



Admin Guide

FortiExtender (Standalone) 7.6.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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 LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



Jun 10, 2026

FortiExtender (Standalone) 7.6.3 Admin Guide

TABLE OF CONTENTS

Change Log	7
Introduction	8
Getting started	9
Management and Operation mode	10
Check current management mode	11
IP pass-through mode	12
NAT mode	13
Essential LTE settings	13
Activate SIM card	14
Configure PIN	14
Create a Data Plan	15
Essential networking configurations	15
LAN interface	16
LAN addressing	16
DHCP server	17
Health checks	18
VWAN interface	19
Essential wireless configurations	21
Country Code	21
Wireless WAN networks	22
Virtual Access Points and SSID	23
Radio profiles	24
IPsec VPN tunnels	25
Main LTE/5G features	28
Cellular capabilities	28
Supported wireless carriers	29
SIM mapping	30
Add a data plan and APN	30
Global SIM with roaming on	31
SIM-switch	31
SIM switch-back	32
Configure SIM-switch based on link health	33
Get modem status	34
Stopping data traffic on overaged LTE interface	35
OBM management	35
Multiple Packet Data Network (PDN)	36
Interface management	37
Interface configuration guideline	38
Physical interface(s)	38
LTE interface	38
Tunnel interface	38
Virtual-WAN interface	38
Access allowance	40

Get interface status	40
Configure LAN switch	41
Configure switch interface	42
Configure VXLAN interface	43
SFP DSL support	44
Aggregate interface support with load-balancing	44
Configure a private network	46
Configure Virtual-WAN interface	47
Configure WiFi VAPs as members of switch interface	50
Dynamic Frequency Selection channels	51
Configure allowaccess for tunnel interface	53
DHCP configurations	54
Configure DHCP server	54
Configure DHCP relay	56
DHCP relay over VPN	57
DHCP client optimization	57
Network utilities	58
Address	58
Service	58
Target	58
System routing	60
Configure static routing	60
Configure PBR routing	61
View routing configurations	62
Move PBR rules	63
Configure dynamic routing — OSPF	63
Configure OSPF from Console (CLI)	64
Configure OSPF redistribution	67
Verify OSPF configurations	69
Configure OSPF GUI	70
Complete OSPF configuration code example	71
Configure multicast routing	73
Firewall	74
Configure address/subnet	74
Configure protocol/port range	75
Configure firewall policies	75
Destination Network Address Translation (DNAT)	76
Move firewall policies	77
VPN	78
Configure VPN	78
Configure phase-1 parameters	79
Configure phase-2 parameters	80
Configure firewall policies	83
Check VPN tunnel status	84

IPsec VPN support for third-party certificates	84
Use third-party certificates for IKE authentication	85
IPsec VPN supports more DH groups	86
DNS Service	87
Enable DNS service	87
Set up DNS database	88
Check DNS statistics	90
Dump the DNS cache	90
Clear the DNS cache	90
Dump the DNS database	91
Force DNS request to go through DNSPROXY	91
SD-WAN	94
Configure an SD-WAN	94
Check SD-WAN health	95
Define an SD-WAN member	97
Wi-Fi Settings	99
Set your geographical location	99
Configure FortiExtender as a Wi-Fi AP	100
Configure FortiExtender as a Wi-Fi station	108
Authentication and security	113
RADIUS authentication	113
Wired 802.1X authentication	118
Health monitoring	125
Monitor interface status	125
Perform link health check	126
Configure health monitoring	128
System management	130
API handling of error messages	130
Add trusted hosts	131
Activate the default admin account	132
Multiple static access controller addresses or FQDN	133
Get system version	133
Get user session status and force log-out	134
Upgrade OS firmware	135
TFTP	135
FTP	135
USB	135
FortiEdge Cloud	135
GUI	135
Upgrade modem firmware	136
TFTP	136
FTP	136
USB	136
FortiEdge Cloud	136
GUI	136

SMS notification	137
Remote diagnostics via SMS	137
Configure the system syslog	138
Export system logs to remote syslog servers	138
Configure syslog database array	138
Support for SNMP (read-only) and traps	139
Typical SNMP commands	139
Sample SNMP commands	140
Executable SNMP commands	142
Get MIB2 interface statistics via SNMP	142
Access other devices via SSH	142
Entity certificates in FortiExtender	143
Certificate for HTTPS management access	143
Third-party certificates through an SCEP server	143
Automation stitching in digital I/O ports	147
Creating automation stitches	147
Digital I/O port functions	152
Configure Bluetooth Low Energy	155
Troubleshooting, diagnostics, and debugging	157
Troubleshooting	157
Can't manage the FortiExtender from FortiEdge Cloud	157
Can't start an Internet session	157
Status, diagnostics, and debugging commands	158
Diagnose from Telnet	158
Collect complete diagnostics information	159
Configure LTE settings	160
Add a new carrier profile	160
Add a new operator/carrier	160
Create a data plan	161
Activate a SIM card	163
Configure start session timeout	163
Check the recorded SIM card IMSI number	164
Delete the recorded SIM card IMSI number	165
Set the default SIM	165
Set the default SIM by preferred carrier	165
Set the default SIM by low cost	165
Set the default SIM by SIM slot	166
Enable SIM-switch	166
Dual modems	168
Dual-modem in IP pass-through mode	169
Dual modems in NAT mode	169
Unlock SIM pin	169

Change Log

Date	Change Description
2026-06-10	Updated IPsec VPN support for third-party certificates on page 84 .
2026-06-03	Updated SMS notification on page 137 and Remote diagnostics via SMS on page 137 .
2026-03-27	Updated Configure address/subnet on page 74 .
2026-03-23	Initial release.

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 FortiEdge 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 FortiEdge Cloud, refer to their respective Admin Guides.

Getting started

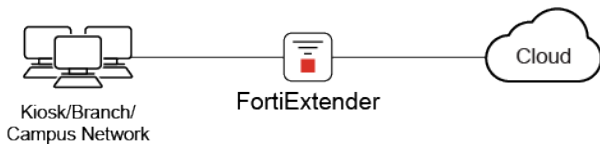
FortiExtender works as a standalone device when it is not managed by FortiGate or FortiEdge Cloud. A standalone FortiExtender can work in either IP pass-through or NAT mode. You can configure a standalone FortiExtender device from its CLI (Console/SSH) or GUI.



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



- When configuring the administrator password, the password must be at least 12 characters long and a combination of uppercase letters, lowercase letters, numbers, and symbols (`\~`!#$%^&* _+=|:;<, >./-``).
 - When accessing a FortiExtender device via SSH, after five failed login attempts there will be a ten minute temporary lockout period before the user is allowed to try again.
-



This section contains topics to help you get started with setting up your FortiExtender.

- [Management and Operation mode on page 10](#)
- [Essential LTE settings on page 13](#)
- [Essential networking configurations on page 15](#)
- [Essential wireless configurations on page 21](#)
- [IPsec VPN tunnels on page 25](#)

Management and Operation mode

When configuring your standalone FortiExtender, set the discovery type to *local* so FortiExtender will not try to search for another Controller such as a FortiGate or FortiEdge Cloud. In local mode, all configuration is done locally on the FortiExtender device.

Once you configure your management mode, you can configure the operation mode. You can configure FortiExtender to operate in either NAT (router) mode, or in IP-passthrough mode.

- **IP pass-through mode:** FortiExtender distributes the WAN IP address provided by the NSP to the device behind it. See [IP pass-through mode on page 12](#)
- **NAT mode:** In this mode, the LAN port on the FortiExtender can support multiple devices (e.g., PCs, printers, etc.). The FortiExtender works as a gateway of the subnet behind it to forward traffic between the LAN and the LTE WAN. See [NAT mode on page 13](#).

To configure the FortiExtender management and mode of operation - CLI:

```
config system management
  set discovery type local
  config local
    set mode [nat | ip-passthrough]
  end
end
```

To configure the FortiExtender management and mode of operation - GUI:

1. From the FortiExtender GUI, go to *Settings > Management* and edit *Management Setup*.
2. In *Controller* section, set the controller to *local*.
3. In the *Local* section, set *Mode* to *nat* or *ip-passthrough*.

The image shows a 'Management Setup' dialog box. At the top right are 'Cancel' and 'Save' buttons. The 'Controller' section has four buttons: 'auto', 'fortigate', 'cloud', and 'local' (which is highlighted in green). The 'Local' section has a 'Mode' label and two buttons: 'nat' (highlighted in green) and 'ip-passthrough'.

4. When you are finished, click Save.

Check current management mode

You can configure and manage your FortiExtender from FortiGate or FortiEdge Cloud. For FortiEdge Cloud management, the FortiExtender must have a valid support contract as well as a FortiEdge Cloud license.

If you are not sure "who" is your FortiExtender's controller, use the following command to find out:

```
FX511FTQ21001152 # get extender status
Extender Status
  name : FX511FTQ21001152
  mode : CAPWAP
  session : active
    fext-addr : 192.168.101.43
    ingress-intf : lan
    fext-wan-addr : 26.237.146.79
    controller-addr : 192.168.101.63:5246,25246
    controller-name : FG200FT921901199
    uptime : 0 days, 0 hours, 2 minutes, 25 seconds
    management-state : CWWS_RUN
  session : standby
    fext-addr : 0.0.0.0
    ingress-intf :
    fext-wan-addr : 26.237.146.79
    controller-addr : 0.0.0.0:5246,25246
    controller-name :
    management-state : CWWS_SULKING (H)
  session : obm
```

```
fext-addr : 10.107.41.43
ingress-intf : wan
controller-addr : fortiextender-alpha-dispatch.forticloud.com:443
account-id : 1208893
uptime : 0 days, 0 hours, 3 minutes, 33 seconds
management-state : CWS_RUN
base-mac : 94:FF:3C:0D:1A:C0
network-mode : ip-passthrough (capwap)
fgt-backup-mode : backup
discovery-type : static
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
```

IP pass-through mode

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

Enable IP pass-through mode

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

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

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

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 lte1-mapping lan
end
```

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

```
config system virtual-wire-pair
    set lte1-mapping port4
end
```



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

NAT mode

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

The following features are supported in NAT mode:

- [Interface management on page 37](#)
- [DHCP configurations on page 54](#)
- [System routing on page 60](#)
- [Configure PBR routing on page 61](#)
- [Firewall on page 74](#)
- [VPN on page 78](#)
- [SD-WAN on page 94](#)
- [Health monitoring on page 125](#)

Essential LTE settings

When setting up your FortiExtender for the first time, you can configure the following LTE settings essential to getting started.

- [Activate SIM card on page 14](#)
- [Configure PIN on page 14](#)
- [Create a Data Plan on page 15](#)

Activate 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.

```
config lte setting
  config modem1
    set advanced enable
    config advanced-settings
      set sim-activation-delay 300
    end
  end
end
end
```

The "set sim-activation-delay 300" command is used 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.

See [Activate a SIM card on page 163](#).

Configure PIN

You must enable and configure a PIN on the SIM setting.

To configure PIN - CLI:

```
config lte setting modem1
  set sim1-pin enable
  set sim1-pin "xxxx"
end
end
```

To configure PIN - GUI:

1. From the FortiExtender GUI, go to *LTE > Settings* and edit *Modem1 System Settings*.
2. In *SIM 1 Pin*, click *enable*.
3. In *SIM 1 Pin Code*, enter the SIM PIN.

Settings

Cancel

Save

Default SIM

sim1

sim2

by-carrier

by-cost

GPS

enable

disable

Active GPS Antenna

enable

disable

SIM 1 Pin

enable

disable

SIM 1 Pin Code*

4. When you are finished, click Save.

Create a Data Plan

A Data Plan contains information about the service plan that you have signed up or subscribed from a mobile service provider or carrier as well as configurations to define how each model selects a SIM card. It identifies your mobile service provider, and contains information such as your SIM credentials, allowed data usage, and billing cycle.

See [Create a data plan on page 161](#).

Essential networking configurations

To get started, you should make the following essential network configurations on your FortiExtender device:

- [LAN interface on page 16](#)
- [LAN addressing on page 16](#)
- [DHCP server on page 17](#)
- [Health checks on page 18](#)
- [VWAN interface on page 19](#)

LAN interface

The 4-port LAN-switch interfaces can be configured. By default, only FortiExtender Vehicle models have the four LAN ports included into the lan-switch interface; for every other model, port4 (PoE port) is not part of the lan-switch interface, but it can be added if required:

See [Configure LAN switch on page 41](#).

LAN addressing

The FortiExtender LAN interface is a critical connection point for integrating the extender into your local network. It allows FortiExtender to deliver cellular WAN connectivity to connected devices. It also enables direct access to the extender's management interface for configuration and monitoring.

A properly configured LAN interface delivers:

- Reliable routing of internet traffic from the LTE/5G network to internal devices.
- Device accessibility for administrators via local web GUI or CLI.
- Correct IP addressing and DHCP behavior, especially when FortiExtender acts as a DHCP server or relay.

To configure the LAN IP address - CLI:

```
config system interface
  edit lan
    set type lan-switch
    set status up
    set mode static
    set ip 192.168.2.1/24
    set gateway 0.0.0.0
    set mtu-override disable
    set distance 50
    set vrrp-virtual-mac disable
    config vrrp
      set status disable
    end
    set allowaccess https
  next
end
```

To configure the LAN IP address - GUI:

1. From the FortiExtender GUI, go to *Networking > Interface* and edit *LAN Switch*.
2. In *IP*, enter the IP address.

The screenshot shows a configuration interface for a network interface. It includes sections for Port Members, Status, STP, MTU Override, Mode, IP, Gateway, and As DHCP Server. Each section contains buttons or input fields to configure the respective settings.

DHCP server

FortiExtender includes a built-in DHCP server that can be enabled on its LAN interface to automatically assign IP addresses and network settings to connected client devices. Administrators can configure the DHCP range, lease time, and static IP reservations. For security, the DHCP server can also be restricted to known MAC addresses

For more information about DHCP servers, see [DHCP configurations on page 54](#)

To configure the DHCP server - CLI:

```
config system dhcpserver
edit dhcpserver1
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 192.168.2.1
set netmask 255.255.255.0
set interface lan
set start-ip 192.168.2.100
set end-ip 192.168.2.200
set mtu 1500
set vci_match disable
set reserved-address disable
next
end
```

To configure the DHCP server - GUI:

1. From the FortiExtender GUI, go to *Networking > Interface* and edit *LAN Switch*.
2. Under the *DHCP Server Config* section, enter your DHCP settings.

IP	192.168.2.1/24	Gateway	0.0.0.0	As DHCP Server		
				<input checked="" type="button" value="enable"/>	disable	backup
DHCP Server Config						
Name*	dhcpserver1		Default Gateway*			
				192.168.2.1		
Net Mask*	255.255.255.0		Lease Time*			
				86400		
Start IP*	192.168.2.100		End IP*			
				192.168.2.200		
DNS Service	default		Static Lease			
				enable	<input checked="" type="button" value="disable"/>	

Health checks

You can configure health checks to verify signal strength and monitor the availability and performance of link connections. They can provide important information for the LTE or 5G links. When a health check instance is configured, it automatically tests connectivity to the predefined targets (such as public IPs). This ensures that FortiExtender can detect network outages or degraded conditions and take corrective actions like WAN failover and failback.

For more information, see [Perform link health check on page 126](#).

To configure a health check - CLI:

```
config hmon hchk
edit hcheck1
set protocol ping
set interval 5
set probe-cnt 1
set probe-tm 2
set probe-target 8.8.8.8
set interface lte1
set src-type none
set filter rtt loss
next
end
```

To configure a health check - GUI:

1. From the FortiExtender GUI, go to *Health Check* and click *Create Health Check*.
2. Configure your health check parameters.

Health Check

Cancel

Save

ID*

hcheck1

Interface

lte1

Protocol

ping

http

dns

Interval

5

Probe Count

1

Probe Timeout

2

Probe Target*

8.8.8.8

Source Type

none

interface

ip

- When you are finished, click Save.

VWAN interface

Once you configure your health checks, you can apply them to a Virtual WAN (VWAN) member. When you create a VWAN member, you can then create a VWAN interface.

For more information, see [Configure Virtual-WAN interface on page 47](#).

To configure a VWAN member and apply a health check - CLI:

```
config system vwan-member
edit lte_vwan
set target
set priority 1
set weight 1
set in-bandwidth-threshold 0
set out-bandwidth-threshold 0
set total-bandwidth-threshold 0
set health-check
set health-check-fail-threshold 5
set health-check-success-threshold 5
set link-cost-factor packet-loss
set latency-threshold 5
set jitter-threshold 5
set packetloss-threshold 100
next
end
```

To configure a VWAN member and apply a health check - GUI:

- From the FortiExtender GUI, go to *Virtual WAN* and click *Create Virtual WAN Member*.
- Configure your VWAN member parameters and select the health check you previously created.

Virtual WAN Member

Cancel

Save

ID*	Target*	
lte_vwan	target.lte1 ▼	
Priority*	Weight*	
1	1	
Health Check	Health Check Fail Threshold	Health Check Success Threshold
hcheck1 ▼	5	5
Link Cost Factor	Latency Threshold	
packet-loss ✕ latency ✕ jitter ✕ ▼	5	
Jitter Threshold	Packet Threshold	
5	100	

3. When you are finished, click Save.

To configure a VWAN interface - CLI:

```
config system interface
edit vwan
set type virtual-wan
set status up
set algorithm redundant/WTT
set redundant-by priority/cost
set FEC connection/dest_ip/source_dest_ip_pair/source_ip
set session-timeout 60
set grace-period 0
set members
next
end
```

To configure a VWAN interface - GUI:

1. From the FortiExtender GUI, go to *Virtual WAN* and click *Create Virtual WAN*.
2. Configure your VWAN parameters and select the VWAN member you previously created.

Virtual WAN

Cancel Save

ID*

1

Type

virtual-wan

Algorithm

redundant

WRR

Redundant By

priority

cost

FEC

source_ip

dest_ip

source_dest_ip_pair

connection

Session Timeout

60

Grace Period

60

Members

lte_vwan x

Status

up

down

3. When you are finished, click Save.

Essential wireless configurations

Some FortiExtender and FortiExtender Vehicle units can be configured as a wireless AP. To get started, you should make the following essential wireless configurations on your FortiExtender device:

- [Country Code on page 21](#)
- [Wireless WAN networks on page 22](#)
- [Virtual Access Points and SSID on page 23](#)
- [Radio profiles on page 24](#)

For more information about configuring WiFi capable FortiExtender Vehicles, refer to the [FortiExtender Vehicle WiFi Configuration Guide](#).

Country Code

The maximum allowed transmitter power and permitted radio channels for WiFi networks vary, depending on the country or region of the world where the WiFi network is located. For this reason, it is important that you set your geographic location correctly before configuring the WiFi settings on your FortiExtender.

To configure the country code - CLI:

```
config wifi wifi-general
  set country-code ES
end
```

To configure the country code - GUI:

1. From the FortiExtender GUI, go to *Wi-Fi > Wi-Fi Settings*.
2. In *Country Code*, select the country the device is located in.
3. When you are finished, click *Save*.

Wireless WAN networks

On FortiExtender and FortiExtender Vehicle models with wireless radios, you can configure them to operate in the following modes:

- **Access Point (AP) mode:** FortiExtender operates as a standalone wireless access point, providing direct Wi-Fi connectivity to local client devices. This mode can be used for remote or temporary locations without existing infrastructure or for mobile deployments such as vehicles or kiosks.
- **Station (STA) mode:** FortiExtender can connect to an external Wi-Fi network as a wireless client, using that wireless connection as a WAN uplink. This enables the FortiExtender to route traffic through an existing Wi-Fi infrastructure instead of—or in addition to—its LTE/5G or Ethernet interfaces.
- **AP and Station mode:** FortiExtender not only forms its own Wi-Fi network, but can also join an existing Wi-Fi network at the same time.

For more information, see [Essential wireless configurations on page 21](#).

To configure a FortiExtender Wi-Fi network - CLI:

```
config wifi wifi-networks
  edit Depot_WiFi
    set ssid DEPOT_WIFI
    set security-mode WPA-Enterprise
    set identity
    set password
  next
end
```

To configure a FortiExtender Wi-Fi network - GUI:

1. From the FortiExtender GUI, go to *Wi-Fi > W-Fi Networks* and click *Create WiFi Networks*.
2. In the *Add/Edit/Connect WiFi Network* dialog, create the WiFi network with an SSID and security mode.

Add/ Edit/ Connect Wi-Fi Client Network Cancel Save

ID Security Mode OPEN ▾

SSID

Scan Results Scan AP

SSID ▾ Channel ▾ Security Mode ▾ Rate ▾ BSSID ▾ RSSI ▾ ⚙

No data available to display

- When you are finished, click **Save**.

Virtual Access Points and SSID

FortiExtender supports the creation of Virtual Access Points (VAPs), each representing a unique SSID. An SSID is the network name broadcast by the extender, allowing client devices to identify and connect to the wireless network.

To configure an SSID - CLI

```
config wifi vap
edit SSID1
set ssid FEV-WIFI
set broadcast-ssid enable
set dtim 1
set rts-threshold 2347
set max-clients 0
set wlan-bridge yes
set wlan-members
config ap-security
set security-mode WPA2-Personal
set pmf
set passphrase *****
end
next
end
```

To configure an SSID - GUI

- From the FortiExtender GUI, go to *Wi-Fi > SSIDs* and click *Create SSID*.
- Configure your SSID and select a security mode.

SSID Cancel Save

ID Broadcast SSID

SSID1 enable disable

SSID WLAN Bridge

FEV-WIFI yes

WLAN Members

Security Mode Passphrase

WPA2-Personal

3. When you are finished, click Save.

Radio profiles

A FortiExtender Radio Profile defines the operational parameters of the device's Wi-Fi radio, such as frequency band, channel settings, and transmit power. It determines how the wireless radio behaves and is essential for ensuring optimal performance, regulatory compliance, and minimal interference in the deployment environment. Each Radio Profile can be associated with one or more VAP, allowing multiple SSIDs to share the same physical radio configuration.

To configure radio profiles - CLI:

```
config wifi radio-profile
edit radio2G
set band 2GHz
set status enable
set role lan
set operating-standards auto
set beacon-interval 100
set 80211d enable
set max-clients 0
set power-mode auto
set channel 1 11 6
set bandwidth auto
set extension-channel auto
set guard-interval auto
set vap SSID1
next
edit radio5G
set band 5GHz
set status enable
set role lan
set operating-standards auto
set beacon-interval 100
set 80211d enable
set max-clients 0
```

```

set power-mode auto
set channel 36 165 44 149 157
set bandwidth auto
set extension-channel auto
set guard-interval auto
set vap SSID1
next
end

```

To configure radio profiles - GUI:

1. From the FortiExtender GUI, go to *Wi-Fi > Radio Profile* and click *Create Radio*.
2. Enter your radio profile configurations.

Radio Profile

Cancel Save

ID*	radio2G	Role	LAN
Band		Bandwidth	auto
Channel	☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11 ☐ 12 ☐ 13	Status	enable
Extension Channel	auto	Guard Interval	auto
Operating Standards	auto	Power Mode	auto
SSID	SSID1 ✕		

3. When you are finished, click *Save*.

IPsec VPN tunnels

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

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

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.

After the phases are defined, you can configure firewall policies and routes to control and direct traffic.

For more information about VPNs, see [Configure VPN on page 78](#).

To configure VPN Phases - CLI:

```
config vpn ipsec
  config phase1-interface
    edit ipsec1
      set ike-version 2
      set keylife 86400
      set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-sha
      set dhgrp 14 5
      set interface
      set type static
      set remote-gw
      set authmethod psk
      set psksecret
      set localid
      set peerid
      set add-gw-route disable
      set dev-id-notification disable
      set monitor
    next
  config phase2-interface
    edit IPsec_p2
      set phase1name
      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 subnet
      set src-subnet 0.0.0.0/0
      set src-port 0
      set dst-addr-type subnet
      set dst-subnet 0.0.0.0/0
      set dst-port 0
    next
  end
```

To configure VPN Phases - GUI:

1. From the FortiExtender GUI, go to *VPN* and click *Create IPsec Tunnel* to initiate the VPN tunnel configuration wizard.
2. Follow the onscreen instructions and enter your configurations.

Create VPN Tunnel

Cancel

Next

1 Basic Setup

2 Authentication

3 Traffic Selection

Basic Setup

Name*

IPsec1

Gateway

static

ddns

Remote IP*

35.128.94.26

Interface

lte1

3. When you are finished, click Save.

Main LTE/5G features

FortiExtender offers the following main LTE/5G features:

- [Cellular capabilities on page 28](#)
- [Supported wireless carriers on page 29](#)
- [SIM mapping on page 30](#)
- [Add a data plan and APN on page 30](#)
- [Global SIM with roaming on on page 31](#)
- [SIM-switch on page 31](#)
- [Get modem status on page 34](#)
- [Stopping data traffic on overaged LTE interface on page 35](#)
- [OBM management on page 35](#)
- [Multiple Packet Data Network \(PDN\) on page 36](#)



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:



To avoid a known Quectel RACH issue on FEX-511F, Fortinet has disabled T-Mobile 5G Band n41 (refer to the FortiExtender Release Notes [Known issues](#)).

- **5G NR:** n1, n3, n5, n7, n8, n20, n28, n38, n40, 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 supports all major wireless carriers in Europe and North America, including the following:

Region	Carrier
Europe	• A1MobilKom • Bouygues • O2 • Orange • SFR • Swisscom • T-Mobile • Vodafone
North America	• AT&T • Bell • Rogers • Sasktel • Sprint • Telus • T-Mobile • Verizon



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

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



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

SIM mapping

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

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

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

```
FX201E5919000035 # config lte simmap
FX201E5919000035 (simmap) # show
config lte simmap
end
FX201E5919000035 (simmap) # edit 1
FX201E5919000035 (1) <M> # set mcc 332
FX201E5919000035 (1) <M> # set mnc 321
FX201E5919000035 (1) <M> # set carrier <carrier name>
FX201E5919000035 (1) <M> # next
```



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

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

Add a data plan and APN

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

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

With SIM-switch enabled, FortiExtender automatically switches to sim2 to maintain the current LTE connection when any of the following situations occurs:

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

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

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

```
config lte setting modem1
    config auto-switch
        set by-signal enable /*enable the switch by signal feature*/
        set by-data-plan enable /*enable the switch by data usage feature*/
    end
end
config lte plan
    edit <plan>
        set capacity <data plan in MB>
        set billing-date <billing date>
```

```

set overage {enable | disable}
set signal-threshold <-100> /*RSSI to be evaluated*/
set signal-period <600> /*Signal evaluation time in seconds*/
next

```

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

RSSI Values and LED State

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



SIM-switch is a feature in data plan configuration which can be configured from FortiEdge Cloud or locally from the FortiExtender GUI. All the aforementioned parameters can be configured from the FortiExtender CLI.

SIM switch-back

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

To enable SIM switch-back:

```

FX211E5919000006 (auto-switch) #
  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 [FortiExtender 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.

Parameter	Description
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.
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: • 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 (overage), 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



For most FortiExtender models, you can connect up to 16 backend devices (including FortiAPs, FortiGates, and even non-Fortinet devices) to the USB OBM port.

For a list of models with hardware-based limitations, refer to [Known issues](#) in the *FortiExtender Release Notes*.

FortiExtender can be connected to the console port of any device behind it through 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 a 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.
```



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

Multiple Packet Data Network (PDN)

The multiple PDN feature is only available in select models such as FEX-511G. This feature enables you to establish up to four data sessions, each over a different APN.

When FortiExtender is in NAT mode, proper routing and firewall policies need to be configured.

When FortiExtender is in IP-passthrough mode, the proper interface mapping needs to be configured between the LTE interfaces and the physical or VLAN interfaces to be used.

Interface management

FortiExtender 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: • <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: • <code>up</code>—Enabled. • <code>down</code>—Disabled.
<code>set mode {static dhcp}</code>	Set the interface IP addressing mode: • <code>static</code>—If selected, FortiExtender will use a fixed IP address. See <code>set ip <ip></code> below. • <code>dhcp</code>—If selected, FortiExtender will work in DHCP client mode.
<code>set ip <ip></code>	(Applicable only when IP addressing mode is set to "static".) Specify an IPv4 address and subnet mask in the format: <code>x.x.x.x/24</code>
<code>set gateway <gateway></code>	Set an IPv4 address for the router in the format: <code>x.x.x.x</code>

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

FortiExtender 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 28](#).

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
  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 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 via LTE, you must use FortiEdge 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

== [ lte1 ]
name: lte1        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 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 - CLI:

```

config system lan-switch
config ports
edit port1
next
edit port2
next
edit port3
next
edit port4
next
end
end

```

To remove a port from the LAN switch - CLI:

```

config system lan-switch
config ports
delete port4
next
end

```

To add a port to the LAN switch - CLI:

```
config system lan-switch
config ports
    edit port4
next
end
```

To configure LAN switch configuration - GUI:

1. From the FortiExtender GUI, go to *Networking > Interface* and edit *LAN Switch*.
2. In *Port Members*, add or remove the LAN ports.

The screenshot shows the configuration page for a LAN switch interface named 'lan'. The 'Type' is set to 'lan-switch'. Under 'Allow Access', the 'https' checkbox is checked, while 'http', 'ping', 'ssh', 'telnet', and 'snmp' are unchecked. The 'Distance' is set to 50. In the 'Port Members' section, there are buttons for 'port1', 'port2', 'port3', and 'port4', each with a close icon. The 'Status' section has 'up' and 'down' buttons, with 'up' being active. The 'STP' section has 'enable' and 'disable' buttons, with 'enable' being active. At the bottom, the 'MTU Override' has 'enable' and 'disable' buttons, with 'disable' being active. The 'Mode' section has 'dhcp' and 'static' buttons, with 'static' being active.

3. When you are finished, click **Save**.

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 agg1
    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
    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

By default, all cellular FortiExtender models block DHCP traffic on port UDP 67, preventing them from passing from the internal to the external side of the LTE/5G modem.

The private-network option located within the `lte` plan enables the cellular modem to forward DHCP packets to the WAN/internet via the LTE/5G modem interface, instead of blocking them. This feature is typically used in

private LTE/5G networks when relaying DHCP requests to a DHCP server hosted within a remote network is required. This feature can also be used on public LTE/5G networks if necessary.

To enable a private network to forward DHCP traffic via the LTE/5G modems:

```
config lte plan
  edit "ATTPlan" <-- As a best practice, the LTE plan name should match your carrier network
  provider's name.
    set private-network enable
  next
end
```

Configure Virtual-WAN interface

Configure a firewall and router policy to enable packets to travel between the LAN and Virtual-WAN (VWAN).

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 lte1
    set src-type none
    set filter rtt loss
  next
end
```

Step 2: Configure VWAN members



The latency-threshold and jitter-threshold values depend on many external factors such as the device location and the cellular network connection. If the default values do not work, Fortinet recommends that you experiment and gradually increase the threshold values if the VWAN status shows as unhealthy (see [VWAN status check on page 96](#)).

You can also run `get hmon hchk <vwan_member_name>` and adjust the latency-threshold value to be greater than the median `rtt max`, and the jitter-threshold value to be greater than the median `rtt sd`.

```
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.lte1
    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 200
    set jitter-threshold 100
    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 lte1
    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
```

Configure WiFi VAPs as members of switch interface

Starting from its 7.4.4 release, FortiExtender has enhanced the configuration schema for the system switch-interface to support WiFi Virtual Access Points (VAPs) as members of a switch-interface. A VAP can now be added as members of a switch-interface as long as it is not specified as a WLAN bridge. In so doing, the VAP shares DHCP servers and firewall policies with the switch-interface.

This feature allows for greater flexibility in configuring switch-interfaces and VAPs, enabling you to manage your network resources and configurations more efficiently.

To add a WiFi VAP as member of a switch interface:

1. Create a virtual access point (VAP), with wlan-bridge set to no.

```
FXW30FTF23000020 # config wifi vap
FXW30FTF23000020 (vap) # show
config wifi vap
    edit vap1
        set ssid FXW30F-WiFi
        set broadcast-ssid enable
        set dtim 1
        set rts-threshold 2347
        set max-clients 0
        set target-wake-time enable
        set bss-color-partial enable
        set mu-mimo enable
        set wlan-bridge no
    config ap-security
        set security-mode WPA2-Personal
        set pmf
        set passphrase *****
    end
next
end
```

2. Add the VAP to the radio profile.

```
FXW30FTF23000020 # config wifi radio-profile
FXW30FTF23000020 (radio-profile) # show
config wifi radio-profile
    edit r2
        set band 5GHz
        set status enable
        set role lan
```

```

        set operating-standards auto
        set beacon-interval 100
        set 80211d enable
        set max-clients 0
        set power-mode auto
        set channel
        set bandwidth auto
        set extension-channel auto
        set guard-interval auto
        set bss-color-mode auto
        set vap vap1
    next
end

```

3. Add the VAP as a member of a switch interface.

```

FXW30FTF23000020 (switch-interface) # show
config system switch-interface
    edit lan
        set vlan-support disable
        config member
            edit m1
                set type vap
                set vap vap1
                set pvid 0
            next
        end
        set stp disable
    next
end

```

4. Verify the current VAP and bridge interface maps.

```

FXW30FTF23000020 # get wifi vap-maps all
vap id          bridg name      ap interface
vap1            lan             aap0
vap2            vap2            aap1
vap3            vap3            aap1

FXW30FTF23000020 #

```

Dynamic Frequency Selection channels

In many countries, regulatory requirements may limit the number of 5 GHz channels available or restrict their usage because the spectrum is shared with other technologies and services. For example, in the US, sixteen of the twenty-five 5 GHz channels are used by military, weather radar, and satellite communications. Wi-Fi

networks operating in those bands are required to employ a radar detection and avoidance capability known as Dynamic Frequency Selection (DFS).

Using DFS, supported FortiExtenders automatically scan for and adjust the frequency of a radio if a radar event is detected. This greatly expands the number of channels available for use, improving performance.



DFS channels are enabled on FEV21xF and FBS10F models, but access is dependent on regional regulations. For example, in the CE region, regulations forbid FEV models from using DFS models when operating in AP mode. They can only use DFS 100-140 channels when operating in client mode.

Note the following behavior when selecting channels:

- You cannot select a fixed DFS channel and must select at least one non-DFS channel. This is to prevent FortiExtender from spending 60-600 seconds running a Channel Availability Check (CAC) to check for signals on that channel.
- To ensure that Wi-Fi on FEV21xF devices is available as quickly as possible, DFS channels are skipped during the automatic initial channel selection on the 5GHz Wi-Fi radio.

The following table summarizes the conditions under which DFS channel selections are available for each FortiExtender model:

Scenario	DFS channel selection permission	
	FEV21xF	FBS10F
Fixed channel	Deny	Deny
Initial channel selection once the radio is up	Deny	Allow
Running time channel selection	Allow	Allow



In FEV-21xF models:

- Channels 132/136 can only work in 20/40MHz.
- Channels 140/165 can only work in 20MHz.
- Channel 144 is not available.

In FEV-21xF-AM:

- Channels 132/136/140/144 can work in 20/40/80Mhz.
- Channel 165 can only work in 20MHz.

To configure DFS channels on a standalone FortiExtender - GUI:

1. From the FortiExtender GUI, go to *WiFi > Radio Profiles* and create a new or edit an existing profile.

2. Make your channel selections.
3. When you are finished, click Save.

To configure DFS channels on a standalone FortiExtender - CLI:

```
config wifi
  config radio-profile
    edit <profile>
      set channel <choose from DFS channel list>
    next
  end
```

Configure allowaccess for tunnel interface

Starting from FortiExtender 7.4.4 release, you can set and change allowaccess for a tunnel interface, as shown in the following example.

```
FX201E5920005963 # config system interface
FX201E5920005963 (interface) # show
edit tunnel_testing
  set type tunnel
  set mode static
  set ip 192.168.170.30/24
  set mtu-override disable
  set allowaccess http https ping snmp ssh telnet <== tunnel interface can edit this option
next
```

DHCP configurations

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

- [Configure DHCP server](#)
- [Configure DHCP relay](#)
- [DHCP client optimization on page 57](#)

Configure DHCP server

You can configure the DHCP server from FortiEdge 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: • <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: • <code>local</code>—The IP address of the interface of the DHCP server that is added becomes clients' DNS server IP address. • <code>default</code>—Clients are assigned the FortiExtender configured DNS server. • <code>specify</code>—Specify up to three DNS servers in the DHCP server configuration. • <code>wan-dns</code>—The DNS of the WAN interface that is added becomes clients' DNS server IP address.
<code>set dns-server1 <dns_server1></code>	Specify the IP address of DNS Server 1.
<code>set dns-server2 <dns_server2></code>	Specify the IP address of DNS Server 2.

CLI command	Description
set dns-server3 <dns_server3>	Specify the IP address of DNS Server 3.
set ntp-service {default specify}	Select an option for assigning a Network Time Protocol (NTP) server to DHCP clients: • local—The IP address of the interface of the DHCP server that is added becomes clients' NTP server IP address. • default—Clients are assigned the FortiExtender configured NTP servers. • specify—Specify up to three NTP servers.
set ntp-server1 <ntp_server1>	Specify the IP address of NTP Server 1.
set ntp-server2 <ntp_server2>	Specify the IP address of NTP Server 2.
set ntp-server3 <ntp_server3>	Specify the IP address of NTP Server 3.
set default-gateway <gateway>	Specify the default gateway IP address assigned by the DHCP server.
set netmask <netmask>	Specify the netmask assigned by the DHCP server.
set interface <interface>	Specify the interface on which the DHCP server is expected to run.
set start-ip <start_ip>	Specify the start IP address of the DHCP IP address range. For example, 192.168.1.100.
set end-ip <end_ip>	Specify the end IP address of the DHCP IP address range. For example, 192.168.1.120.
Set mtu <mtu size>	Specify the MTU size. The default value is 1500.
Set reserved-address <enable/disable>	Set the reserved address enable or disable: • enable—enable reserved address option by configuring ip, mac and action as reserved or block. • disable—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 LAN interface(s) can be configured in static IP address mode locally or from FortiEdge 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 FortiEdge 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>
    next
end

```

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 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 58](#)
- [Service on page 58](#)
- [Target on page 58](#)

Address

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

Service

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

For example:

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

Target

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

The table below describes the commands for setting a target.

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

Example target configuration:

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



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

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

System routing

FortiExtender supports static routing and Policy Based Routing (PBR). Dynamic routing, such as ISIS and EIGRP, is not supported.



Both static routing and PBR apply to NAT mode only.

This section covers the following topics:

- [Configure static routing on page 60](#)
- [Configure PBR routing on page 61](#)
- [Configure dynamic routing — OSPF on page 63](#)
- [Configure multicast routing on page 73](#)

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: • <code>enable</code>—Enable the static route. • <code>disable</code>—Disable the static route.
<code>set dst <dst></code>	Specify the destination IP address and netmask of the static route in the format: <code>x.x.x.x/x</code>
<code>set gateway <gateway></code>	Specify the IP address of the gateway.
<code>set distance <distance></code>	Specify the administrative distance. The range is 1–255. The default is 1.
<code>set device <device></code>	Specify the name of the outgoing interface.
<code>set comment [comment]</code>	Enter a comment (optional).

Example static route configuration:

```
config router static
```

```

edit 1
    set status enable
    set dst 0.0.0.0/0
    set gateway 192.168.2.1
    set distance 5
    set device lan
    set comment
next
End

```

Configure PBR routing

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

CLI Command	Description
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 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.



- 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)

```
FX201E5919000057 (ospf) # show
config router ospf
  set status disable
  set router-id 0.0.0.0
  config area
    edit 192.168.200.24
    next
  end
  config network
    edit 1
      set prefix 192.168.200.0/24
      set area 192.168.200.24
    next
  end
  config ospf-interface
    edit 1
      set status enable
      set interface lan
      set mtu-ignore enable
      set cost 3400
    next
  end
  config redistribute
    config connected
      set status disable
      set metric-type 2
      set metric 10
      set routemap redist-local-connected
    end
    config static
      set status disable
      set metric-type 2
      set metric 10
      set routemap redist-static
    end
  end
end
end
```

Parameter	Description	Type	Size	Default								
status	Set the status of the OSPF.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable OSPF.</td></tr><tr><td>disable</td><td>Disable OSPF.</td></tr></table>	Option	Description	enable	Enable OSPF.	disable	Disable OSPF.					
Option	Description											
enable	Enable OSPF.											
disable	Disable OSPF.											
router-id	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.	IPv4 address	-	0.0.0.0								
config area	OSPF area configuration. 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	IPv4 address	-	none								
config network	OSPF network configuration.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>prefix</td><td>Prefix is used to identify network/subnet address for advertising to the OSPF domain.</td></tr><tr><td>area</td><td>Attach the network to area.</td></tr></table>	Option	Description	prefix	Prefix is used to identify network/subnet address for advertising to the OSPF domain.	area	Attach the network to area.					
Option	Description											
prefix	Prefix is used to identify network/subnet address for advertising to the OSPF domain.											
area	Attach the network to area.											
config ospf-interface	OSPF interface configuration.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>status</td><td>Enable/disable OSPF processing on the said interface.</td></tr><tr><td>interface</td><td>Interface name must be the VPN tunnel interface as OSPF is built over IPSEC VPN.</td></tr><tr><td>cost</td><td>Cost of the interface: 0 - 65535; 0 means auto-cost.</td></tr></table>	Option	Description	status	Enable/disable OSPF processing on the said interface.	interface	Interface name must be the VPN tunnel interface as OSPF is built over IPSEC VPN.	cost	Cost of the interface: 0 - 65535; 0 means auto-cost.			
Option	Description											
status	Enable/disable OSPF processing on the said interface.											
interface	Interface name must be the VPN tunnel interface as OSPF is built over IPSEC VPN.											
cost	Cost of the interface: 0 - 65535; 0 means auto-cost.											

Parameter	Description	Type	Size	Default																										
		<table><tr><th>Option</th><th>Description</th></tr><tr><td></td><td>Interface cost used to calculate the best path to reach other routers in the same area.</td></tr><tr><td>mtu-ignore</td><td>Enable/disable ignore MTU. <code>mtu-ignore</code> prevents OSPF neighbor adjacency failure caused by mismatched MTUs. When <code>mtu-ignore</code> is enabled, OSPF will stop detecting mismatched MTUs before forming OSPF adjacency. When <code>mtu-ignore</code> is disabled, OSPF will detect mismatched MTUs, and OSPF adjacency is not established if MTU is mismatched.</td></tr></table>			Option	Description		Interface cost used to calculate the best path to reach other routers in the same area.	mtu-ignore	Enable/disable ignore MTU. <code>mtu-ignore</code> prevents OSPF neighbor adjacency failure caused by mismatched MTUs. When <code>mtu-ignore</code> is enabled, OSPF will stop detecting mismatched MTUs before forming OSPF adjacency. When <code>mtu-ignore</code> is disabled, OSPF will detect mismatched MTUs, and OSPF adjacency is not established if MTU is mismatched.																				
	Option	Description																												
		Interface cost used to calculate the best path to reach other routers in the same area.																												
mtu-ignore	Enable/disable ignore MTU. <code>mtu-ignore</code> prevents OSPF neighbor adjacency failure caused by mismatched MTUs. When <code>mtu-ignore</code> is enabled, OSPF will stop detecting mismatched MTUs before forming OSPF adjacency. When <code>mtu-ignore</code> is disabled, OSPF will detect mismatched MTUs, and OSPF adjacency is not established if MTU is mismatched.																													
config redistribute	Redistribute configuration.	option	-	none																										
		<table><tr><th>Option</th><th>Description</th></tr><tr><td rowspan="5">config connected</td><td><table><tr><th>Option</th><th>Description</th></tr><tr><td>status</td><td>Enable/disable redistributing connected routes.</td></tr><tr><td>metric-type</td><td>Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).</td></tr><tr><td>metric</td><td>Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.</td></tr><tr><td>routemap</td><td>Route map name.</td></tr></table></td></tr><tr><td rowspan="5">config static</td><td><table><tr><th>Option</th><th>Description</th></tr><tr><td>status</td><td>Enable/disable redistributing static routes.</td></tr><tr><td>metric-type</td><td>Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).</td></tr><tr><td>metric</td><td>Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.</td></tr><tr><td>routemap</td><td>Route map name.</td></tr></table></td></tr></table>			Option	Description	config connected	<table><tr><th>Option</th><th>Description</th></tr><tr><td>status</td><td>Enable/disable redistributing connected routes.</td></tr><tr><td>metric-type</td><td>Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).</td></tr><tr><td>metric</td><td>Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.</td></tr><tr><td>routemap</td><td>Route map name.</td></tr></table>	Option	Description	status	Enable/disable redistributing connected routes.	metric-type	Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).	metric	Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.	routemap	Route map name.	config static	<table><tr><th>Option</th><th>Description</th></tr><tr><td>status</td><td>Enable/disable redistributing static routes.</td></tr><tr><td>metric-type</td><td>Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).</td></tr><tr><td>metric</td><td>Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.</td></tr><tr><td>routemap</td><td>Route map name.</td></tr></table>	Option	Description	status	Enable/disable redistributing static routes.	metric-type	Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).	metric	Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.	routemap	Route map name.
	Option	Description																												
	config connected	<table><tr><th>Option</th><th>Description</th></tr><tr><td>status</td><td>Enable/disable redistributing connected routes.</td></tr><tr><td>metric-type</td><td>Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).</td></tr><tr><td>metric</td><td>Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.</td></tr><tr><td>routemap</td><td>Route map name.</td></tr></table>	Option	Description	status	Enable/disable redistributing connected routes.		metric-type	Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).	metric	Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.	routemap	Route map name.																	
		Option	Description																											
		status	Enable/disable redistributing connected routes.																											
		metric-type	Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).																											
		metric	Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.																											
	routemap	Route map name.																												
	config static	<table><tr><th>Option</th><th>Description</th></tr><tr><td>status</td><td>Enable/disable redistributing static routes.</td></tr><tr><td>metric-type</td><td>Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).</td></tr><tr><td>metric</td><td>Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.</td></tr><tr><td>routemap</td><td>Route map name.</td></tr></table>	Option	Description	status	Enable/disable redistributing static routes.	metric-type	Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).	metric	Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.	routemap	Route map name.																		
		Option	Description																											
		status	Enable/disable redistributing static routes.																											
		metric-type	Metric type integer. Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).																											
		metric	Used for the redistributed routes. The value range is from 1 to 16777214. The default is 10.																											
routemap	Route map name.																													

Configure OSPF redistribution

FortiExtender 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 prefix list

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>	Configure the prefix-list which defines the prefix (IP address and netmask) for the filter of redistribution. • prefix-name— for either static routes or connected routes • id—rule-id (1-65535) • action—permit/deny. Permit if it matches prefix network; deny if it does not match the exact prefix network. • le—(less than or equal to). The le 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. • ge— (greater than or equal to) The length specified should be longer than the length of the initial prefix.

Example configuration:

```

FortiExtender# 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> set action [permit deny] set match-ip- address <prefix- list> </pre>	Configure route-map which defines the redistributed routes. - route-map name—defines the route-map name - rule—routing rule - 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. 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.

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] </pre>	Configure router OSPF redistribute. - 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. - route-map—defined and configured on the route-map, see Configure

CLI Command	Description
<pre>set metric <value> set route-map <route-map name></pre>	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 can use the following CLI commands to verify that your configurations works as expected.

Verify OSPF status

```
#get router info ospf status
```

Verify OSPF interface

```
#get router info ospf interface
```

Verify OSPF neighbor adjacency

```
#get router info ospf neighbor
```

Verify OSPF database

```
#get router info ospf database
```

Verify OSPF routes

```
#get router info ospf route
```

Verify routing table

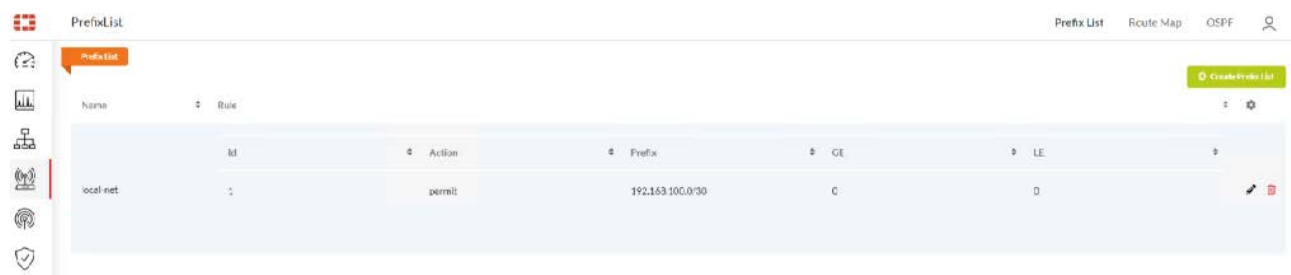
```
#get router info routing-table all
```

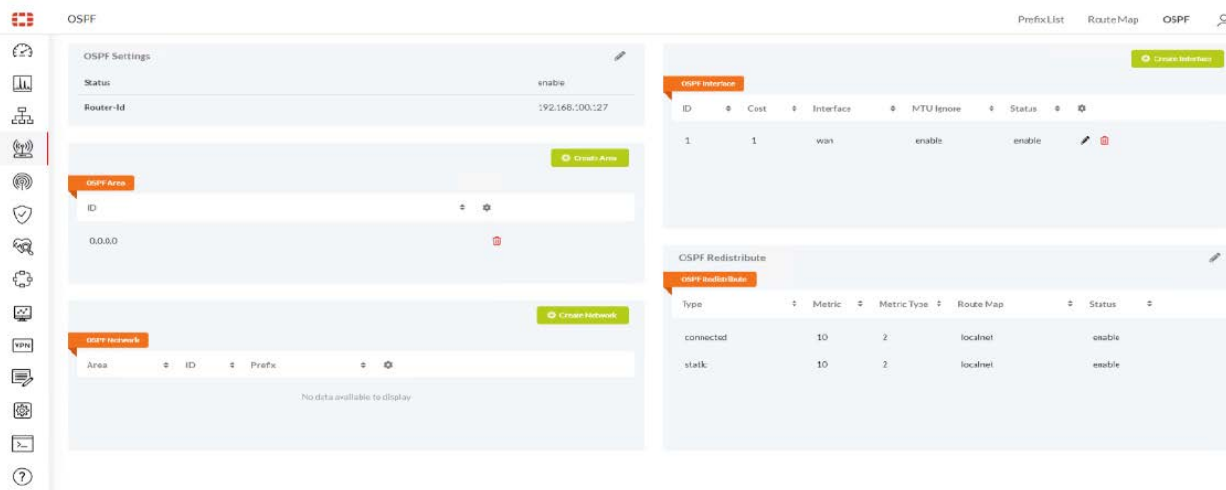
Configure OSPF GUI

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.





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

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
end

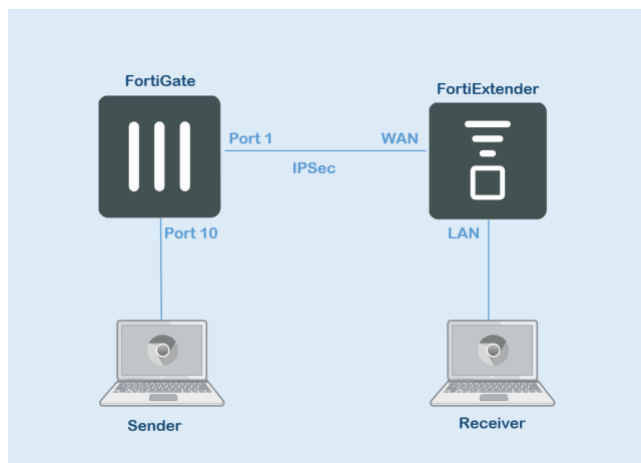
FortiExtender#config router ospf
    set status enable
    set router-id 169.254.254.127
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 169.254.254.0/24
            set area 0.0.0.0 next
        edit 2
            set prefix 169.254.254.127/32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

Multicasting network topology



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 74](#)
- [Configure protocol/port range on page 75](#)
- [Configure firewall policies on page 75](#)
- [Move firewall policies on page 77](#)

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>	Specify the address type: • <code>ipmask</code>—IPv4 address/mask in the format: <code>x.x.x.x/x</code> • <code>iprange</code>—IP addresses range. • <code>vsdb</code>—Video Streaming Database for video streaming traffic.

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.

CLI command	Description
<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.
<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: • <code>allow</code>—Allow access. • <code>deny</code>—Deny access.
<code>set status {enable disable}</code>	Set the status of the policy: • <code>enable</code>—Enable the policy. • <code>disable</code>—Disable the policy.
<code>set nat {enable disable}</code>	Select an option for NAT: • <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

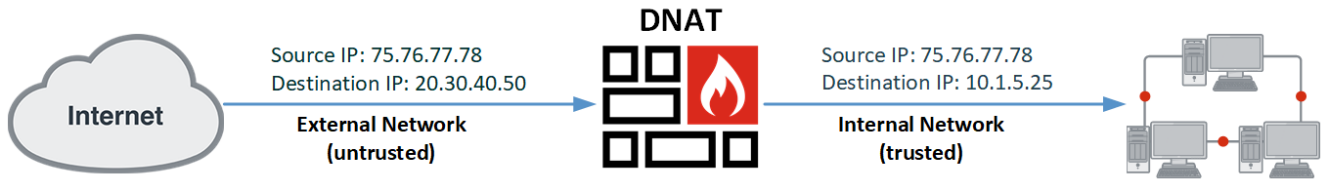
```



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

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.

Move firewall policies

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

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

```
config firewall policy
  edit filter1
    set srcintf any
    set dstintf any
    set srcaddr rec
    set dstaddr internet
    set action deny
    set status enable
    set service service1 service2 service3 service4
    set nat disable
  next
  edit filter2
    set srcintf lan
    set dstintf wan
    set srcaddr wow
    set dstaddr internet
    set action allow
    set status enable
    set service service1 service2 service3 service4
    set nat disable
  next
end
```

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

```
move filter1 after filter2
```

or

```
move filter2 before filter1
```

VPN

FortiExtender uses site-to-site IPsec VPN tunnels to connect branch offices to each other.

An IPsec VPN is established in two phases: Phase 1 and Phase 2. Several parameters determine how this is done, but the settings (except for IP addresses) need to match at both VPN gateways. There are default configurations that are applicable for most situations.

When a FortiExtender unit initiates a connection request to 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:

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



FortiExtender only supports Point-to-Point VPN, requiring the remote gateway to be explicitly defined in its IPsec Phase-1 configuration. This limits FortiExtender to operating solely as a Spoke in a Hub-Spoke VPN topology.

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 a FortiExtender, it must have a static public IP address and can work in VPN server mode.
-

Configure VPN

VPN configurations include the following operations:

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

Configure phase-1 parameters

Use the following commands to configure a VPN tunnel.

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

CLI command	Description
localid	Specify the local ID.
peerid	Accept the peer ID.
add-gw-route	Enable/disable automatically adding a route to the remote gateway.
dev-id-notification	Enable/disable the Device ID notification for the first IKE message.
monitor	Specify the IPsec phase1 interface as primary.

A Phase-1 interface can be of two categories:

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

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

- psk (pre-shared key)
- signature

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

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

Configure phase-2 parameters

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

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

Example VPN configuration:

```

config vpn ipsec phase1-interface
edit sec
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 port2

```

```
set type static
set remote-gw 192.168.100.100
set authmethod psk
set psksecret *****
set localid
set peerid
set add-gw-route disable
set dev-id-notification disable
set monitor pri
next
edit pri
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 port1
set type static
set remote-gw 192.168.90.100
set authmethod psk
set psksecret *****
set localid
set peerid
set add-gw-route disable
set dev-id-notification disable
set monitor
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
```

```
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
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
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

```

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

Import a third-party CA certificate

- From the Console: execute `vpn certificate ca import tftp <remote_file> <local_name> <ip>`
- From the GUI: Go to *Settings > Certificate* and under CA Certificate, click *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: Go to *Settings > Certificate* and under Entity Certificate, click *Import New Certificate*.

Use third-party certificates for IKE authentication

Two fields, "certificate" and "peer", are available in 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>
set peer <ca_cert_name>
set localid
set peerid
next
end
```

IPsec VPN supports more DH groups

Diffie-Hellman (DH) key exchange in phase1 is used to negotiate and exchange private keys for phase2. FortiExtender now provides more DH group options. New DH group options ("15", "16", "17", "18", "19", "20", "21", "27", "28", "29", "30", "31", "32") are added to the `ipsec phase1-interface/phase2-interface config` file.

Any DH groups less than 15 are not recommended due to their low security levels. And Elliptic Curve Groups ("19", "20", "21", "27", "28", "29", "30", "31", "32") offer better security compared to the MODP groups ("1", "2", "5", "14", "15", "16", "17", "18"). The DH groups in phase2 should be set to the same value as those for phase1, and PFS is recommended.

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.

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: • 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	The status of the DNS zone: - enable (default) - disable Note: This field is NOT required.
domain	Domain name. Note: The maximum length is 225 characters. This field is required.
type	Zone type. primary (default) — The primary DNS zone to manage entries directly. Note: This field is NOT required.
view	Zone view. - shadow: Shadow DNS zone to serve internal clients. (default) - public: Public DNS zone to serve public clients.

Parameter	Description
	Note: This field is NOT required
primary-name	Domain name of the default DNS server for this zone. Note: The maximum length is 225 characters. The default is dns. 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 host. This field is NOT required
ttd	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: • 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: • enable (default) • disable Note: This field is NOT required.
type	Resource record type: • 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.
ttd	Time-to-live for this entry. Note: The value ranges from 0 to 2147483647. The default is 0. The field is NOT required.

Parameter	Description
hostname	Hostname of the host. 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

Field	Description	Mandatory	Type	Value	Default value
server-select-method	Specify how configured servers are prioritized. - 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 from the shortest one. - 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).	Yes	option	least-rtt / failover	least-rtt

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.

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: • up—Enable the interface. • down—Disable the interface.
<code>set FEC {source dest ip-pair connection}</code>	Select a LLB metric to denote how to distribute traffic: • source—Traffic from the same source IP is forwarded to the same target.

CLI command	Description
	dest—Traffic to the same destination IP is forwarded to the same target. ip-pair—Traffic from the same source IP and to the same destination IP is forwarded to the same target. connection—Traffic with the same 5 tuples (i.e., a source IP address/port number, destination IP address/port number and the protocol) is forwarded to the same target
<code>set algorithm {redundant WRR}</code>	Select the LLB algorithm: redundant—Targets work in primary-secondary mode. WRR—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 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%
```

VWAN status check

To check the status of your VWAN connections, you can use the “`get vwan status`” command.

```
# get vwan status
vwan1:
algorithm redundant, by priority, FEC source_dest_ip_pair, target count 2, session count 0,
session_timeout 60, version 6
no name priority overage weight sess_cnt ref intf nexthop in_bw out_bw tot_bw data in/out TP
in/out
0 wan_vwan 1 no 1 0 2 wan 10.1.10.1 0 0 0 0/ 0 0/ 0
[unhealthy]
1 lte_vwan 1 no 1 0 2 lte1 100.101.237.166 0 0 0 0/ 0 0/ 0
[unhealthy]
```

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
```

Wi-Fi Settings

FortiExtender models with integrated Wi-Fi provide enhanced deployment flexibility by combining LTE/5G WAN connectivity with local wireless LAN access. With support for 802.11 standards, FortiExtender Wi-Fi models can function as standalone access points or complement existing Fortinet infrastructure.

The following Wi-Fi modes are supported:

- **Access Point (AP) mode:** FortiExtender operates as a standalone wireless access point, providing direct Wi-Fi connectivity to local client devices. In AP mode, FortiExtender can broadcast one or more SSIDs, support both 2.4 GHz and 5 GHz bands and apply standard wireless security settings. Client devices connect directly to the FortiExtender's Wi-Fi network and route their traffic through the device's LTE or Ethernet WAN uplink, depending on configuration.
This mode can be used for remote or temporary locations without existing infrastructure or for mobile deployments such as vehicles or kiosks.
- **Station (STA) mode:** FortiExtender can connect to an external Wi-Fi network as a wireless client, using that wireless connection as a WAN uplink. This enables the FortiExtender to route traffic through an existing Wi-Fi infrastructure instead of—or in addition to—its LTE/5G or Ethernet interfaces. The FortiExtender scans for available wireless networks, connects to a selected SSID, and obtains an IP address via DHCP. The connected Wi-Fi uplink is then used as the primary or backup WAN interface, depending on failover settings.
- **AP and Station mode:** When configured as both Wi-Fi AP and Station, FortiExtender not only forms its own Wi-Fi network, but can also join an existing Wi-Fi network at the same time.

This section provides instructions on how to configure the wireless network settings of your FortiExtender device:

- [Set your geographical location on page 99](#)
- [Configure FortiExtender as a Wi-Fi AP on page 100](#)
- [Configure FortiExtender as a Wi-Fi station on page 108](#)

Set your geographical location

The maximum allowed transmitter power and permitted radio channels for WiFi networks vary, depending on the country or region of the world where the WiFi network is located. For this reason, it is important that you set your geographic location correctly before configuring the WiFi settings on your FortiExtender.

You can set the geographical location of your device using the FortiExtender software Console or GUI.

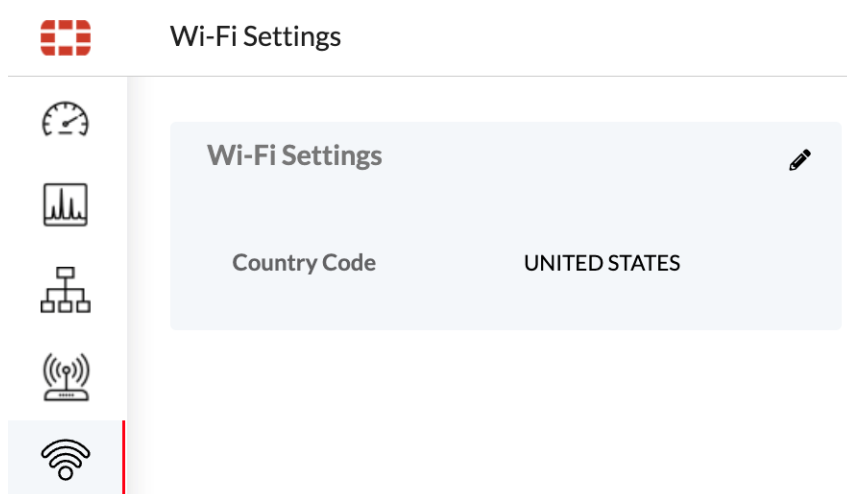
To set your geographical location - CLI:

```
FXW51GS224000030 (wifi-general) # show  
config wifi wifi-general
```

```
set country-code US
end
```

To set your geographical location - GUI:

1. From the main menu, select *WiFi > Settings*.
2. Select the country where your FortiExtender is to be deployed.



Configure FortiExtender as a Wi-Fi AP

You can configure your FortiExtender in AP mode for local client connectivity.

To configure FortiExtender in AP mode - CLI

1. From the FortiExtender CLI, create a virtual access point (VAP).

```
FXW51GS224000030 # config wifi
FXW51GS224000030 (wifi) # config vap
FXW51GS224000030 (vap) # edit FEX-WiFi-SSID
  set ssid FEX-WiFi-SSID
  set broadcast-ssid enable
  set dtim 1
  set rts-threshold 2347
  set max-clients 0
  set wlan-bridge yes
  set wlan-members
  config ap-security
    set security-mode WPA2-Personal
    set pmf
    set passphrase *****
```

```
end
next
```

2. Add the VAP to Radio profile.

```
FXW51GS224000030 # config wifi
FXW51GS224000030 (wifi) # config radio-profile
FXW51GS224000030 (radio-profile) # edit 5g-profile
  set band 5GHz
  set enable enable
  set role lan
  set operating-standards auto
  set beacon-interval 100
  set 80211d enable
  set max-clients 0
  set power-mode auto
  set channel 36 40 44 48 149 153 157 161
  set bandwidth auto
  set extension-channel auto
  set guard-interval auto
  set vap FEX-WiFi-SSID
next
```

3. Set VAP LAN interface IP address.

```
FXW51GS224000030 # config system interface
FXW51GS224000030 (interface) # edit FEX-WiFi-SSID
  set type wifi-lan
  set status up
  set mode static
  set ip 192.168.5.1/24
  set gateway 0.0.0.0
  set mtu-override disable
  set distance 51
  set vrrp-virtual-mac disable
  config vrrp
    set status disable
  end
  set allowaccess http https ping ssh telnet snmp
next
```

4. Configure LAN interface DHCP service.

```
FXW51GS224000030 # config system dhcpserver
FXW51GS224000030 (dhcpserver) # edit FEX-WiFi-SSID
  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 192.168.5.1
set netmask 255.255.255.0
set interface FEX-WiFi-SSID
set start-ip 192.168.5.2
set end-ip 192.168.5.254
set mtu 1500
set vci_match disable
set reserved-address disable
next
```

5. Configure LAN interface firewall. There are two methods of configuring.

- Option 1: Set srcaddr to allow all traffic.
 - i. From the Console, execute the following:

```
FXW51GS224000030 # config firewall policy
FXW51GS224000030 (policy) # edit all-nat
set srcintf any
set dstintf any
set srcaddr lan all
set dnat disable
set dstaddr all
set action accept
set status enable
set service ALL
set nat enable
next
```

- Option 2: Add additional firewall policy to allow traffic via the Wi-Fi LAN interface.
 - i. Add the IP address of the Wi-Fi LAN interface:

```
FXW51GS224000030 # config network address
FXW51GS224000030 (address) # edit FEX-WiFi-SSID
set type ipmask
set subnet 192.168.5.0/24
next
```

- ii. Then add the additional firewall policy for the Wi-Fi LAN interface:

```
FXW51GS224000030 # config firewall policy
FXW51GS224000030 (policy) # edit FEX-WiFi-SSID
set srcintf any
set dstintf any
set srcaddr FEX-WiFi-SSID
set dnat disable
set dstaddr all
set action accept
set status enable
set service ALL
set nat disable
next
```

6. Check Wi-Fi LAN interface status.

- a. From the Console, enter `get system interface` to display the status of the Wi-Fi LAN interface.
- b. Ensure that the LAN interface is in "up" status, as highlighted in the following:

Console

```
EVA22FTF23000010 # get system interface
== [ wan ]
name: wan          status: online/up/link down   type: physical      mac: 74:78:a6:8b:53:5d   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: 74:78:a6:8c:53:58   mode
: static          ip: 192.168.200.99/24   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
== [ lte1 ]
name: lte1         status: online/up/link up       type: lte            mac: aa:33:f6:a8:5b:08   mode
: dhcp            ip: 100.67.1.192/25     mtu: 1428
                  gateway: 100.67.1.193      dns: 198.224.174.135, 198.224.173.135
== [ lte2 ]
name: lte2         status: online/up/link down     type: lte            mac: aa:33:f6:a8:5b:08   mode
: dhcp            ip: 0.0.0.0/0          mtu: 1500
                  gateway: 0.0.0.0
== [ bsta0 ]
name: bsta0        status: online/up/link up       type: wifi-wan       mac: 74:78:a6:8b:53:61   mode
: dhcp            ip: 192.168.1.216/24    mtu: 1500
                  gateway: 192.168.1.1      dns: 192.168.1.1
== [ asta0 ]
name: asta0        status: offline/down/link down  type: wifi-wan       mac:                      mode
: dhcp            ip: 0.0.0.0/0          mtu: 0
                  gateway: 0.0.0.0
== [ FEX-WiFi-SSID ]
name: FEX-WiFi-SSID status: online/up/link up       type: wifi-lan       mac: 74:78:a6:8b:53:67   mode
: static          ip: 192.168.5.1/24     mtu: 1500
                  gateway: 0.0.0.0
EVA22FTF23000010 #
```

c.

Alternatively, you can check the status of the LAN interface using the *Networking* tab on the GUI, as shown in the following:

Networking

Interface VXLAN Switch Interface Aggregate Interface DNS DNS Servers Routing Address Service Target Multicast DHCP Relay

Status	Name	Members	Mode	Allow Access	Distance	Mac	IP	Gateway	Mtu	Ref	
🟢	fev-home-5g-1		static	http https ping snmp ssh telnet	51		192.168.5.1/24	enable	0	1	✎
🟢	fev-home-5g-2		static	http https ping snmp ssh telnet	51		192.168.6.1/24	enable	0	1	✎
🟢	fev-home-5g-3		static	http https ping snmp ssh telnet	51		192.168.7.1/24	enable	0	1	✎
🟢	fev-home-5g-4		static	http https ping snmp ssh telnet	51		192.168.8.1/24	enable	0	1	✎

To configure FortiExtender in AP mode - GUI

1. Create an SSID for the AP.

a. Go to *WiFi > SSIDs > Create SSID*.

ID	Broadcast SSID	SSID	Security Mode	Wlan Members
fev-home-5g-1	enable	fev-home-5g-1	WPA2-Personal	
fev-home-5g-2	enable	fev-home-5g-2	WPA2-Personal	
fev-home-5g-3	enable	fev-home-5g-3	WPA2-Personal	
fev-home-5g-4	enable	fev-home-5g-4	WPA2-Personal	

b. In the SSID dialog, make the desired configurations or selections, as shown in the following:

SSID [Cancel] [Save]

ID: fev-home-5g-1 Broadcast SSID: ☒ enable ☐ disable

SSID: fev-home-5g-1 Wlan Members: lan port2 port3 port4

Security Mode: WPA2-Personal PassPhrase:

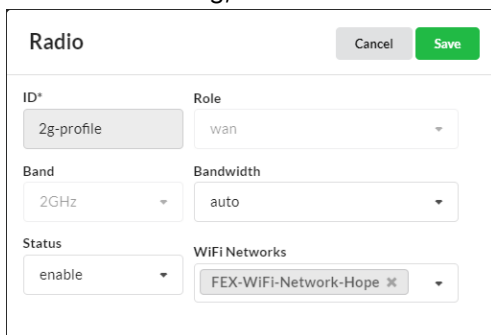
c. Click Save.

2. Associate the SSID with a Radio profile.

a. Go to *WiFi > Radio > Create Radio*.

ID	Role	Band	Bandwidth	Enable
5g-profile	lan	5GHz	20MHz	enable
2g-arlo	wan	2GHz	auto	enable

- b. In the *Radio* dialog, make the desired configurations or selections as shown in the following illustration.



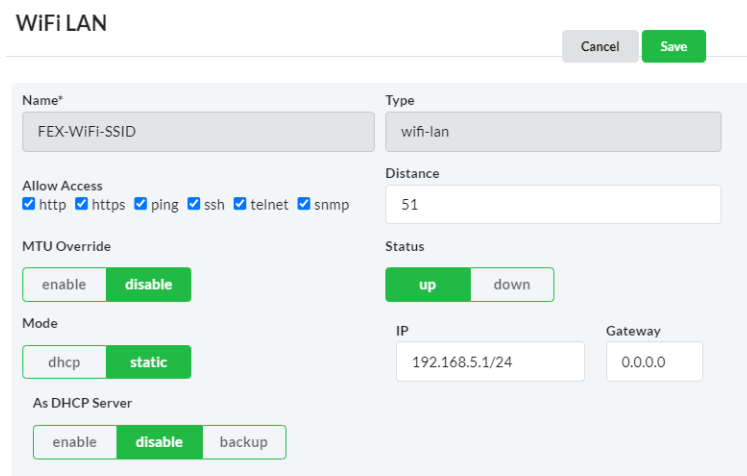
The **Radio** dialog box contains the following settings:

- ID***: 2g-profile
- Role**: wan
- Band**: 2GHz
- Bandwidth**: auto
- Status**: enable
- WiFi Networks**: FEX-WiFi-Network-Hope

- c. Click **Save**

3. Configure the VAP LAN interface IP address.

- a. Go to *WiFi > Networking > Edit*.
 b. In the *WiFi LAN* dialog, make the desired configurations or selection.



The **WiFi LAN** dialog box contains the following settings:

- Name***: FEX-WiFi-SSID
- Type**: wifi-lan
- Allow Access**: ☒ http ☒ https ☒ ping ☒ ssh ☒ telnet ☒ snmp
- Distance**: 51
- MTU Override**: enable (disabled)
- Status**: up (down)
- Mode**: dhcp (static)
- IP**: 192.168.5.1/24
- Gateway**: 0.0.0.0
- As DHCP Server**: enable (disabled) backup

- c. Click **OK**

4. Configure DHCP service for the Wi-Fi LAN interface.

- a. From the main menu, click *WiFi > WiFi Networks*.
 b. Select the Wi-Fi network, and then click *Edit*.

- c. In the *WiFi LAN* dialog, make the desired configurations or selections.

WiFi LAN Cancel Save

Name* FEX-WiFi-SSID	Type wifi-lan
Allow Access ☒ http ☒ https ☒ ping ☒ ssh ☒ telnet ☒ snmp	Distance 51
MTU Override enable disable	Status up down
Mode dhcp static	IP 192.168.5.1/24
As DHCP Server enable disable backup	Gateway 0.0.0.0
DHCP Server Config	
Name* FEX-WiFi-SSID	Default Gateway* 192.168.5.1
Net Mask* 255.255.255.0	Lease Time* 86400
Start IP* 192.168.5.2	End IP* 192.168.5.254
DNS Service default	Static Lease enable disable

- d. Click **Save**.

5. Configure a firewall policy for the VAP LAN interface. There are two methods of configuring.

- Option 1: Set the source address for all traffic
 - i. From the main menu, click *Firewall > Policy*.

Policy Policy Vip Traffic Shaper Traffic Shaping Policy 👤

Rules Reorder Create Rule 🗑️

Status	Name	Source Interface	Destination Int...	Source Address	Destination Ad...	Service	VIP	Action	NAT	DNAT	⚙️
🟢	all-nat	any	any	all	all	ALL	-	accept	enable	disable	🔧 🗑️
🟢	WiFi-vap-5g-1	any	any	all	all	ALL	-	accept	disable	disable	🔧 🗑️

Firewall

- ii. Select *Create Rule*.

- iii. In the *Rule* dialog, make the selections, and click **Save**.

Rule [Cancel] [Save]

Name* all-nat

Source Addresses* lan x all x

Destination Addresses* all x

Service* ALL x

Action accept deny

Status enable disable

NAT enable disable

DNAT enable disable

Source Interface* any

Destination Interface* any

- Option 2: Add additional Firewall Policy to allow traffic via the Wi-Fi LAN interface.
 - i. Add the IP address of the Wi-Fi LAN interface by selecting *Networking > Address > Create Address* from the main menu.

Address [Cancel] [Save]

Name* FEX-WiFi-SSID

Type ipmask iprange

Subnet 192.168.5.0/24

- ii. Add the additional Firewall policy for the Wi-Fi LAN interface.

Rule [Cancel] [Save]

Name* FEX-WiFi-SSID

Source Addresses* FEX-WiFi-SSID x

Destination Addresses* all x

Service* ALL x

Action accept deny

Status enable disable

NAT enable disable

DNAT enable disable

Source Interface* any

Destination Interface* any

6. Check Wi-Fi LAN interface status.

- a. Go to *Networking > Interface* and verify that the status is up.

If the Wi-Fi LAN interface status is UP, with DHCP service enabled and firewall correctly configured, you can use a laptop or mobile device access Wi-Fi service from your FortiExtender.

Configure FortiExtender as a Wi-Fi station

You can configure your FortiExtender as a Wi-Fi station using the FortiExtender CLI and GUI.

To configure FortiExtender as a Wi-Fi station from the CLI:

1. Configure the Wi-Fi network settings of the station.
 - a. From the FortiExtender GUI, open the CLI console and configure the following:

```
FXW51GS224000030 # config wifi
FXW51GS224000030 (wifi) # config <wifi-networks>
FXW51GS224000030 (wifi-networks) # edit FEX-WiFi-Network-Hope
    set ssid
    set security-mode
    set pmf
    set passphrase
next
```



The security-mode that you choose must be the same as the one used by your Wi-Fi service provider.

- b. Upon successful configuration of the Wi-Fi network, use the show command to check the configuration, which will generate the screen output like the following:

```

FXW51GS224000030 (FEX-WiFi-Network-Hope) <M> # show
edit FEX-WiFi-Network-Hope
  set ssid Hope
  set security-mode WPA2-Personal
  set pmf
  set passphrase *****
next

```

2. Add the Wi-Fi network to Radio profile.
 - a. From the FortiExtender Console, execute the following:

```

FXW51GS224000030 # config wifi
FXW51GS224000030 (wifi) # config radio-profile
FXW51GS224000030 (radio-profile) # edit 2g-profile
  set band 2GHz
  set enable enable
  set role wan
  set wifi-networks FEX-WiFi-Network-Hope
next

```



Because your FortiExtender is configured as a Wi-Fi station (in Step 1) which will be using services provided by an existing WAN, make sure that you set its role to wan.

3. Check the station WAN interface status.
 - a. After the Wi-Fi settings of the station has been successfully added to the Radio profile, use the `get system interface` command to view the wan interface, making sure that it is in "up" status, as highlighted in the following:

```

FVA22FTF23000010 # get system interface
== [ wan ]
name: wan          status: online/up/link down  type: physical      mac: 74:78:a6:8b:53:5d  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: 74:78:a6:8c:53:58  mode
: static          ip: 192.168.200.99/24    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
== [ lte1 ]
name: lte1         status: online/up/link up      type: lte             mac: aa:33:f6:a8:5b:08  mode
: dhcp            ip: 100.67.1.192/25      mtu: 1428
                  gateway: 100.67.1.193  dns: 198.224.174.135, 198.224.173.135
== [ lte2 ]
name: lte2         status: online/up/link down    type: lte             mac: aa:33:f6:a8:5b:08  mode
: dhcp            ip: 0.0.0.0/0          mtu: 1500
                  gateway: 0.0.0.0
== [ bsta0 ]
name: bsta0        status: online/up/link up      type: wifi-wan        mac: 74:78:a6:8b:53:61  mode
: dhcp            ip: 192.168.1.216/24     mtu: 1500
                  gateway: 192.168.1.1  dns: 192.168.1.1
== [ asta0 ]
name: asta0        status: offline/down/link down type: wifi-wan        mac:                   mode
: dhcp            ip: 0.0.0.0/0          mtu: 0
                  gateway: 0.0.0.0
== [ FEX-WiFi-SSID ]
name: FEX-WiFi-SSID status: online/up/link up      type: wifi-lan        mac: 74:78:a6:8b:53:67  mode
: static          ip: 0.0.0.0/0          mtu: 1500
                  gateway: 0.0.0.0
FVA22FTF23000010 #

```



Some FortiExtender models have two embedded Wi-Fi interfaces: `asta0` and `bsta0`. `asta0` is for the 5 GHz band, and `bsta0` is for the 2.4 GHz band.

You can also check the status of the WAN interface from the FortiExtender GUI under *Networking > Interface*:

Interface	Type	Mode	MAC	IP	Gateway	Mtu	Ref
port3	static	51	ac:71:2e:87:fe:2a	0.0.0.0	0.0.0.0	1500	
port2	static	51	ac:71:2e:87:fe:2b	0.0.0.0	0.0.0.0	1500	
wan	dhcp	5	ac:71:2e:87:fe:2d	0.0.0.0	0.0.0.0	1500	

Status	Name	Mode	Allow Access	Distance	Mac	IP	Gateway	Mtu	Ref
+	lte1	dhcp	ping telnet ssh http https snmp	15	ce:6a:1b:af:3f:08	10.33.134.226/30	0.0.0.0	1500	0

Status	Name	Mode	Allow Access	Distance	Mac	IP	Gateway	Mtu	Ref
+	bsta0	dhcp	ping ssh telnet http https snmp	15			enable	1000	0
+	asta0	dhcp	ping ssh telnet http https snmp	15			enable	1500	0

To configure FortiExtender as a Wi-Fi station - GUI:

1. Create a Wi-Fi network (SSID).

- From the FortiExtender GUI, go to *WiFi > WiFi Networks* and click *Create WiFi Networks*.

ID	Security Mode	SSID
2g-arlo	WPA2-Personal	ArloNetwork
Dream	WPA2-Personal	Dream
Hope	OPEN	Hope
2gOffice	WPA2-Personal	fev-office-2g-1

- In the *Add/Edit/Connect WiFi Network* dialog, create the Wi-Fi network with an SSID and password.

Add/ Edit/ Connect WiFi Network Cancel Save

Id: Dream Security Mode: WPA2-Personal

SSID: Dream PassPhrase:

Scan Results Scan AP

SSID	Channel	Security Mode	Rate	BSSID	RSSI	
fortinet	1	WPA2	54	e0:23:ff:d6:2c:40	-76	↑
2g	1	WPA2	54	ac:71:2e:87:fd:02	-45	↑
fortinet	6	WPA2	54	e0:23:ff:d6:2b:20	-88	↑
fev-office-2g-1	11	WPA2	54	ac:71:2e:87:fd:22	-19	↑
fev-office-2g-2	11	WPA2	54	ac:71:2e:87:fd:23	-18	↑

2. Add the Wi-Fi network to the Radio profile.
 - a. Go to *WiFi > Radio* and edit the radio you want to add the profile to.
 - b. In *WiFi Networks*, select the Wi-Fi network you created and then click *Save*.

Radio Cancel Save

ID*: 2g-profile Role: wan

Band: 2GHz Bandwidth: auto

Status: enable WiFi Networks: FEX-WiFi-Network-Hope ✕

3. Verify the Wi-Fi WAN interface status.
 - a. Go to *Networking > Interfaces* and verify that the Wi-Fi WAN interface status is up.

Networking Interface VXLAN Switch Interface Aggregate Interface DNS DNS Servers Routing Address Service Target Multicast

Status	Name	Mode	Allow Access	Distance	Mac	IP	Gateway	Mtu	Ref	
Physical Ports										
wan	dhcp			5	74:78:a6:8b:53:5d	0.0.0.0/0	0.0.0.0	1500	0	
L2E										
lte1	dhcp			15	aa:33:f6:a8:5b:08	100.67.1.192/25	100.67.1.193	1428	0	
lte2	dhcp			20	aa:33:f6:a8:5b:08	0.0.0.0/0	0.0.0.0	1500	0	
WiFi WAN										
bst0	dhcp			20	74:78:a6:8b:53:...	192.168.1.1	192.168.1.1	1500	0	
asta0	dhcp			20		0.0.0.0/0	0.0.0.0	0	0	



Some FortiExtender models have two embedded Wi-Fi interfaces: `asta0` and `bsta0`. `asta0` is for the 5 GHz band, and `bsta0` is for the 2.4 GHz band.

Authentication and security

The following topics provide instructions on configuring FortiExtender related authentication and security:

- [RADIUS authentication on page 113](#)
- [Wired 802.1X authentication on page 118](#)

RADIUS authentication

Using RADIUS authentication, users can use a remote account to log in to FortiExtender. RADIUS authentication uses the default port 1812 and requires configuring a RADIUS server. Once you configure the RADIUS server, apply it to a user group. FortiExtender will refer to the user group to authenticate the remote account.

To configure the FortiExtender to use RADIUS authentication - CLI

1. Configure the FortiExtender to access a RADIUS server.

```
config user radius
  edit example_radius
    set server {<IPv4 address> | <FQDN>}
    set secret <password>
    set auth-type auto
    set timeout 5
    set transport-protocol udp
    set nas-ip <IPv4 address>
  next
end
```

Parameter	Description
name	Name of the RADIUS server table.
server	Enter the primary RADIUS server FQDN or IP address.
secret	Pre-shared secret key used to access the primary RADIUS server. Character range is 1-128.
auth-type	Authentication protocols permitted for this RADIUS server. You can select the following options: • auto (default) • ms_chap_v2 • ms_chap • chap • pap

Parameter	Description
	If the authentication type is set to auto, FortiExtender uses the following protocols in sequence: PAP → MSCHAP_v2 → CHAP FortiExtender will only try the next protocol once it receives a RADIUS-reject message
timeout	Time in seconds to retry connecting to the RADIUS server. Default = 5.
transport-protocol	Transport protocol to be used. Default = udp.
nas-ip	IP address used for the FortiExtender to communicate with the RADIUS server. It is also used as the NAS-IP-Address and Called-Station-ID attributes.

2. Apply the RADIUS server table to a user group.

```
config user group
  edit group1
    set member [RADIUS server name1] [RADIUS server name2]
  next
end
```

Parameter	Description
name	Name of the FortiExtender user group.
member	Names of users and RADIUS server tables you want to add to the user group. You can apply multiple RADIUS server tables to a user group.

3. Enable remote access on FortiExtender.

```
config system admin
  edit remote1
    set accprofile super_admin
    set remote-auth enable
    set wildcard enable
    set password ENC *
    set remote-group group1
    set trusthost1
    set trusthost2
  next
end
```

Parameter	Description
remote-auth	Enable/disable authentication using a remote RADIUS server
wildcard	Enable/disable wildcard RADIUS authentication
remote-group	Enter the FortiExtender user group name you want to use for remote authentication.

Parameter	Description
	Note: If remote-auth is enabled, remote-group becomes mandatory. Otherwise remote-group is hidden. If remote-auth is enabled but wildcard is disabled, you must set a local password. If the RADIUS server is unreachable, FortiExtender uses the local password. For other situations, such as if FortiExtender receives a RADIUS reject message, the local password is omitted.
password	Admin user password Note: If wildcard is enabled, you cannot set a password.

If wildcard is enabled, the remote user can share the account and log in without needing to create multiple user accounts. That means, you can use the user and password pair stored in the remote server without needing to match the table name. See the following example:

```
config system admin
  edit "rs_admin"
    set remote-auth enable
    set accprofile "super_admin"
    set wildcard enable
    set remote-group "user"
  next
end
```



Only one wildcard remote account is allowed to exist under system admin.

4. Verify that the RADIUS server connection is successful.

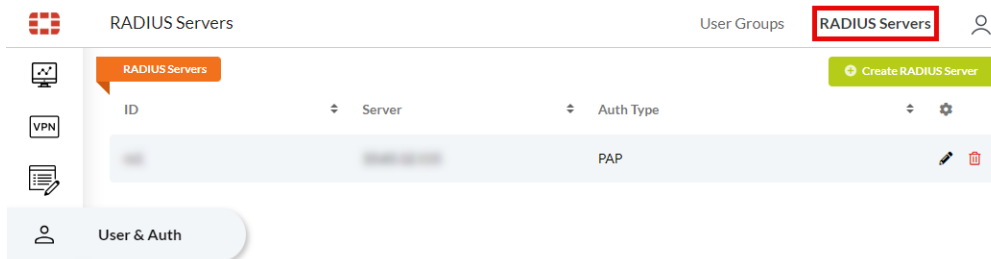
```
execute test authserver radius <server_name> <chap | pap | mschap | mschap2> <username>
<password>
  <server_name>:          radius server table name
  <auto | chap | pap | mschap | mschap2>:  choose a protocol
  <username>:             enter user name
  <password>:             enter password
```

```
execute test authserver radius-direct <IP> <port number (0 default port)> <udp> <secret> <pap
| chap | mschap | mschap2> <user> <password>
  <IP>:                  RADIUS server IP
  <port number (0 default port)>:  choose default port number
  <udp>:                  choose transport protocol
  <secret>:               authserver pre-key
  <auto | chap | pap | mschap | mschap2>:  choose a protocol
  <username>:             enter user name
  <password>:             enter password
```

To configure the FortiExtender to use RADIUS authentication - GUI

1. Configure the FortiExtender to access a RADIUS server.

- a. From the FortiExtender GUI, go to *User & Auth* and select the *RADIUS Servers* tab.



- b. Click *Create RADIUS Server* and enter your RADIUS server configurations.

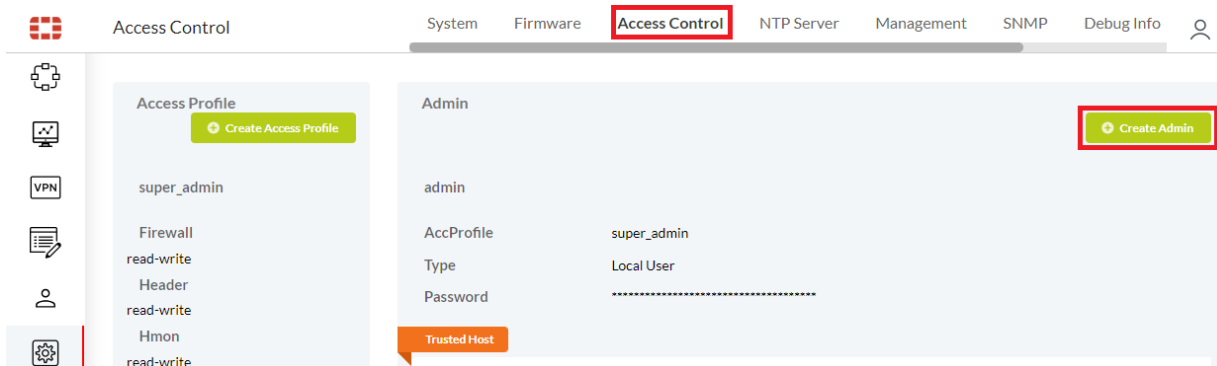
- c. When you are finished, click *Save*.

2. Apply the RADIUS server table to a user group.

- a. Go to *User & Auth* and select *Create User Group* or edit an existing user group.
 b. In the RADIUS Servers field, select the RADIUS server you previously configured.
 c. When you are finished, click *Save*.

3. Enable remote access on FortiExtender.

- a. Go to *Settings > Access Control* and select *Create Admin* or edit an existing Admin profile.



- b. In the Type field, select from the following options:

- *Local User*: Disable remote authentication.
- *Match a user on a remote server group*: Enable remote authentication, wildcard is disabled.

- *Match all users in a remote server group:* Remote authentication is enabled, wildcard is also enabled.
 - c. When you are finished, click **Save**.
4. Verify that the RADIUS server connection is successful.
- a. Go to **User & Auth > RADIUS Servers** and edit the RADIUS server you configured.
 - b. Click **Test Connectivity** and **Test User Credential** to verify the connection.

Add/ Edit/ Delete RADIUS Server Cancel Save

ID*	Server*
rs1	
Secret*	Auth Type
*****	Auto
NAS IP	
0.0.0.0	

Test Connectivity
Test User Credential

To check the DNS result:

To check whether the FQDN has been resolved, you can use the following commands from the FortiExtender:

- Use the `get dnsproxy cache dump` command.

```
# execute dnsproxy cache dump
name=fortinet.com, ttl=3600:3331:1531
    54.151.118.105 (ttl=3600) 54.177.212.176 (ttl=3600)
name=www.fortinet.com, ttl=13:0:1523
    54.189.112.223 (ttl=60)
name=www.fortinet.com, ttl=19:0:1523
    2600:1f14:b5a:da02:fd16:5d1:8062:ffdc (ttl=60)
CACHE num=3
```

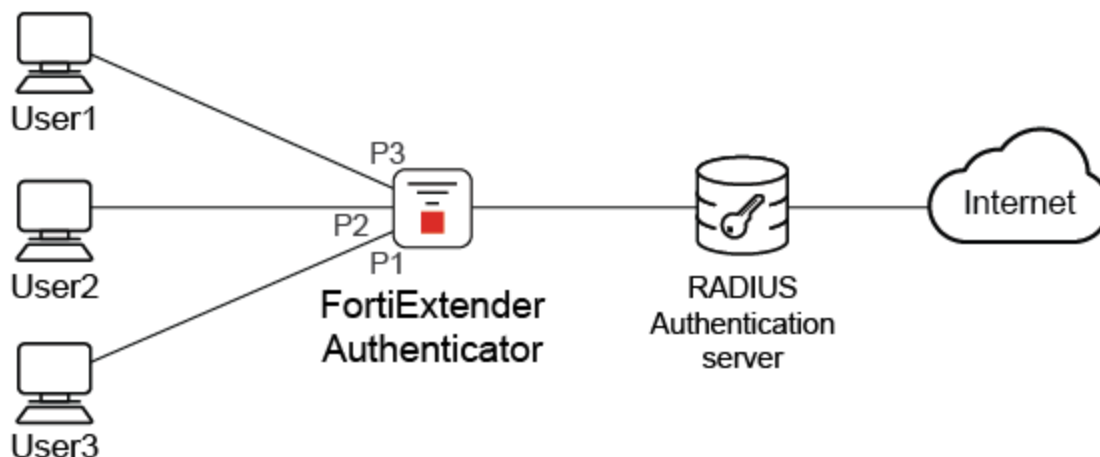
- Use the `get dnsproxy stats` command to check the statistics of DNS cache:

```
# get dnsproxy stats
retry_interval=500 query_timeout=2495
DNS latency info:
    server=208.91.112.53 latency=1 updated=33387
    server=208.91.112.52 latency=1 updated=34120
    server=172.16.100.100 latency=1 updated=33388
    server=172.16.100.80 latency=1 updated=5620
DNS_CACHE: alloc=5, hit=80936
DNS query: alloc=0
DNS UDP: req=82621 res=82621 fwd=1685 retrans=0 to=0
    cur=85 switched=1757500726 num_switched=16
DNS TCP: requests=0 responses=0 fwd=0 retransmit=0 timeout=0
```

Wired 802.1X authentication

To control network access, select FortiExtender models support MAC-based wired 802.1X port authentication. When enabled, only valid supplicants (end-user devices trying to connect to the 802.1X network) can access the FortiExtender.

Example topology



In the example topology, 802.1X authentication is enabled on FortiExtender port 1-3, meaning devices connected to those ports must be authenticated by the RADIUS authentication server to access the FortiExtender.

The process to enable 802.1X and the supplicant capacity varies depending on your FortiExtender platform type.

Platform	Models	Supplicant capacity	Configuration method
Mobility	FEV-211F-AM FEV-211F FEV-212F-AM FEV-212F	40 supplicants per FortiExtender.	GUI: Under the LAN Switch menu. CLI: Under config system lan-switch.
Branch	FBS-10F-WIFI FBS-20G FBS-20G-WIFI FER-511G FEXT-511G FEXT-511G-WIFI	8 supplicants for each port.	GUI: Under the Switch Interface menu. CLI: Under config system switch-interface.

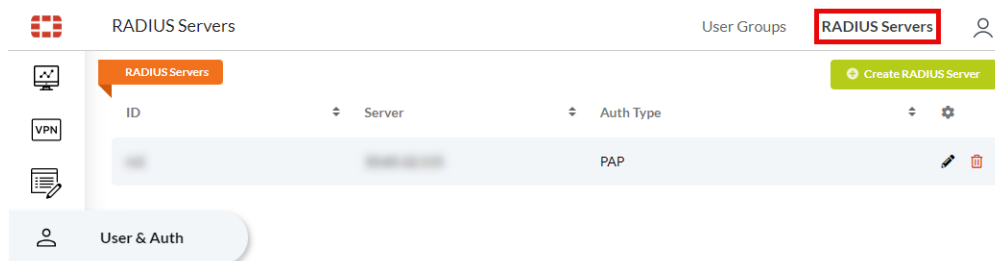
To enable 802.1X authentication on a FortiExtender, you must perform the following actions:

1. Configure a RADIUS User.
2. Configure a User Group.

3. Enable 802.1X authentication and assign the User Group to the appropriate interface depending on the FortiExtender platform type.
4. Optionally, disable 802.1X authentication on individual ports.

To configure a RADIUS User and User Group - GUI:

1. From the FortiExtender GUI, go to *User & Auth* and select the *RADIUS Servers* tab.



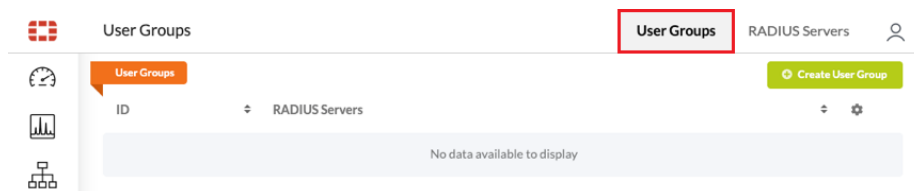
2. Click *Create RADIUS Server* and enter your RADIUS server information.

Add/ Edit/ Delete RADIUS Server Cancel Save

ID*	Server*
1	192.168.1.111
Secret*	Auth Type
*****	Auto
NAS IP	
0.0.0.0	

Test Connectivity Test User Credential

3. When you are finished, click *Save*.
4. From the FortiExtender GUI, go to *User & Auth* and select the *User Groups* tab.



5. Click *Create User Group* and enter your RADIUS server information.

Add/ Edit/ Delete User Group Cancel Save

ID
test
RADIUS Servers
1 x

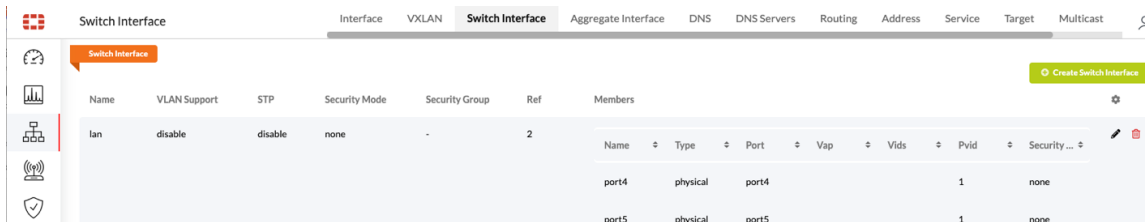


When you apply a user group to the wired 802.1X authentication, the RADIUS servers in this group are limited to four, with the first serving as the primary server and the rest as secondary servers.

- When you are finished, click **Save**.

To enable wired 802.1X authentication on a Branch platform FortiExtender - GUI:

- From the FortiExtender GUI, go to *Networking* and select the *Switch Interface* tab.



- Click *Create Switch Interface* or edit an existing one.
- Configure the following fields:
 - Enable *Security Mode* and then select *802.1X*.
 - In *User Group*, select the group you previously configured.

Switch-Interface

Cancel Save

Name*

lan

STP

enable disable

Security Mode

enable disable

802.1X

User Group

test

Create Member

Name	Type	Port	Vap	Vids	Pvid	Security M...	
port4	physical	port4			1	802.1X	
port5	physical	port5			1	802.1X	

- If you want to disable 802.1X authentication on a specific port, click *Edit* to edit that port and then disable *security-8021x-member*.

Members

Cancel

Save

Name*

port4

Type*

physical

Port*

port4

No results found.



Pvid

1

security-8021x-member

enable

disable

- When you are finished, click Save.

To enable wired 802.1X authentication on a Mobility platform FortiExtender - GUI:

- From the FortiExtender GUI, go to *Networking > Interface*.

Status	Name	Members	Mode	Allow Access	Distance	Mac	IP	Gateway	Mtu	Ref	
🔴	lan	port1 port2 port3 port4	static	ping telnet ssh http	50	74:78:a6:8c:53:c8	192.168.200.99/24	0.0.0.0	1500	2	✎

- In the *LAN Switch* section, click *Edit* and configure the following fields:
 - Enable *Security Mode* and then select *802.1X*.
 - In *User Group*, select the group you previously configured.

LAN Switch [Cancel] [Save]

Name* Type

Allow Access ☒ http ☐ https ☒ ping ☒ ssh ☒ telnet ☐ snmp Distance

Port Members Status STP

MTU Override MTU Mode

Security Mode User Group

security-8021x-member

IP Gateway As DHCP Server

VRRP Status

- c. If you want to disable 802.1X authentication on a specific port, remove that port from *security-8021x-member*.

3. When you are finished, click Save.

To configure a RADIUS User and RADIUS User Group - CLI:

1. Configure a RADIUS user.

```
config user radius
edit 1
set server 192.168.1.111
set secret *****
set auth-type auto
set timeout 5
set transport-protocol udp
set nas-ip 0.0.0.0
set nas-identifier
set port 1812
```

```
next
end
```

2. Create a RADIUS group.

```
config user group
edit test
set member 1
next
end
```

To enable wired 802.1X authentication on a Branch platform FortiExtender - CLI:

1. Under config system switch-interface, enable 802.1X and set a security group.

```
config system switch-interface
edit lan
set vlan-support disable
config member
edit port4
set type physical
set port port4
set vids
set pvid 1
set security-8021x-member-mode enable
next
edit port5
set type physical
set port port5
set vids
set pvid 1
set security-8021x-member-mode enable
next
end
set stp disable
set ts-mode disable
set wired-security-mode 802.1X
set wired-security-group test
next
end
```

2. If 802.1X authentication is not required on a specific port, you can disable it on that port. In this example, 802.1X is disabled on port4.

```
config system switch-interface
edit lan
config member
edit port4
set security-8021x-member-mode disable
end
next
end
```

To enable wired 802.1X authentication on a Mobility platform FortiExtender - CLI:

1. Under config system lan-switch, enable 802.1X and set a security group.

```
config system lan-switch
  set stp enable
  config ports
    edit port1
      set security-8021x-member-mode enable
    next
    edit port4
      set security-8021x-member-mode enable
    next
    edit port2
      set security-8021x-member-mode enable
    next
  end
  set wired-security-mode 802.1X
  set wired-security-group test
end
```

2. If 802.1X authentication is not required on a specific port, you can disable it on that port. In this example, 802.1X is disabled on port4.

```
config system lan-switch
  config ports
    edit port4
      set security-8021x-member-mode disable
    end
  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 125](#)
- [Perform link health check on page 126](#)
- [Configure health monitoring on page 128](#)

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: • rx_bytes—The number of bytes received. • tx_bytes—The number of bytes transmitted . • rx_packets—The number of packets received. • tx_packets—The number of packets transmitted. • rx_dropped—The number of incoming packets dropped. • tx_dropped—The number of outgoing packets dropped. • rx_bps—The number of bytes received per second. • tx_bps—The number of bytes transmitted per second. • rx_pps—The number of packets received per second. • tx_pps—The number of packets transmitted per second.

Example interface monitoring configuration:

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

```

        edit ifmon
            set internal 30
            set interface lte1
            set filter rx_bytes tx_bytes
        next
    end

```

You can monitor the aforementioned configuration using the following commands:

```

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

X04DA5918004433 # get hmon interface-monitoring ifmon
                rx_bytes tx_bytes rx_packets tx_
packets rx_dropped tx_dropped rx_bps tx_bps
rx_pps tx_pps
lte1: 22.20MB 11.50MB 83137 72281
0 0 101.85Kb 21.14Kb 15 14
0

```

Perform link health check

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

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

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

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.

Parameter	Descriptions
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 /.
*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 FortiEdge Cloud or FortiGate, respectively. One instance could involve data overage, another could be probing targets via ping or HTTP, and another could be checking link usability based on RTT or packet loss.

To configure interface monitoring:

```
config hmon
    config interface-monitoring
        edit < interface specific monitor name >
            set interval <interval size in seconds, default:30>
            set interface <interfaces to monitor: lte1, lte2>
            set filter <interested fields: rx_bytes,tx_bytes,rx_packets,tx_packets,rx_
                dropped,tx_dropped,rx_bps,tx_bps,rx_pps,tx_pps>
        next
    end
```

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

```
config hchk
    edit < health check type name >
        set protocol <ping|http|dns, default: ping>
        set interval <interval size in seconds, default :30>
        set probe-cnt <probes to be sent within an intervalm default:1>
        set probe-tm <probe timeout, default:2>
        set probe-target <target to be probed>
        set interface <uplink interfaces on which probe has to be sent>
        set src-iface <interface whose source IP is to be used>
        set filter <rtt |loss>
    next
end
```

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:

- [API handling of error messages on page 130](#)
- [Add trusted hosts on page 131](#)
- [Activate the default admin account on page 132](#)
- [Multiple static access controller addresses or FQDN on page 133](#)
- [Get system version on page 133](#)
- [Get user session status and force log-out on page 134](#)
- [Upgrade OS firmware on page 135](#)
- [Upgrade modem firmware on page 136](#)
- [SMS notification on page 137](#)
- [Remote diagnostics via SMS on page 137](#)
- [Configure the system syslog on page 138](#)
- [Support for SNMP \(read-only\) and traps on page 139](#)
- [Get MIB2 interface statistics via SNMP on page 142](#)
- [Access other devices via SSH on page 142](#)
- [Entity certificates in FortiExtender on page 143](#)
- [Automation stitching in digital I/O ports on page 147](#)
- [Configure Bluetooth Low Energy on page 155](#)

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/wEHn8yAs8Ap19pcBrYE6092jEI9OnDSY6Y/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. The password must be at least 12 characters long and a combination of uppercase letters, lowercase letters, numbers, and symbols (\~`!#\$%^&*_+= :; '<, > . / -).
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.
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/wEHn8yAs8Ap19pcBrYE6092jEI90nDSY6Y/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
        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 OS firmware from FortiGate or FortiEdge 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.

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

GUI

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

Upgrade modem firmware

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

TFTP

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

FTP

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

USB

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

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

GUI

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

SMS notification



SMS notification is only supported on the following FortiExtender models: FEX-201E, FEX-211E, FEX-201F, and FEX-212F.

Select FortiExtender models support Simple Message Service (SMS). This enables you to configure multiple mobile phone numbers on the FortiExtender to receive SMS alerts. Not all receivers can receive SMS notifications. Ensure the receiver sequence is set so the first receiver always receives SMS notifications.

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



SMS remote diagnostics is only supported on the following FortiExtender models: FEX-201E, FEX-211E, FEX-201F, and FEX-212F.

Select FortiExtender models support 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 1234567890
            set allowed-command-type factory-reset reboot get-system-status
        next
        edit user2
            set sender enable
            set phone-number 1234567890
            set allowed-command-type reboot get-modem-status get-extender-status
        next
    end
end
```

Configure the system syslog

Export system logs to remote syslog servers

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

Configure syslog database array

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

```
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
end
```

```
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.

Entity certificates in FortiExtender

FortiExtender supports entity certificates for HTTPS management access as well as importing third-party certificates through an SCEP server.

Certificate for HTTPS management access

FortiExtender supports specifying custom certificates for HTTPS management access. By default, the factory certificate is set to "Fortinet_Factory_Backup".

To import a custom certificate - CLI

From the FortiExtender console, enter the following command:

```
execute vpn certificate local import tftp <remote_file> <local_name> <ip> <passwd>
```

To import a custom certificate - GUI

1. From the FortiExtender GUI, go to *Settings* and select the *Certificate* tab.
2. Under *Entity Certificate*, click *Import New Certificate*.
3. Configure the *Name* and *Password* of the certificate and then upload the certificate.
4. When you are finished, click *Save*.

To configure custom certificates - CLI

```
config system global
  set admin-server-cert <cert_name>
end
```

Once you configure *admin-server-cert*, FortiExtender will use this certificate for remote HTTPS management on the admin interface. All new HTTPS management connections will be established using the configured certificate.



Existing HTTPS management connections will not be affected until you close and reopen the web browser.

Third-party certificates through an SCEP server

FortiExtender supports generating a Certificate Signing Request (CSR) and sending it to a Simple Certificate Enrollment Protocol (SCEP) server for signing. FortiExtender then adds the signed certificate to a local device. FortiExtender waits one minute to check the SCEP server for the CSR request status.

- If the certificate is approved, the CSR status changes from *pending* to *valid*.
- If the certificate is still pending approval after one minute, FortiExtender waits for twice the previous waiting time before checking again.
- If the waiting time exceeds 24 hours, the request is dropped. When a CSR is rejected or dropped, the status changes to *unknown*.

The user can regenerate the certificate using the same certificate name. However, once a certificate is created, the certificate details cannot be modified, even if the parameters are modified to trigger the execution command. Note that if the certificate is in a *pending* state, you cannot regenerate the certificate.



FortiExtender supports an *http* connection to the SCEP server.

To generate a CSR - GUI:

1. From the FortiExtender GUI, go to *Setting > Certificate*.

Name	Subject	Issuer	Expires	Status	Source	Ref	Comments
Fortinet_CA_Backup	C=US, ST=California, L=Sunnyvale, O=...	C=US, ST=California, L=Sunnyvale, O=...	2038-01-19 22:34:39 GMT	Valid	factory	0	
Fortinet_CA	C=US, ST=California, L=Sunnyvale, O=...	C=US, ST=California, L=Sunnyvale, O=...	2056-05-27 20:27:39 GMT	Valid	factory	0	
Fortinet_Sub_CA	C=US, ST=California, L=Sunnyvale, O=...	C=US, ST=California, L=Sunnyvale, O=...	2056-05-27 20:48:33 GMT	Valid	factory	0	

Name	Subject	Issuer	Expires	Status	Source	Ref	Comments
Fortinet_Factory_Backup	C=US, ST=California, L=Sunnyvale, O=...	C=US, ST=California, L=Sunnyvale, O=...	2038-01-19 03:14:07 GMT	Valid	factory	1	
Fortinet_Factory	C=US, ST=California, L=Sunnyvale, O=...	C=US, ST=California, L=Sunnyvale, O=...	2056-01-19 03:14:07 GMT	Valid	factory	0	

2. Under *Entity Certificate*, click *Generate CSR*.
3. Complete the CSR fields.

Generate Certificate Signing Request

Cancel

Save

Certificate Name*

ID Type

☒ host_ip
 ☐ domain_name
 ☐ id_email

IP*

Organization Unit

+

Organization

Locality(City)

State / Province

Country / Region

E-Mail

Subject Alternative Name

Key Size

☐ 1024 Bit
 ☐ 1536 Bit
 ☒ 2048 Bit
 ☐ 4096 Bit

CA Server URL*

Challenge Password

4. When you are finished, click Save.

To generate a CSR - CLI:

Certificates can be added through CLI execution commands, rather than through the FortiExtender configuration command.

```
# execute vpn certificate local generate rsa <cert_name> <key_size> <subject> <country name>
<state> <city> <org> <Units> <email> <subject_alter_name> <URL> <challenge>
```

Field	Description	Mandatory	Type	Value Range
cert_name	Specify the certificate name.	Yes	String	
key_size	Specify the key size.	Yes	Number	1024, 1536, 2048, 4096
subject	Specify the subject(Host-IP/Domain Name/E-Mail).	Yes	String	
country name	Specify the country name.	No	String	
state	Specify the state name.	No	String	
city	Specify the city name.	No	String	
org	Specify the organization name.	No	String	
Units	Specify the unit name. If there are multiple units, use ',' as a delimiter.	No	String	
email	Specify the email address.	No	String	

Field	Description	Mandatory	Type	Value Range
subject_ alter_name	Specify the subject alternative name.	No	String	
URL	Specify the URL.	Yes	String	
challenge	Specify the challenge password.	No	String	

To view all pending CSR - CLI:

View a list of pending CSRs.

```
# get vpn certificate local csr-pending-table
== [ CSR Pending Table ]
Name           Destination IP      Remaining Time to Send    Renew Case
Cert-test1     10.65.12.115       0 days 00:00:56         No
Cert-test2     10.65.12.115       0 days 00:01:50         Yes
```

Field	Description
Name	The pending certificate name.
Destination IP	SCEP server IP address.
Remaining Time to Send	Countdown Timer to download certificate from SCEP server.
Renew Case	If this certificate is original request, it shows No. If the certificate is renew request, it shows Yes.

To regenerate a CSR - CLI:

You can use the same certificate name to regenerate a previous CSR. Note that the parameters cannot be modified when regenerating.

```
# execute vpn certificate local generate rsa test1 1024 cert US CA Sunnyvale Fortinet
102,203,303 test@fortinet.com null http://192.168.100.99/app/cert/scep/ fortinet
Are you sure to re-generate the certificate?
Do you want to continue? (y/n)y
```

To delete a certificate - GUI:

1. From the FortiExtender GUI, go to *Setting > Certificate*.
2. Under *Entity Certificate*, locate the certificate you want to delete and click *Delete*.

To delete a certificate - CLI:

```
config vpn certificate local
  delete <name>
end
```

Automation stitching in digital I/O ports

FortiVehicle models support Automation Stitches for digital I/O (DIO) port functions.

Automation stitches automate the activities between the different component in the FortiExtender. An automation stitch consists of two parts: the *trigger* and the *action*.

- The *trigger* is the condition or event on the FortiExtender that activates the action.
- The *action* is what the FortiExtender does in response to the trigger.

Creating automation stitches

To create an automation stitch, you must select a trigger event and a response action.

To configure an automation stitch from the FortiExtender - GUI:

1. From the FortiExtender GUI, go to *Setting > Automation*.

The FortiExtender Automation tab loads.

The screenshot shows the FortiExtender GUI with the 'Automation' tab selected. The interface is divided into three main sections: Triggers, Actions, and Stitches. Each section has a 'Create' button and a table of existing items.

Triggers

Name	Description	Trigger Type	Event Type	Digital IO Alert ID
digital-io-low	digital io in low	event-based	digital-io-alert	alert-in-low

Actions

Name	Description	Action Type	Digital IO Action ID	Modem ID	Minimum Interval
digital-io-low	digital out low	digital-output	action-out-low	-	0

Stitches

Name	Description	Status	Trigger	Actions								
digital-io-st-low	digital st low	disable	digital-io-low	<table border="1"> <thead> <tr> <th>Name</th> <th>Action</th> <th>Delay</th> <th>Required</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>digital-io-low</td> <td>0</td> <td>enable</td> </tr> </tbody> </table>	Name	Action	Delay	Required	1	digital-io-low	0	enable
Name	Action	Delay	Required									
1	digital-io-low	0	enable									

2. Automation stitches, actions, and triggers are configured in the separate dialogs. Click on each dialog to create either a trigger, action, or automation stitch.

- a. Click *Create Trigger* to create a trigger. To modify an existing trigger, click the edit icon.

Trigger

Cancel Save

Name*

Description

Trigger Type

event-based ▾

Event Type*

digital-io-alert ▾

Digital IO Alert ID

alert-in-high ▾

- i. Complete the following fields:

Trigger fields	Description
<i>Name</i>	Enter a name for the trigger.
<i>Description</i>	Describe the automation trigger.
<i>Trigger Type</i>	Select a trigger type: event-based: Set to trigger at specific system events or conditions, for example a digital I/O alert.
<i>Event Type</i>	If the <i>Trigger Type</i> is set to <i>event-based</i> , you must select the type of event to trigger the automation stitch action. digital-io-alert: A digital I/O alert is detected.
<i>Digital IO Alert ID</i>	If <i>Event Type</i> is set to <i>digital-io-alert</i> , you must select a digital I/O alert ID.

- ii. When you are finished, click *Save*.
- b. Click *Create Action* to create an action. To modify an existing action, click the edit icon.

Action

Cancel Save

Name*

Description

Action Type*

sim-switch ▾

Modem ID*

modem2 ▾

Minimum Interval

- i. Complete the following fields:

Action fields	Description
<i>Name</i>	Enter a name for the automation action.
<i>Description</i>	Describe the automation action.
<i>Action Type</i>	Select the type of action to perform: - digital-output: Output a digital signal via the digital out pin. - sim-switch: Change the currently active SIM card to an alternate one, enabling the device to connect through a different network or carrier as needed. - modem-reset: Perform a reboot or reset operation on the modem to reinitialize its settings and restore connectivity in case of issues.
<i>Digital IO Action ID</i>	If <i>Action Type</i> is set to <i>digital-output</i> , you must configure a digital I/O action ID
<i>Modem ID</i>	If <i>Action Type</i> is set to <i>sim-switch</i> or <i>modem-reset</i> , you must configure a modem ID.
<i>Minimum Interval</i>	Limit performing this action to no more than once in this interval (in seconds).

- ii. When you are finished, click **Save**.
- c. Click **Create Stitch** to create a stitch. To modify an existing stitch, click the edit icon.

Stitch

Cancel Save

Name*

Description

Status

Trigger*

stitch1

stitch test1

enable disable

trigger1

Create Action

Name

Action

Delay

Required

1

action1

2

enable

- i. Complete the following fields:

Stitch fields	Description
<i>Name</i>	Enter a name for the automation stitch.
<i>Description</i>	Describe the automation stitch.
<i>Status</i>	Enable or disable the automation stitch.
<i>Trigger</i>	Select the name of the trigger for this automation stitch.
<i>Create Action</i>	Click to create actions.
<i>Name</i>	Enter a name for the stitch action.
<i>Action</i>	Select the name of the action configuration for this automation stitch.
<i>Delay</i>	Set the delay before execution (in seconds)
<i>Required</i>	Select if this action is required or not in the action chain. • enable • disable

- ii. When you are finished, click Save.

To configure an automation stitch from the FortiExtender - CLI:

1. Configure a trigger.

There are two triggers in this example, one trigger for detecting the digital IO alert "alert-in-low" and one trigger for detecting the digital IO alert "alert-in-high". You can create or edit own digital IO alert (see [Digital I/O port functions on page 152](#)).

```
config system automation trigger
  edit digital-io-low
    set description digital io in low
    set trigger-type event-based
    set event-type digital-io-alert
    set digital-io-alert-id alert-in-low
  next
  edit trigger1
    set description trigger test1
    set trigger-type event-based
    set event-type digital-io-alert
    set digital-io-alert-id alert-in-high
  next
end
```

2. Configure an action.

There are three actions in this example:

- "digital-io-low" outputs a digital signal.
- "action1" changes the currently active SIM card to another one on modem2.
- "reset-modem" resets modem1.

```
config system automation action
  edit digital-io-low
    set description digital out low
    set action-type digital-output
    set digital-io-action-id action-out-low
    set minimum-interval 0
  next
  edit action1
    set description action test1
    set action-type sim-switch
    set modem-id modem2
    set minimum-interval 3
  next
  edit reset-modem
    set description reset modem
    set action-type modem-reset
    set modem-id modem1
    set minimum-interval 0
  next
end
```

3. Configure a stitch.

There are two twitches in this example. For the first automation stitch, when the event "digital-io-low" is detected, the action "digital-io-low" will be performed immediately. For the second automation stitch, when the event "trigger1" is detected, the action "action1" will be performed two seconds later.

```
config system automation stitch
  edit digital-io-st-low
    set description digital st low
    set status disable
    set trigger digital-io-low
    config actions
      edit 1
        set action digital-io-low
        set delay 0
        set required enable
      next
    end
  next
  edit stitch1
    set description stitch test1
    set status enable
    set trigger trigger1
    config actions
      edit 1
        set action action1
        set delay 2
        set required enable
      next
    end
  next
end
```

Digital I/O port functions

FortiVehicle models have five digital I/O (DIO) ports that can function as either input or output ports for handling analog or digital signals. These ports can be used to collect data, detect events, and subsequently generate reports or trigger actions based on the collected information.

You can enable this feature by configuring input ports as *alerts* and output ports as *actions*.

- Digital I/O alerts can be referenced by the automation trigger `digital-io-alert`.

```
config system automation trigger
edit digital-io-low
set description digital io in low
set trigger-type event-based
set event-type digital-io-alert
set digital-io-alert-id alert-in-low
next
end
```

- Digital I/O actions can be referenced by the automation action `digital-output`.

```
config system automation action
edit digital-io-low
set description digital out low
set action-type digital-output
set digital-io-action-id action-out-low
set minimum-interval 0
next
end
```

To configure digital I/O port functions - GUI:

- From the FortiExtender GUI, go to *Setting > Digital I/O*.

The FortiExtender Digital I/O tab loads.

The screenshot displays the FortiExtender Digital I/O configuration page. The top navigation bar includes tabs for Digital I/O, Automation, and others. The main content area is divided into two sections: Alerts and Actions.

Alerts Section:

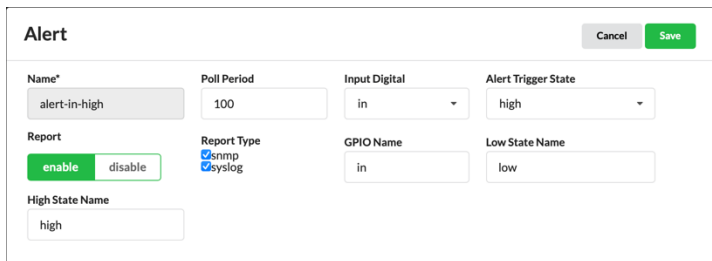
Name	Poll Period	Input Digital	Alert Trigger Sta...	Report	Report Type	GPIO Name	Low State Name	High State Name	
alert-in-high	100	in	high	enable	snmp, syslog	in	low	high	[Edit] [Delete]
alert-in-low	100	in	low	enable	snmp, syslog	in-1	low-1	high-1	[Edit] [Delete]

Actions Section:

Name	Output Digital	Output Digital State	
action-out-high	out	high	[Edit] [Delete]
action-out-low	out	low	[Edit] [Delete]

2. Digital I/O alerts and actions are configured in the separate dialogs. Click on each dialog to create either an alert or action.

- a. Click *Create Alert* to create an alert. To modify an existing alert, click the edit icon.



The **Alert** dialog box contains the following fields:

- Name***: alert-in-high
- Poll Period**: 100
- Input Digital**: in
- Alert Trigger State**: high
- Report**: enable (selected), disable
- Report Type**: snmp, syslog (selected)
- GPIO Name**: in
- Low State Name**: low
- High State Name**: high

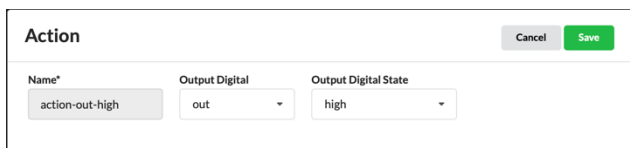
Buttons: Cancel, Save

- i. Complete the following fields:

Stitch fields	Description
<i>Name</i>	Enter a name for the digital I/O alert.
<i>Poll Period</i>	The interval between general-purpose I/O (GPIO) status checks, in milliseconds.
<i>Input Digital</i>	Select a digital name
<i>Alert Trigger State</i>	Select the changing state that will trigger the GPIO alert report and action: - no-alert: No alert. - high: The state is changed from low to high. - low: The state is changed from high to low. - both: The state is changed.
<i>Report</i>	Enable or disable reporting.
<i>Report Type</i>	Select a report type.
<i>GPIO Name</i>	The GPIO name that will be generated in the report log.
<i>Low State Name</i>	The low state name that will be generated in the report log.
<i>High State Name</i>	The high state name that will be generated in the report log.

- ii. When you are finished, click *Save*.

- b. Click *Create Action* to create an action. To modify an existing action, click the edit icon.



The **Action** dialog box contains the following fields:

- Name***: action-out-high
- Output Digital**: out
- Output Digital State**: high

Buttons: Cancel, Save

- i. Complete the following fields:

Stitch fields	Description
<i>Name</i>	Enter a name for the digital I/O action.
<i>Output Digital</i>	Select the name of the digital that will run the alert action on.
<i>Output Digital State</i>	Select the digital state that will be set when the alert is detected: - high: Change the state to high. - low: Change the state to low.

- ii. When you are finished, click **Save**.

To configure the digital I/O ports - CLI:

1. Configure a digital I/O port alert:

There are two alerts in this example. One alert is configured so that when the "digital io in" state changes from "low" to "high", an alert event will be reported. The other alert is configured so that when the "digital io in" state changes from "high" to "low", an alert event will be reported.

```
config system digital-io alert
edit alert-in-high
set poll-period 100
set input-digital in
set alert-trigger-state high
set report enable
set report-type snmp syslog
set gpio-name in
set low-state-name low
set high-state-name high
next
edit alert-in-low
set poll-period 100
set input-digital in
set alert-trigger-state low
set report enable
set report-type snmp syslog
set gpio-name in-1
set low-state-name low-1
set high-state-name high-1
next
end
```

2. Configure a digital I/O action:

There are two digital I/O actions in this example. One action sets the digital "out" port state to "high" when an alert is detected, and one alert sets the digital "out" port state to "low".

```
config system digital-io action
edit action-out-high
set output-digital out
set output-digital-state high
next
```

```
edit action-out-low
    set output-digital out
    set output-digital-state low
next
end
```

Configure Bluetooth Low Energy

Some FortiExtender models have a Bluetooth Low Energy (BLE) 5.0 interface that operates in the 2.4 GHz band. By default, the BLE interface is turned off to prevent unauthorized access. When BLE is active, any nearby device can attempt to connect.

For specific instructions on enabling BLE, refer to the QuickStart Guide that came with your FortiExtender. In general, you can enable Bluetooth pairing mode by holding the Bluetooth button for more than 3 seconds. This opens a brief *pairing window*, during which the device's BLE radio is active and discoverable. Once in pairing mode, the device will "listen" for connection attempts for 90 seconds. If no pairing is completed during that interval, the BLE window closes and the LED turns off.



Fortinet recommends always securing your FortiExtender by setting a strong admin password and disabling Bluetooth when not in use. Only press the Bluetooth button when you are ready to pair a device. Do not leave a FortiExtender in pairing mode unattended.

For additional security, you can disable the Bluetooth button so that pressing it will not trigger BLE function.

To disable the FortiExtender BLE button - GUI:

1. From the FortiExtender GUI, go to *Settings > System* and click *Edit*.
2. In the *Bluetooth* dropdown list, select *disable*.

System Settings

Cancel

Save

Host Name

Modem Firmware Server

fortiextender-firmware.forticloud.com

OS Firmware Server

fortiextender-firmware.forticloud.com

Admin Server Certificate

Fortinet_Factory_Backup ▼

Time Zone

(GMT) Greenwich Mean Time ▼

System Setting

Ike Port*

500

Admin Setting

HTTP Port*

80

HTTPS Port*

443

SSH Port*

22

Telnet Port*

23

Idle Timeout (mins)*

300

Bluetooth

enable ▼

3. When you are finished, click Save.

To disable the FortiExtender BLE button - CLI:

```
config system bluetooth
set status disable
end
```

Troubleshooting, diagnostics, and debugging

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

- [Troubleshooting on page 157](#)
- [Status, diagnostics, and debugging commands on page 158](#)
- [Diagnose from Telnet on page 158](#)
- [Collect complete diagnostics information on page 159](#)

Troubleshooting

Below are some common error situations with their suggested solutions.

Can't manage the FortiExtender from FortiEdge Cloud

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

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

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>
```

Configure LTE settings

This section discusses LTE configurations. It covers the following topics:

- [Add a new carrier profile on page 160](#)
- [Add a new operator/carrier on page 160](#)
- [Activate a SIM card on page 163](#)
- [Configure start session timeout on page 163](#)
- [Check the recorded SIM card IMSI number on page 164](#)
- [Delete the recorded SIM card IMSI number on page 165](#)
- [Set the default SIM on page 165](#)
- [Enable SIM-switch on page 166](#)
- [Dual modems on page 168](#)
- [Unlock SIM pin on page 169](#)

Add a new carrier profile

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

```
config lte carrier
show
end
```

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

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

Add a new operator/carrier

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

```
get lte carrier <MCC> <MNC>
```

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

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



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

To create a data plan - CLI:

You can configure a data plan with the following CLI parameters:

```
config lte plan
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 an LTE interface has breached its data usage limit (overage), 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
-

Parameter	Description
modem	Choose “modem1”, “modem2”, or “all”.
type	Choose the way for the modem to select the SIM card: • 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). • generic— Compatible with any SIM. Assigned if no other data plan matches the chosen SIM.
iccid	The serial number of the SIM, mandatory for “set type by-iccid”.
carrier	The SIM card carrier, mandatory for “set type by-carrier”.
slot	The SIM card slot, mandatory for “set type by-slot”
apn	The APN of the SIM card.
auth-type	The Authorization mode.
username	The username.
password	The password.
pdn	The Packet Data Network (PDN) IP address family.
signal-threshold	The signal-strength threshold beyond which SIM switch will occur. Note: Enter an integer value from <50> to <100> (default = <100>).
signal-period	The length of time (from 600 to 18000 seconds) for SIM switch to occur when signal strength remains below the set signal threshold for more than half of the set period.
capacity	The data capacity per month (from 0 to 102400000 MB).
monthly-fee	The monthly fee for the data plan (from 0 to 10000000).
billing-date	The billing date of the month.
overage	Whether the SIM card can continue to use data once the allotted amount is used up.
preferred-subnet	DHCP subnet.
private-network	When enabled, FortiExtender allows the flow of non-NATed IP traffic on to an LTE interface.

To create a data plan - GUI:

1. From the FortiExtender GUI, go to *LTE > Plan > Create Plan*.
2. Enter your desired plan configurations.
3. When you are finished, click *Save*.

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
    config advanced-settings
        set sim-activation-delay 300
    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 165](#)
- [Set the default SIM by low cost on page 165](#)
- [Set the default SIM by SIM slot on page 166](#)

Set the default SIM by preferred carrier

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

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

Set the default SIM by low cost

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

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

```
config lte setting
  config modem1
    set default-sim by-cost
  end
next
end
```

Set the default SIM by SIM slot

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

```
config lte setting
  config modem1
    set default-sim sim1|sim2
  end
next
end
```

Enable SIM-switch

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

Parameter	Description
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.

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 169](#)
- [Dual modems in NAT mode on page 169](#)

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 lte1-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 38](#) for Virtual-WAN interface and [System routing on page 60](#) for policy-based route configurations.

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.



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.