The 'OSPF Areas' section shows a table with columns: ID, Metric, Metric Type, Route Map, Status, and Action. A single entry is visible:

ID	Metric	Metric Type	Route Map	Status	Action
0.0.0.0	1	2	local-net	enable	enable

The 'OSPF Redistribute' section shows a table with columns: Type, Metric, Metric Type, Route Map, Status, and Action. Two entries are visible:

Type	Metric	Metric Type	Route Map	Status	Action
connected	10	2	local-net	enable	enable
static	10	2	local-net	enable	enable

Complete OSPF configuration code example

```
FortiExtender#config router prefix-list
edit static-routes
config rule
edit 20
set action permit
set prefix 2.2.2.0/24
set ge 0
set le 0
next
edit 10
set action permit
set prefix 1.1.1.0/24
set ge 0
set le 0
```

```
        next
    end
    next
        edit local-nets
            config rule
                edit 10
                    set action permit set prefix 192.168.0.0/24
                    set ge 0
                    set le 0
                next
            end
        next
    end
end

FortiExtender#config router route-map
edit redist-local-connected
    config rule
        edit 10
            set action permit
            set match-ip-address local-nets
        next
        edit 20
            set action deny
            set match-ip-address
        next
    end
next
edit redist-static
    config rule
        edit 20
            set action deny
            set match-ip-address
        next
        edit 10
            set action permit
            set match-ip-address static-routes
        next
    end

FortiExtender#config router ospf
set status enable
set router-id 169.254.254.127
config area
    edit 0.0.0.0
    next
end
config network
    edit 1
        set prefix 169.254.254.0/24
        set area 0.0.0.0 next
    edit 2
        set prefix 169.254.254.127/32
        set area 0.0.0.0
    next
end
config ospf-interface
    edit 1
```

```
        set status enable
        set interface vti1
        set mtu-ignore enable
        set cost 5
    next
end
config redistribute
    config connected
        set status enable
        set metric-type 2
        set metric 10
        set routemap redist-local-connected
    end
    config static
        set status enable
        set metric-type 2
        set metric 10
        set routemap redist-static
    end
end
end
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

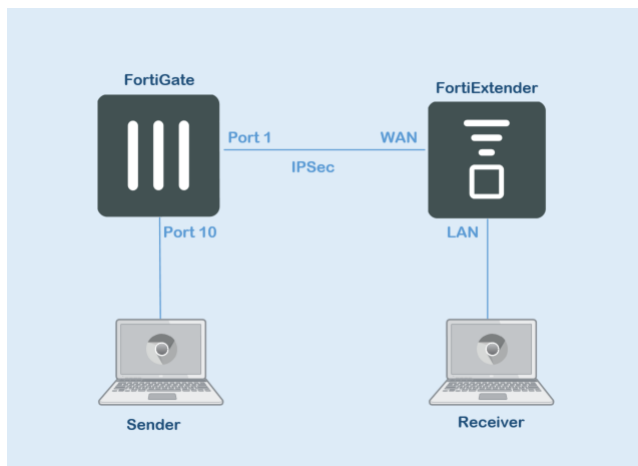
```
move two before one
```

Configure multicast routing

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

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

Multicasting network topology



Target

Target is the network connected to FortiExtender (Standalone). It is usually an up-link network, such as an NSP network provided by a wireless carrier. A target consists of an outgoing interface and a next hop. Targets are

always used in routing systems and SD-WANs to define the destination network to which traffic is sent.

The table below describes the commands for setting a target.

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

Example target configuration:

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

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



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

Firewall

Firewall allows 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 55](#)
- [Configure protocol/port range on page 55](#)
- [Configure firewall policies on page 56](#)
- [Move firewall policies on page 57](#)

Configure address/subnet

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

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

Example address/mask configurations:

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

Configure protocol/port range

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

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

Example protocol/port range configurations:

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

Configure firewall policies

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

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

CLI command	Description
<code>set srcaddr</code>	Specify the source IP address, which can be either a single IP address or a range of IP addresses.
<code>set action {allow deny}</code>	Select either of the following actions: <ul style="list-style-type: none"> <code>allow</code>—Allow access. <code>deny</code>—Deny access.
<code>set status {enable disable}</code>	Set the status of the policy: <ul style="list-style-type: none"> <code>enable</code>—Enable the policy. <code>disable</code>—Disable the policy.
<code>set nat {enable disable}</code>	Select an option for NAT: <ul style="list-style-type: none"> <code>enable</code>—Enable NAT. <code>disable</code>—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 (Standalone) 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 (Standalone) 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 59](#)
- [Check VPN tunnel status on page 65](#)
- [IPsec VPN support for third-party certificates on page 65](#)

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
<code>ike-version</code>	Specify the IKE protocol version, 1 or 2.
<code>keylife</code>	Specify the time (in seconds) to wait before the Phase-1 encryption key expires. The valid range is 20 –172800.
<code>proposal</code>	Specify Phase-1 proposal.
<code>Dhgrp</code>	Select one of the following DH groups: <ul style="list-style-type: none"> • 1 • 2 • 5 • 14
<code>*interface</code>	Use either of the following: <ul style="list-style-type: none"> • wan • eth1/lte1/lte2
<code>type</code>	Select a remote gateway type: <ul style="list-style-type: none"> • static • ddns
<code>*remote-gw</code>	Specify the IPv4 address of the remote gateway's external interface.
<code>*remotegw-ddns</code>	Specify the domain name of the remote gateway, e.g., xyz.DDNS.com.
<code>authmethod</code>	Select an authentication method: <ul style="list-style-type: none"> • psk(pre-shared key) • signature
<code>*psksecret</code>	Specify the pre-shared secret created when configuring the VPN client.
<code>*certificate</code>	<code>set certificate <local-cert-name></code> Specify the name of local signed personal certificates. This entry is only available when <code>authmethod</code> 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.
<code>*peer</code>	<code>set peer <ca-cert-name></code> 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 <code>authmethod</code> 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.
<code>Localid</code>	Specify the local ID.

CLI command	Description
<code>peerid</code>	Accept the peer ID.
<code>Add-gw-route</code>	Enable/disable automatically adding a route to the remote gateway.
<code>Dev-id-notification</code>	Enable/disable the Device ID notification for the first IKE message.

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 (Standalone) 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
<code>phasename</code>	The name of Phase-1 which determines the options required for Phase- 2.
<code>proposal</code>	Phase-2 proposal.
<code>pfs</code>	Select either of the following: <ul style="list-style-type: none"> • <code>enable</code> • <code>disable</code>
<code>Dhgrp</code>	Phase-2 DH group.
<code>keylife-type</code>	Key life type.
<code>keylifeseconds</code>	Phase-2 key life time in seconds. Note: The valid range is 120—172800.
<code>encapsulation</code>	ESP encapsulation mode
<code>protocol</code>	Quick mode protocol selector. Note: The valid range is 1—255. 0 means for all.
<code>src-addr-type</code>	Local proxy ID type. Select one of the following: <ul style="list-style-type: none"> • <code>subnet</code>—IPv4 subnet • <code>range</code>—IPv4 range • <code>ip</code>—IPv4 IP • <code>name</code>—IPv4 network address name
<code>src-subnet</code>	Local proxy ID subnet.

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

Example VPN configuration:

```

FX511FTQ21001262 # config vpn ipsec
FX511FTQ21001262 (ipsec) # show
config vpn ipsec
    config phase1-interface
        edit test511
            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 ltel
            set type static
            set remote-gw 166.253.42.217

```

```
        set authmethod psk
        set psksecret *****
        set localid
        set peerid
        set add-gw-route disable
        set dev-id-notification disable
    next
end
config phase2-interface
    edit test511_p2_1
        set phase1name test511
        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 43200
        set encapsulation tunnel-mode
        set protocol 0
        set src-addr-type name
        set src-name test511_local_subnet_1
        set src-port 0
        set dst-addr-type name
        set dst-name test511_remote_subnet_1
        set dst-port 0
    next
end
end

FX511FTQ21001262 # config network address
FX511FTQ21001262 (address) # show
config network address
    edit test511_local_subnet_1
        set type ipmask
        set subnet 192.168.180.0/24
    next
    edit test511_remote_subnet_1
        set type ipmask
        set subnet 20.0.0.0/8
    next
end
FX511FTQ21001262 # config firewall policy
FX511FTQ21001262 (policy) # show
config firewall policy
    edit vpn_test511_local
        set srcintf any
        set dstintf test511
        set srcaddr test511_local_subnet_1
        set dnat disable
        set dstaddr test511_remote_subnet_1
        set action accept
        set status enable
        set service ALL
        set nat disable
    next
    edit vpn_test511_remote
```

```

        set srcintf test511
        set dstintf any
        set srcaddr test511_remote_subnet_1
        set dnat disable
        set dstaddr test511_local_subnet_1
        set action accept
        set status enable
        set service ALL
        set nat disable
    next
end
FX511FTQ21001262 # config router policy
FX511FTQ21001262 (policy) # show
config router policy
    edit vpn_test511_remote
        set input-device
        set srcaddr test511_local_subnet_1
        set dstaddr test511_remote_subnet_1
        set service ALL
        set target target.test511
        set status enable
        set comment
    next
end

```

Configure firewall policies

You must define two ACCEPT firewall policies 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

```

```
next
end
```



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: Click **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
```

DNS Service

Starting with its 7.2.0 release, FortiExtender can work as a DNS server. You can configure it as a pure DNS proxy server which forwards DNS requests directly to the upstream DNS server, or as a normal DNS server that maintains DNS resource records without forwarding, or a combination of the two, as needed.

When DNS service is enabled on a specific interface, the FortiExtender listens for DNS query requests on that interface. Depending on the configuration, the DNS service on FortiExtender can work in three modes:

- **Recursive** — Is for the shadow DNS database and forward. In this mode, FortiExtender looks up the local shadow DNS database first. If no DNS RR (resource record) is found, the DNS request will be forwarded to the configured system DNS server.
- **Non-recursive** — Is for the public DNS database only. In this mode, FortiExtender only looks up the local public DNS database. If no DNS RR (resource record) is found, it will reply with an error status of NXDOMAIN.
- **Forward-only** — Is for forwarding to the system DNS server only. In this mode, FortiExtender will forward DNS requests directly to the configured system DNS servers.

For more information, see:

- [Enable DNS service on page 67](#)
- [Set up DNS database on page 68](#)

Enable DNS service

To enable DNS service on a specific interface:

```
config system dns-server
    edit <name>
        set interface <interface name>
        set mode [recursive|non-recursive|forward-only]
    next
end
```

Parameter	Description
interface	Required. Specify the interface to enable the DNS service. Only one DNS service can be enabled on an interface.
mode	Required. Select the DNS server mode, which can be one of the following: <ul style="list-style-type: none">• recursive (default)• non-recursive• forward-only

Set up DNS database

To set up the DNS database:

```
config system dns-database
    edit <name>
        set status [enable|disable]
        set domain {string}
        set type [primary]
        set view [shadow|public]
        set primary-name {string}
        set contact {string}
        set ttl {integer}
        set authoritative [enable|disable]
        set forwarder {space-separated list of ipv4-address}
        set source-ip {ipv4-address}
        config dns-entry
            edit <id>
                set status [enable|disable]
                set type [A|NS|CNAME|MX|PTR]
                set ttl {integer}
                set hostname {string}
                set preference {integer}
                set ip {ipv4-address-any}
                set canonical-name {string}
            next
        end
    next
end
```

dns-database

Parameter	Description
status	<p>The status of the DNS zone:</p> <ul style="list-style-type: none"> enable (default) disable <p>Note: This field is NOT required.</p>
domain	<p>Domain name.</p> <p>Note: The maximum length is 225 characters. This field is required.</p>
type	<p>Zone type.</p> <ul style="list-style-type: none"> primary (default) — The primary DNS zone to manage entries directly. <p>Note: This field is NOT required.</p>
view	<p>Zone view.</p> <ul style="list-style-type: none"> shadow: Shadow DNS zone to serve internal clients. (default) public: Public DNS zone to serve public clients. <p>Note: This field is NOT required</p>

Parameter	Description
primary-name	Domain name of the default DNS server for this zone. Note: The maximum length is 225 characters. The default is <code>dns</code> . This field is NOT required
contact	Email address of the zone administrator. You can specify either the username (e.g., admin) or the full email address (e.g., admin@test.com). When using a simple username, the domain of the email will be this zone. Note: The maximum length is 225 characters. The default is <code>host</code> . This field is NOT required
ttl	Default time-to-live value for the entries of this DNS zone. Note: The value ranges from 0 to 2147483647. The default is 86400. This field is NOT required.
authoritative	(Status of) authoritative zone: <ul style="list-style-type: none"> • enable (default) • disable Note: This field is NOT required.
forwarder	DNS zone forwarder IP address list. Note: List of IPv4 address only. The maximum number of IP addresses is 12. This field is Not required.
source-ip	Source IP for forwarding to the DNS server. Note: IPv4 address only. The default is 0.0.0.0.

dns-entry

Parameter	Description
status	Resource record status: <ul style="list-style-type: none"> • enable (default) • disable Note: This field is NOT required.
type	Resource record type: <ul style="list-style-type: none"> • A — Host type. (default) • NS — Name server type • CNAME — Canonical name type • MX — Mail exchange type • PTR — Pointer type Note: This field is NOT required.
ttl	Time-to-live for this entry. Note: The value ranges from 0 to 2147483647. The default is 0. The field is NOT required.
hostname	Hostname of the host.

Parameter	Description
	Note: The maximum length is 155 characters. The field is required.
preference	DNS entry preference, 0 is the highest preference. Note: Applicable to MX (type) only. The value ranges from 0 to 65535. The default is 10. This field is NOT required.
ip	IPv4 address of the host. Note: Applicable to A and PTR(types) only. This field is required.
canonical-name	Canonical name of the host. Note: Applicable to CNAME (type) only. The maximum length is 255 characters. This field is required.

Check DNS statistics

```
FX201E5919000046 # get dnsproxy stats
retry_interval=500 query_timeout=1995
DNS latency info:
    server=208.91.112.53 latency=6 updated=3249
DNS_CACHE: alloc=2, hit=0
DNS query: alloc=0
DNS UDP: req=2 res=2 fwd=2 retrans=0 to=0
    cur=2 switched=1720994010 num_switched=0
DNS TCP: requests=0 responses=0 fwd=0 retransmit=0 timeout=0
```

Dump the DNS cache

```
FX201E5919000046 # execute dnsproxy cache dump
name=gmail.google.com, ttl=300:298:1798
    142.250.189.238 (ttl=300)
name=www.google.com, ttl=300:283:1783
    142.250.189.196 (ttl=300)
CACHE num=2
```

Clear the DNS cache

```
FX201E5919000046 # execute dnsproxy cache clear
FX201E5919000046 # execute dnsproxy cache dump
CACHE num=0#
```

Dump the DNS database

```
FX201E5919000046 # execute dnsproxy database dump
name=test1 domain=example.com ttl=86400 authoritative=0 view=shadow type=primary
serial=1714636915
    A: host1.example.com-->192.168.200.100(86400)
    SOA: example.com (primary: dns.example.com, contact: host@example.com, serial:
```

```

1714636915) (86400)
PTR: 100.200.168.192.in-addr.arpa-->host1.example.com(86400)
MX: example.com-->mail1.example.com 10 (86400)
NS: example.com-->dns.example.com(86400)
CNAME: cn1.example.com-->host1.example.com(86400)

```

Force DNS request to go through DNSPROXY

In 7.2.2, FortiExtender has replaced the `system/dns/search-order` option and the default `dns (8.8.8.8)`, and uses two algorithms to decide the dns-server selection order:

- `least-rtt` — In the dns-server selection pool, the round-trip time of each dns-server IP is now calculated and sorted from the shortest to the longest. FortiExtender picks from the shortest one.
- `failover` — This algorithm is a relatively fixed order. The first pick does not change until it fails the first time. The order is primary dns > secondary dns > dynamic dns (learned from DHCP).

In addition, you now can configure system DNS parameters on the FortiExtender that include the following:

- primary dns server
- secondary dns server
- timeout
- retry attempts
- maximum dns cache limit
- dns cache ttl
- cache not found response option,
- source ip, and
- server select method

```

### get system dns
"redesign this command to show all the DNS configuration info"
e.g.
# get system dns
primary                : 208.91.112.53
secondary              : 208.91.112.52
timeout                : 5
retry                  : 3
dns-cache-limit        : 5000
dns-cache-ttl          : 1800
cache-notfound-responses: disable
source-ip              : 0.0.0.0
server-select-method   : least-rtt
acquired servers       :
wan: 172.30.1.105

```

```

###config system dns
config system dns
    set primary 208.91.112.53
    set secondary 208.91.112.52
    set timeout 5
    set retry 3

```

```

set dns-cache-limit 5000
set dns-cache-ttl 1800
set cache-notfound-responses disable
set source-ip 0.0.0.0
set server-select-method least-rtt
end

```

Field	Description	Mandatory	Type	Value	Default value
primary	Specify the primary static DNS server IP.	Yes	string	IPV4	208.91.112.53
secondary	Specify the secondary static DNS server IP.	Yes	string	IPV4	208.91.112.52
timeout	Specify the timeout in seconds.	Yes	number	0-10	5
retry	Specify the number of retry attempts allowed for unsuccessful connections.	Yes	number	0-5	3
dns-cache-limit	Specify the maximum amount of cache that can be stored.	Yes	number	0-4294967295	5000
dns-cache-ttl	Specify the TTL of cached DNS value in seconds.	Yes	number	60-86400	1800
cache not-found response	Specify whether or not to save the not-found response into cache. If enabled, no need to forward the not-found response to the DNS server in the future.	Yes	option	disable/enable	disable
source-ip	Specify the IP address used by the DNS server as its source IP.	Yes	string	IPV4	0.0.0.0
server-select-method	Specify how configured servers are prioritized. <ul style="list-style-type: none"> least-rtt —In the dns-server selection pool, the round-trip time of each dns-server ip is —calculated and sorted from the shortest to the longest, picking 	Yes	option	least-rtt / failover	least-rtt

Field	Description	Mandatory	Type	Value	Default value
	<p>from the shortest one.</p> <ul style="list-style-type: none">• failover — This algorithm is a relatively fixed order. The first pick doesn't change until it fails the first time. The order is primary dns -> secondary dns > dynamic dns (learned from DHCP).				

SD-WAN

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 the 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 interfaces 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 an SD-WAN member for data transmission based on:
 - Priority
 - Cost
- Two LTE interfaces as members of a redundant SD-WAN by cost algorithm:
 - The lowest cost target works as the primary. When the primary fails, the next lowest cost target will take over the primary role (fail-over).
 - When the 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 the lowest cost target and works as the primary.

This section covers the following topics:

- [Configure an SD-WAN on page 74](#)
- [Check SD-WAN health on page 75](#)
- [Define an SD-WAN member on page 76](#)

Configure an SD-WAN

Use the following commands to configure an SD-WAN.

CLI command	Description
<code>config system interface</code>	Enters system interface configuration mode.
<code>edit <vwan_name></code>	Specify the name of the SD-WAN interface.
<code>set type virtual-wan</code>	Set the interface type to virtual-wan.
<code>set status <status></code>	Set the status of the interface: <ul style="list-style-type: none"> • <code>up</code>—Enable the interface. • <code>down</code>—Disable the interface.
<code>set FEC {source </code>	Select a LLB metric to denote how to distribute traffic:

CLI command	Description
<code>dest ip-pair connection}</code>	<ul style="list-style-type: none"> <code>source</code>—Traffic from the same source IP is forwarded to the same target. <code>dest</code>—Traffic to the same destination IP is forwarded to the same target. <code>ip-pair</code>—Traffic from the same source IP and to the same destination IP is forwarded to the same target. <code>connection</code>—Traffic with the same 5 tuples (i.e., a source IP address/port number, destination IP address/port number and the protocol) is forwarded to the same target
<code>set algorithm {redundant WRR}</code>	Select the LLB algorithm: <ul style="list-style-type: none"> <code>redundant</code>—Targets work in primary-secondary mode. <code>WRR</code>—Targets work in Weighted Round Robin mode.
<code>Set grace-period</code>	Specify the grace period in seconds to delay fail-back.
<code>set session-timeout 60</code>	Specify the session timeout threshold in seconds. The default is 60. This is used to time out a VWAN session. A LLB session is created for each traffic stream. However, when a session times out, it is deleted.
<code>set members</code>	Add VWAN members to the VWAN interface.

FortiExtender (Standalone) 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

An `hmon.hchk` object is required 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.

Example SD-WAN health check configuration:

The following commands are used to define a `vwan_health_check` and use it to perform health check for the VWAN member, `vwchk1`.

```
config hmon hchk
  edit vwchk1
    set protocol ping
    set interval 5
    set probe-cnt 1
    set probe-tm 2
    set probe-target 8.8.8.8
    set interface fcs-0-phase-1
    set src-type interface
    set src-iface nas1
    set filter rtt loss
  next
  edit vwchk2
    set protocol ping
    set interval 5
    set probe-cnt 1
    set probe-tm 2
    set probe-target 8.8.8.8
    set interface fcs-1-phase-1
    set src-type interface
    set src-iface nas1
    set filter rtt loss
  next
end
```

You can use the “`get hmon hchk vwan.<vwan_member_name>`” command to show the latest statistics that 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

```
FFX04DA5918000098 # get hmon hchk vwchk1
  median rtt:      avg      max      min      now      sd      am/s
fcs-0-phase-1: 182.23ms 182.47ms 182.00ms 182.00ms 0.24ms 775.3
  packet loss:      avg      max      min      now
fcs-0-phase-1:      0%      0%      0%      0%
```

Define an SD-WAN member

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

Use the following commands to define a link member.

CLI command	Description
<code>set target</code>	Specify the target to which traffic is forwarded.
<code>set priority</code>	Specify the priority of the link member. The valid value range is 1—7.
<code>set weight</code>	Specify the weight of the member.
<code>set health-check</code>	Specify the link health check of the VWAN.
<code>set health-check-fail-threshold</code>	Specify the number of consecutive failed probes before the member is considered dead. Notes: The valid value range is 1—10; the default is 5.
<code>set health-check-success-threshold</code>	Specify the number of consecutive successful probes before the member is considered alive. Note: The valid value range is 1—10; the default is 5.

Example SD-WAN members 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
    set health-check-fail-threshold 5
    set health-check-success-threshold 5
  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 vwchk2
    set health-check-fail-threshold 5
    set health-check-success-threshold 5
  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 78](#)
- [Perform link health check on page 79](#)
- [Configure health monitoring on page 81](#)

Monitor interface status

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

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

Example interface monitoring configuration:

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

```

        set interface ltel
        set filter rx_bytes tx_bytes
    next
end

```

You can monitor the aforementioned configuration using the following commands:

```

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

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

```

Perform link health check

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

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

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

Parameter	Descriptions
protocol {ping http dns}	The protocol used for status check.
interval	The monitoring interval in seconds. The valid value 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.
probe-tm	The timeout for a probe in seconds. The valid value range is 1—10; the default is 2.
*probe-target	The target to which a probe is sent.
port	The port number used to communicate with the server. The valid value range is 165535; the default is 80.
http-get	The URL used to communicate with the server. The default is /.

Parameter	Descriptions
*interface	The outbound interface of probe packets.
src-type {none interface ip}	Specify the way to set the source address for probes.
src-iface	Set the source address as the address derived from the specified interface.
src-ip	Set the source address as a specific IP.
filter {rtt loss}	Specify the desired filter.

Example health monitor health check configurations:

```

config hmon hchk
    edit fcs-0-phase-1-chk
        set protocol ping
        set interval 5
        set probe-cnt 1
        set probe-tm 2
        set probe-target 34.207.95.79
        set interface fcs-0-phase-1
        set src-type interface
        set src-iface lan
        set filter rtt loss
    next
    edit fcs-1-phase-1-chk
        set protocol ping
        set interval 5
        set probe-cnt 1
        set probe-tm 2
        set probe-target 34.207.95.79
        set interface fcs-1-phase-1
        set src-type interface
        set src-iface lan
        set filter rtt loss
    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 interval default:1>
        set probe-tm <probe timeout, default:2>
        set probe-target <target to be probed>
        set interface <uplink interfaces on which probe has to be sent>
        set src-iface <interface whose source IP is to be used>
        set filter <rtt |loss>
    next
end
```

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

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

To display health check statistics:

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

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

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

To run health check instance on a specific interface:

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

System management

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

- [Get system version on page 85](#)
- [Upgrade OS firmware on page 86](#)
- [Upgrade modem firmware on page 87](#)
- [SMS notification on page 88](#)
- [Remote diagnostics via SMS on page 88](#)
- [Export system logs to remote syslog servers on page 89](#)
- [Support for SNMP \(read-only\) and traps on page 90](#)

API handling of error messages

FortiExtender now displays more informative messages about the success or failure of any CRUD operation, including any or all references to the messages.

The API payload either has the "details" property or comes without it at all. If there is the "details" property in the API payload, FortiExtender shows the "details" property or the "message" property; if there is any reference to the "message"/"details", it uses the "path" property. This applies to the entire FortiExtender product line.

Sample payload

Success:

```
{
  "payload": {}/[],
  "error": {
    "code": "Success",
    "message": "The request has succeeded.",
    "path": "<The resource location that produced the error>"
  }
}
```

Error 1 without details:

```
{
  "error": {
    "code": "MethodNotAllowed",
    "message": "The method is not allowed for the requested resource.",
    "path": "<The resource location that produced the error>"
  }
}
```

Error 2 without details:

```
{
  "error": {
    "code": "InvalidConfig",
    "message": "The configuration is invalid.",
    "details": "<details messages without path>",
    "path": "<The resource location that produced the error>"
  }
}
```

```
}
}
```

Add trusted hosts

FortiExtender OS enables you to add trusted hosts so that administrators of the hosts can connect to it (the FortiExtender device) via the IP/network. You can specify any IPv4 address or subnet address and netmask from which an administrator can connect to the FortiExtender.

Each administrator can create up to 10 trusted hosts, which can access the device from any IPv4 address by default.

To add trusted hosts:

```
FX201E5919000054 # config system admin
FX201E5919000054 (admin) # edit admin
FX201E5919000054 (admin) # show
edit admin
  set accprofile super_admin
  set password ENC $5$Ht4I..iMtoqzQdJn$tA/wEHn8yAs8Ap19pcBrYE6O92jEI9OnDSY6Y/ujJ9B
  set trusthost1 192.168.1.115
  set trusthost2
  set trusthost3 192.168.2.0/24
  set trusthost4
  set trusthost5
  set trusthost6
  set trusthost7
  set trusthost8
  set trusthost9
  set trusthost10
next
```

Parameter	Description
edit <usernaem>	Specify the admin username.
set accprofile	Specify the access profile name.
set password	Specify the admin user password.
set trusthost1	Specify the IPv4 address or subnet address/netmask of the host from which the administrator connects to the device.
set trusthost2	See "trusthost1" above.
set trusthost3	See "trusthost1" above.
set trusthost4	See "trusthost1" above.
set trusthost5	See "trusthost1" above.
set trusthost6	See "trusthost1" above.
set trusthost7	See "trusthost1" above.

Parameter	Description
set trusthost8	See "trusthost1" above.
set trusthost9	See "trusthost1" above.
set trusthost10	See "trusthost1" above.

Activate the default admin account

This feature enables you to activate (i.e., make visible) the admin user account created and hidden in previous versions of your FortiExtender so that you can edit or remove it if needed.

To activate the hidden default admin account:

```
FX201E5919000054 # config system admin
FX201E5919000054 (admin) # show
config system admin
  edit admin
    set accprofile super_admin
    set password ENC
      $5$Ht4I..iMtoqzQdJn$tA/wEHn8yAs8Ap19pcBrYE6O92jEI9OnDSY6Y/ujJ9B
    set trusthost1
    set trusthost2
    set trusthost3
    set trusthost4
    set trusthost5
    set trusthost6
    set trusthost7
    set trusthost8
    set trusthost9
    set trusthost10
  next
end
FX201E5919000054 (admin) #
```

Multiple static access controller addresses or FQDN

FortiExtender enables you to specify multiple access controllers while "ac-discovery-type" is static, or specify FQDN (static-ac-ip-addr has been changed to static-ac-addr).

To configure multiple static access controller or FQDN:

```
config system management fortigate
  set ac-discovery-type static
  config static-ac-addr <=== New table which replaced previous static-ac-ip-addr
    edit 1
      set server 192.168.1.99
    next
  next
end
```

```

edit 2
    set server fortisase.fortiextender.com
next
...
end
set ac-ctl-port 5246
set ac-data-port 25246
set discovery-intf wan lan port1 port2 port3 port4
set ingress-intf
end

```

The "static-ac-ip-addr" in pre-7.0.2 releases has now been replaced by "static-ac-addr" which is a table that allows you to configure up to 16 entries. For each entry, you can specify the server as in FQDN string or IPv4-address string format.



If you have static-ac-ip-addr specified in a pre-7.0.2 version of FortiExtender OS, an entry "1" will be automatically generated and its value of "server" will be the string configured in "static-ac-ip-addr" of old version, after you have upgraded to 7.0.2.

Get system version

Use the following command to find out your system version:

```

FX201E5920012136 # get system version
System version:
Image version : FXT201E-v7.0.3-build056
Image type : GA
Model : FortiExtender-201E
MAC : e0:23:ff:0a:38:ad
Serial-Number : FX201E5920012136
License : e30d247b0ca07b5e
OEM SN : FX201E5920012136
BIOS version : 00020005
System Part-Number : P23421-02
ROM REV : FX201E
Fallback image : FXT201E-v7.0.2-build045
Fallback image type : GA

```

Get user session status and force log-out

FortiExtender enables you to get the session status of users currently logged in the system and to log them out if necessary.

To get the session status of current users:

```

FX201E5919000054 # get system admin status
admin accprofile: super_admin
    session: Console start time: 2021-10-27 20:50:36

```

```
session: GUI start time: 2021-10-28 10:13:35 remote: 192.168.1.115

test1 accprofile: super_admin
    session: GUI start time: 2021-10-28 11:33:20 remote: 192.168.1.120
    session: Telnet start time: 2021-10-28 13:42:15 remote: 192.168.1.115
```

To force-log out users:

```
FX201E5919000054 # execute disconnect-admin-session
all All sessions
console Console session
telnet Telnet session
ssh SSH session
gui GUI session
gui-console GUI Console session

FX201E5919000054 # execute disconnect-admin-session all
Usage: disconnect-admin-session <session-type> <logged-in-admin>

FX201E5919000054 # execute disconnect-admin-session all test1
```

Upgrade OS firmware

You can upgrade FortiExtender (Standalone) OS firmware from FortiGate or FortiExtender (Standalone) 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 (Standalone).

FortiExtender Cloud

Even when FortiExtender is managed locally in standalone mode, you can upgrade its OS image by pulling the latest version from the Cloud.

1. Enter this command:

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

The available OS images show on FortiExtender (Standalone) Cloud.

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

GUI

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

Upgrade modem firmware

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

TFTP

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

FTP

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

USB

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

FortiExtender Cloud

Even when FortiExtender is managed locally in standalone mode, you can upgrade its firmware image by pulling the latest version from the Cloud.

1. Enter this command:

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

The available modem images show on FortiExtender (Standalone) Cloud.

2. Select the appropriate option in the CLI.
FortiExtender (Standalone) 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.

Configure syslog database array

FortiExtender supports configuration of multiple syslog servers. The server array adds syslog database instead of plain text files.

```
FX511F5921000020 # config system syslog
FX511F5921000020 (syslog) # show
config system syslog
    config remote-servers
        edit 1
            set ip 192.168.2.99
            set port 514
        next
        edit 2
            set ip 192.168.2.168
            set port 514
        next
    end
    config statistic-report
        set status disable
        set interval 30
```

```
        config cpu-usage
            set threshold 70
            set variance 5
        end
        config memory-usage
            set threshold 50
            set variance 5
        end
        config cpu-temperature
            set threshold 80
            set variance 5
        end
    end
end
```

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

```
FX511FTQ21001262 # execute snmpmibs export tftp
FORTINET-CORE-MIB.mib          download FORTINET-CORE-MIB.mib
FORTINET-FORTIEXTENDER-MIB.mib download FORTINET-FORTIEXTENDER-MIB.mib
```

Get MIB2 interface statistics via SNMP

FortiExtender supports MIB2 interface, which enables you to get interface statistics directly from the device via SNMP.

It supports the OID range from 1.3.6.1.2.1.2.2.1.1 to 1.3.6.1.2.1.2.2.1.22. Below are some examples:

```
OID: .1.3.6.1.2.1.2.2.1.16.3
Value: 29002
Type: Integer
```

```
OID: .1.3.6.1.2.1.2.2.1.16.4
Value: 10614
Type: Integer
```

```
OID: .1.3.6.1.2.1.2.2.1.16.5
Value: 0
Type: Integer
```

```
OID: .1.3.6.1.2.1.2.2.1.16.6
Value: 2794
Type: Integer
```

Access other devices via SSH

You can log into other devices from FortiExtender via SSH using the following command:

```
#execute ssh username serverip
```

For example, "execute ssh admin 192.168.1.115" lets the user "admin" to log into the device with the IP address "192.168.1.115" via SSH.

Dual modems

Dual modem means that a FortiExtender unit comes with two LTE interfaces for internet connectivity. These two LTE interfaces can be used for link load balancing.

- [Dual-modem in IP pass-through mode on page 105](#)
- [Dual modems in NAT mode on page 106](#)

Dual modems in NAT mode

In NAT mode, FortiExtender functions as a gateway with two LTE interfaces. You can use either a virtual WAN interface or a policy-based route to do link-load balancing.

For more information, refer to [Interface configuration guideline on page 23](#) for Virtual-WAN interface and [System routing on page 39](#) for policy-based route configurations.

Troubleshooting, diagnostics, and debugging

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

- [Troubleshooting on page 95](#)
- [Status, diagnostics, and debugging commands on page 96](#)
- [Diagnose FortiExtender](#)

Troubleshooting

Below are some common error situations with their suggested solutions.

Can't manage the FortiExtender (Standalone) from FortiExtender (Standalone) Cloud

Upgrade the FortiExtender (Standalone) to OS version 3.3.0 or higher.

Can't start an Internet session

```
execute show-hidden
FXA11FTQ21000008 # execute modemfw AtTest modem1
open tty /dev/ttyUSB3
Then enter in the correct troubleshooting AT command such as
at+cgdcont?

FXA11FTQ21000008 # execute modemfw AtTest modem1
open tty /dev/ttyUSB3
at+cgdcont?
at+cgdcont?

+CGDCONT: 1,"IPV4V6","ims","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0
+CGDCONT: 2,"IPV4V6","vzwadmin","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0
+CGDCONT: 3,"IPV4V6","VZWINTERNET","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0
+CGDCONT: 4,"IPV4V6","vzwapp","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0
+CGDCONT: 5,"IPV4V6","vzw800","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,0
+CGDCONT: 6,"IPV4V6","vzwemergency","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,1

OK
\
```

Status, diagnostics, and debugging commands

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

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

Diagnose from Telnet

1. From the Windows Command prompt, type `cmd`.
2. Type `telnet [modem ip address]`. (The default IP address is 192.168.200.99/24.)
3. Enter your user name and password as required.
4. Enter the command you want.



Collect complete diagnostics information

FortiExtender (Standalone) 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>
```

Appendix A: Configure LTE settings

- [Add a new carrier profile on page 98](#)
- [Add a new operator/carrier on page 98](#)
- [Activate a SIM card on page 100](#)
- [Configure start session timeout on page 101](#)
- [Check the recorded SIM card IMSI number on page 102](#)
- [Delete the recorded SIM card IMSI number on page 102](#)
- [Set the default SIM on page 102](#)
- [Enable SIM-switch on page 103](#)
- [Dual modems on page 105](#)
- [Unlock SIM pin on page 104](#)

Add a new carrier profile

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

```
FX511FTQ21001262 # config lte carrier
FX511FTQ21001262 (carrier) # show
```

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:

```
FX511FTQ21001262 # get lte carrier
Usage: get lte carrier mcc-number mnc-number
```

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

```
FX511FTQ21001262 # config lte simmap
FX511FTQ21001262 (simmap) # show
config lte simmap
end
```

```

FX511FTQ21001262 (simmap) # edit 1
FX511FTQ21001262 (1) <M> # show
edit 1
    set mcc
    set mnc
    set carrier
next

```



The new operator/carrier requires at least one matched carrier profile entry from “get extender lte-carrier-list <FEX SN>” to take effect.

Create a data plan

You can configure a data plan on the FortiGate with the following parameters:

```

config extender-controller dataplan
    edit Verizon
        set modem modem1
        set type by-carrier
        set carrier Verizon
        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
end

```



When “private network” is enabled, FortiExtender allows the flow of non-NATed IP traffic on to an LTE interface. Otherwise, it does not.

Parameter	Description
modem	Choose “modem1”, “modem2”, or “all”.
type	Choose the way for the modem to select the SIM card: <ul style="list-style-type: none"> carrier— Assign by SIM carrier. slot— Assign to SIM slot 1 or 2. iccid— Assign to a specific SIM by its serial number (18 to 22 digits).

Parameter	Description
	<ul style="list-style-type: none"> <code>generic</code>— Compatible with any SIM. Assigned if no other data plan matches the chosen SIM.
<code>iccid</code>	The serial number of the SIM, mandatory for <code>"set type by-iccid"</code> .
<code>carrier</code>	The SIM card carrier, mandatory for <code>"set type by-carrier"</code> .
<code>slot</code>	The SIM card slot, mandatory for <code>"set type by-slot"</code> .
<code>apn</code>	The APN of the SIM card.
<code>auth-type</code>	The Authorization mode.
<code>username</code>	The username.
<code>password</code>	The password.
<code>pdn</code>	The Packet Data Network (PDN) IP address family.
<code>signal-threshold</code>	<p>The signal-strength threshold beyond which SIM switch will occur.</p> <p>Note: Enter an integer value from <50> to <100> (default = <100>).</p>
<code>signal-period</code>	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.
<code>capacity</code>	The data capacity per month (from 0 to 102400000 MB).
<code>monthly-fee</code>	The monthly fee for the data plan (from 0 to 1000000).
<code>billing-date</code>	The billing date of the month.
<code>preferred-subnet</code>	DHCP subnet.
<code>private-network</code>	(Enable/disable) blocking all non-NATed traffic.

Activate a SIM card



A new SIM card must be activated to connect to the ISP network. Activating a SIM card generally takes about 10 seconds to complete, but it might take minutes or longer in some rare cases.

The `"set sim-activation-delay 300"` command comes into play when a new SIM card fails to be activated within 10 seconds. It has a default value of 300 seconds to activate a SIM, and the configurable range is from 5 seconds to 600 seconds.

To activate a SIM card:

```
FX201E5919000035 # config lte setting
FX201E5919000035 (setting) # show
config lte setting
config controller-report
```

```
        set status disable
    end
    config modem1
        set cert-mode disable
        set default-sim sim1
        set session-down-detection 3
        set gps enable
        set sim1-pin disable
        set sim2-pin disable
        config auto-switch
            set by-disconnect disable
            set by-signal disable
            set by-data-plan disable
            set switch-back
        end
    end
    set advanced enable <==new, default is disable
    config advanced-settings <==new, display only when "set advanced enable"
        set sim-activation-delay 300 <==(5 - 600 sec, default = 300 sec)
    end
end
```

Configure start session timeout



Generally, the "set session-dial-timeout 0" command has a default value of 0, meaning "disabled".

In some case, it may take time for the modem to establish a session, so you may need to set it to a larger value to ensure that the modem has enough time to connect.

To set up a timeout for start session:

```
FX201E5919000035 (plan) # edit 1
FX201E5919000035 (1) <M> # show
edit 1
    set modem all
    set type by-default
    set apn
    set auth NONE
    set user
    set pwd
    set pdn ipv4-only
    set signal-threshold -100
    set signal-period 3600
    set capacity 0
    set monthly-fee 0
    set billing-date 1
    set overage disable
    set preferred-subnet 0
    set private-network disable
    set session-dial-timeout 0 <=== new, default is 0, means no special wait,
keep the previous design. range": "0-180"
```

```
next

FX511F5919000000 # execute modem delete-sim-record modem1
all delete all the IMSI for modem1
imsi delete one IMSI for modem1
```

Check the recorded SIM card IMSI number

When a SIM card is activated, FortiExtender records the IMSI number of the card. You can use the following command to check the records.

To check the recorded SIM card IMSI number:

```
FX201E5919000035 # get lte sim-imsi-record
Modem1:
***No-record!***
End
FX201E5919000035 #

FX201E5919000035 # get lte sim-imsi-record
Modem1:
Index IMSI
1: 310260888228819
End
```

Delete the recorded SIM card IMSI number

FortiExtender records the IMSI number of a SIM card when the card is activated. The following command enables you to remove the IMSI number from the record.

To delete the recorded SIM card IMSI number:

```
FX511F5919000000 # execute modem delete-sim-record
modem1 Print latest modem log
modem2 Print previous modem log
```

Set the default SIM

When installing two SIM cards in one modem, you can set the default SIM to use.

You can set the default SIM by

- [Set the default SIM by preferred carrier on page 103](#)
- [Set the default SIM by low cost on page 103](#)
- [Set the default SIM by SIM slot on page 103](#)

Set the default SIM by preferred carrier

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

```
FX511FTQ21001262 # config lte setting modem1
FX511FTQ21001262 (modem1) # set default-sim
sim1
sim2
by-carrier
by-cost

FX511FTQ21001262 (modem1) # set default-sim by-carrier
FX511FTQ21001262 (modem1) <M> # set preferred-carrier
```

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”.

```
FX511FTQ21001262 # config lte setting modem1
FX511FTQ21001262 (modem1) # set default-sim
sim1
sim2
by-carrier
by-cost

FX511FTQ21001262 (modem1) # set default-sim by-cost
```

Set the default SIM by SIM slot

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

```
FX511FTQ21001262 # config lte setting modem1
FX511FTQ21001262 (modem1) # set default-sim
sim1
sim2
by-carrier
by-cost

FX511FTQ21001262 (modem1) # set default-sim sim1/sim2
```

Enable SIM-switch

```
config lte setting modem1
  config auto-switch
    set by-disconnect enable
    set by-signal enable
    set by-data-plan enable
    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

```



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 when the active card gets disconnected according to the 'disconnect-threshold' and 'disconnect-period'.
by-signal	The SIM card switches when the signal strength gets weaker than the signal-threshold.
by-data-plan	The SIM card switches when 'capacity' is overrun and 'overage' is enabled.
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 (3600-2147483647) in seconds.

Unlock SIM pin

A SIM card is automatically locked following three incorrect pin uses. You can unlock a locked SIM card with PUK code using AT commands.



This feature applies to FEX-511F only.

To unlock a SIM card with PUK code:

1. Pause the modem manager to prevent SIM switching:

```

config lte setting
config modem1
    set pause-modem-manager enable
end

```

2. Run the following command with the appropriate PUK code and new SIM pin.

```
execute modem modem1 sim1 puk unlock 12345678 1111
```

Note: In the sample code above, the PUK is 12345678 and the new SIM pin is 1111.

3. Disable pause-modem-manager in Step 1 above.

```
set pause-modem-manager disable
```

4. Configure the newly configured SIM pin, i.e., 1111 in the example above, to activate the session.

Dual modems

Dual modem means that a FortiExtender unit comes with two LTE interfaces for internet connectivity. These two LTE interfaces can be used for link load balancing.

- [Dual-modem in IP pass-through mode on page 105](#)
- [Dual modems in NAT mode on page 106](#)

Dual-modem in IP pass-through mode

Dual modems mean that a FortiExtender unit comes with two LTE interfaces for internet connectivity. These two LTE interfaces can be used for link load balancing. FortiExtender works in local IP pass-through mode, as an extended modem of any router. In this mode, FortiExtender must be connected directly to the WAN port of the router and the router WAN port must be in DHCP mode.

Enable local IP pass-through mode

To enable local IP pass-through mode:

```
FX212E5919000009 # config system management local
FX212E5919000009 (local) # set mode ip-passthrough
FX212E5919000009 (local) # end
FX212E5919000009 # config system management
FX212E5919000009 # set discovery-type local
FX212E5919000009 # end
```

Configure a virtual Wire Pair

A virtual wire pair configuration is necessary to enable the IP Pass-through forwarding between two ports.

To configure a virtual pair:

```
FX212E5919000009 # config system virtual-wire-pair
FX212E5919000009 (virtual-wire-pair) # set ltel-mapping lan
FX212E5919000009 (virtual-wire-pair) # end
```

Dual modems in NAT mode

In NAT mode, FortiExtender functions as a gateway with two LTE interfaces. You can use either a virtual WAN interface or a policy-based route to do link-load balancing.

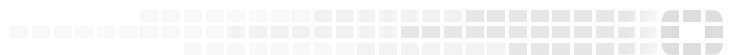
For more information, refer to [Interface configuration guideline on page 23](#) for Virtual-WAN interface and [System routing on page 39](#) for policy-based route configurations.

Change Log

Date	Change Description
July 14, 2023	Initial release.



FORTINET®



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.