FORTINET

Admin Guide

FortiExtender (Standalone) 7.6.4

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

Feb 4, 2026
FortiExtender (Standalone) 7.6.4 Admin Guide

TABLE OF CONTENTS

Change Log **8**
Introduction **9**
Getting started **10**
Management and Operation mode 11
Check current management mode 12
IP pass-through mode 13
NAT mode 14
Essential LTE settings 14
Activate SIM card 15
Configure PIN 15
Create a Data Plan 16
Essential networking configurations 16
LAN interface 17
LAN addressing 17
DHCP server 18
Health checks 19
VWAN interface 20
Essential wireless configurations 22
Country Code 22
Wireless WAN networks 23
Virtual Access Points and SSID 24
Radio profiles 25
IPsec VPN tunnels 26
Main LTE/5G features **29**
Cellular capabilities 29
Supported wireless carriers 30
SIM mapping 31
Add a data plan and APN 31
Global SIM with roaming on 32
SIM-switch 32
SIM switch-back 33
Configure SIM-switch based on link health 34
Get modem status 35
Stopping data traffic on overaged LTE interface 36
OBM management 36
Multiple Packet Data Network (PDN) 37
Interface management **38**
Interface configuration guideline 39
Physical interface(s) 39
LTE interface 40
Tunnel interface 40
Virtual-WAN interface 40
Access allowance 41

Get interface status 42
Configure LAN switch 42
Configure switch interface 44
Configure VXLAN interface 45
SFP DSL support 46
Aggregate interface support with load-balancing 46
Configure a private network 48
Configure Virtual-WAN interface 48
Dynamic Frequency Selection channels 51
IPv6 53
Configuring IPv6 53
Configure IPv6 SLAAC on an interface 58
Configure captive portals 61
Example captive portal configuration 63
DHCP configurations 67
Configure DHCP server 67
Configure DHCP relay 69
DHCP relay over VPN 70
DHCP client optimization 70
Network utilities 71
Address 71
Service 71
Target 71
System routing 73
Configure static routing 73
IPv4 static routing 73
IPv6 static routing 74
Configure Policy Based Routing 74
Router target 75
Router policy 75
View routing configurations 76
Move PBR rules 77
Configure dynamic routing — OSPF 78
Configure OSPF from Console (CLI) 78
Configure OSPF redistribution 81
Verify OSPF configurations 83
Configure OSPF GUI 84
Complete OSPF configuration code example 85
Configure multicast routing 87
Firewall 88
Configure address/subnet 88
IPv4 88
IPv6 88
Configure protocol/port range 89
Configure firewall policies 90

Move firewall policies ... 92
Destination Network Address Translation (DNAT) ... 93
VPN ... 94
Configure VPN ... 94
Configure phase-1 parameters ... 95
Configure phase-2 parameters ... 96
Configure firewall policies ... 99
Check VPN tunnel status ... 100
IPsec VPN support for third-party certificates ... 101
Use third-party certificates for IKE authentication ... 101
DNS Service ... 103
Set up DNS database ... 104
Check DNS statistics ... 106
Dump the DNS cache ... 106
Clear the DNS cache ... 107
Dump the DNS database ... 107
Configuring FortiExtender as a DNS proxy server ... 107
DNS Filtering ... 109
SD-WAN ... 115
Configure an SD-WAN ... 115
Check SD-WAN health ... 116
Define an SD-WAN member ... 118
Wi-Fi Settings ... 120
Set your geographical location ... 120
Configure FortiExtender as a Wi-Fi AP ... 121
Configure FortiExtender Wi-Fi APs as members of switch interface ... 129
Configure FortiExtender as a Wi-Fi station ... 131
Authentication and security ... 136
RADIUS authentication ... 136
Wired 802.1X authentication ... 140
Health monitoring ... 147
Monitor interface status ... 147
Perform link health check ... 148
Configure health monitoring ... 150
Logs ... 152
System management ... 153
Add trusted hosts ... 153
Activate the default admin account ... 154
Configuration backups and restore ... 155
Multiple static access controller addresses or FQDN ... 157
Get user session status and force log-out ... 158
Upgrade OS firmware ... 159
TFTP ... 159
FTP ... 159

USB 159
FortiEdge Cloud 160
GUI 160
Upgrade modem firmware 160
TFTP 160
FTP 160
USB 160
FortiEdge Cloud 161
GUI 161
SMS notification 161
Remote diagnostics via SMS 162
Configure the system syslog 163
Export system logs to remote syslog servers 163
Configure syslog database array 163
Support for SNMP (read-only) and traps 164
Typical SNMP commands 164
Sample SNMP commands 165
Executable SNMP commands 166
Get MIB2 interface statistics via SNMP 166
Access other devices via SSH 167
Entity certificates in FortiExtender 167
Certificate for HTTPS management access 167
Third-party certificates through an SCEP server 168
Automation stitching in digital I/O ports 171
Creating automation stitches 171
Digital I/O port functions 177
Configure Bluetooth Low Energy 180
LTE settings 182
Add a new carrier profile 182
Add a new operator/carrier 182
Create a data plan 183
Activate a SIM or eSIM 185
Activate an eSIM 185
Configure start session timeout 188
Managing the SIM card IMSI number 189
Set the default SIM 189
Set the default SIM by preferred carrier 190
Set the default SIM by low cost 190
Set the default SIM by SIM slot 190
Enable SIM-switch 191
Dual modems 193
Dual-modem in IP pass-through mode 194
Dual modems in NAT mode 194
Unlock SIM pin 194

FortiExtender API **196**
Troubleshooting, diagnostics, and debugging **197**
Diagnose from Telnet 197
Collect complete diagnostics information 197

Change Log

Date	Change Description
2026-02-04	Updated Configure Virtual-WAN interface on page 48.
2026-01-15	Updated Configure Virtual-WAN interface on page 48 and Check SD-WAN health on page 116.
2025-11-18	Updated Wi-Fi Settings on page 120 and Configure FortiExtender Wi-Fi APs as members of switch interface on page 129.
2025-11-05	Updated VPN on page 94.
2025-09-23	Updated Activate a SIM or eSIM on page 185 and Enable SIM-switch on page 191.
2025-09-22	Initial release.

Introduction

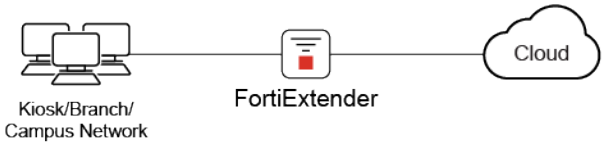
FortiExtender is a plug-and-play customer premises equipment (CPE) device. As a 3G/4G LTE and 5G wireless WAN extender, FortiExtender can provide a primary WAN link for retail POS, ATM, and kiosk systems, or a failover WAN link to your primary Internet connection to ensure business continuity. You can 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.



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

- Management and Operation mode on page 11
- Essential LTE settings on page 14
- Essential networking configurations on page 16
- Essential wireless configurations on page 22
- IPsec VPN tunnels on page 26

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 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.

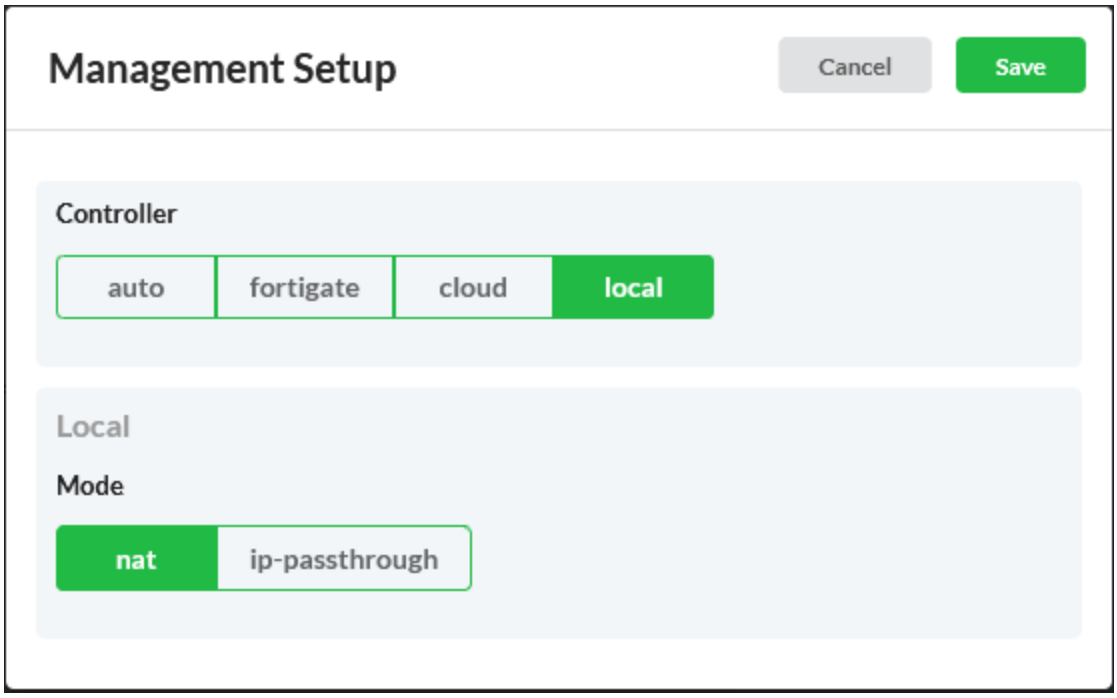
- **IP pass-through mode**: FortiExtender distributes the WAN IP address provided by the NSP to the device behind it. See IP pass-through mode on page 13
- **NAT mode**: In this mode, the LAN port on the FortiExtender can support multiple devices (e.g., PCs, printers, etc.). The FortiExtender works as a gateway of the subnet behind it to forward traffic between the LAN and the LTE WAN. See NAT mode on page 14.

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*.



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 : CWWS_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 38
- DHCP configurations on page 67
- System routing on page 73
- Configure Policy Based Routing on page 74
- Firewall on page 88
- VPN on page 94
- SD-WAN on page 115
- Health monitoring on page 147

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 15
- Configure PIN on page 15
- Create a Data Plan on page 16

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.

eSIM support is available on select FortiExtender models and can only be activated via the FortiExtender GUI. For more information, see Activate a SIM or eSIM on page 185.

Configure PIN

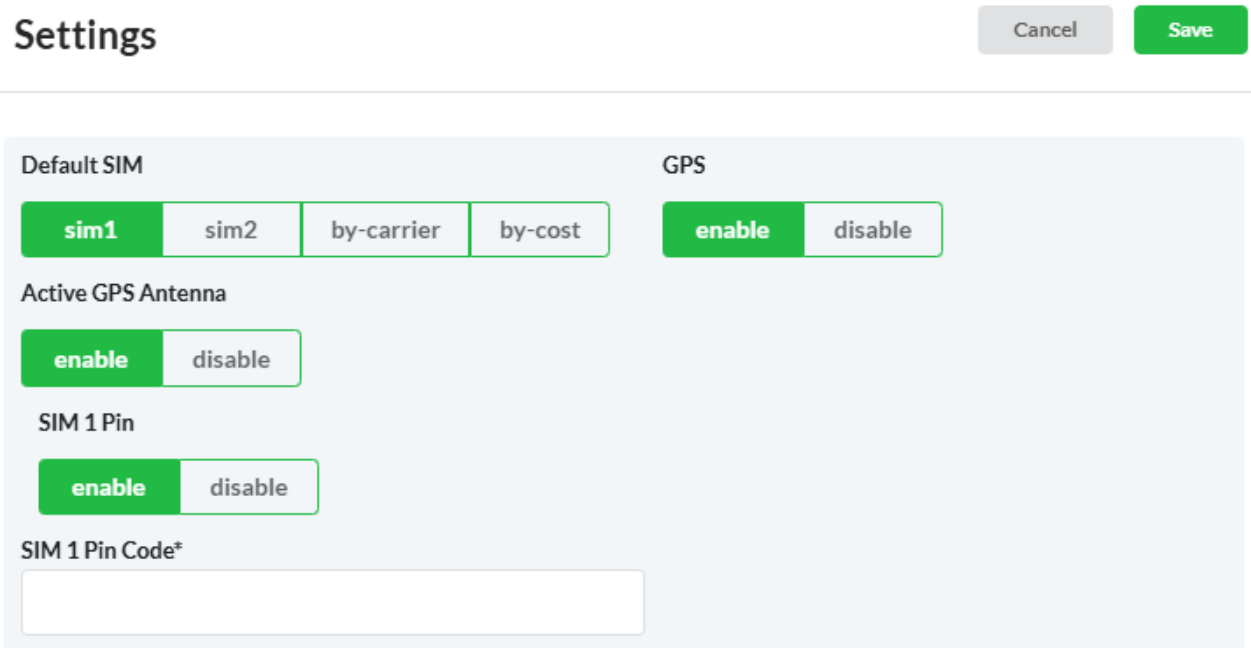
You must enable and configure a PIN on the SIM setting.

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.



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 183.

Essential networking configurations

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

- LAN interface on page 17
- LAN addressing on page 17
- DHCP server on page 18
- Health checks on page 19
- VWAN interface on page 20

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 42.

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:

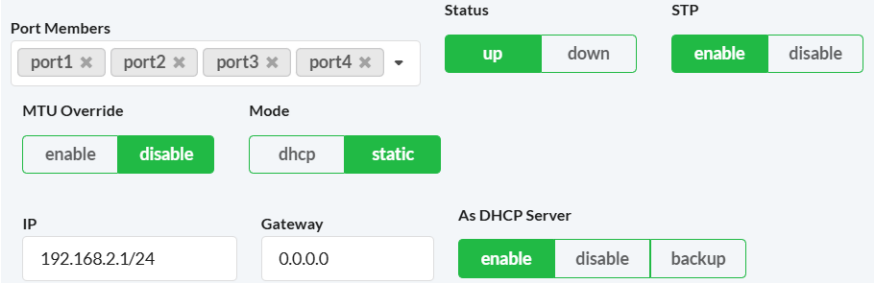
- Reliable routing of internet traffic from the LTE/5G network to internal devices.
- Device accessibility for administrators via local web GUI or CLI.
- Correct IP addressing and DHCP behavior, especially when FortiExtender acts as a DHCP server or relay.

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.



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.

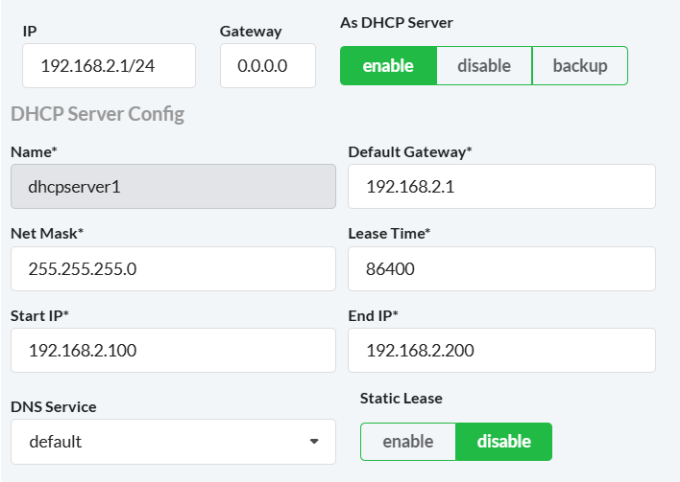
For more information about DHCP servers, see DHCP configurations on page 67

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.



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.

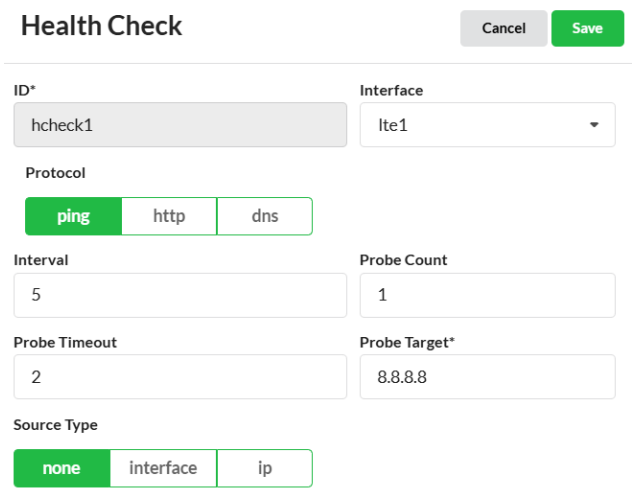
For more information, see Perform link health check on page 148.

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 Heath Check*.
2. Configure your heath check parameters.



3. 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.

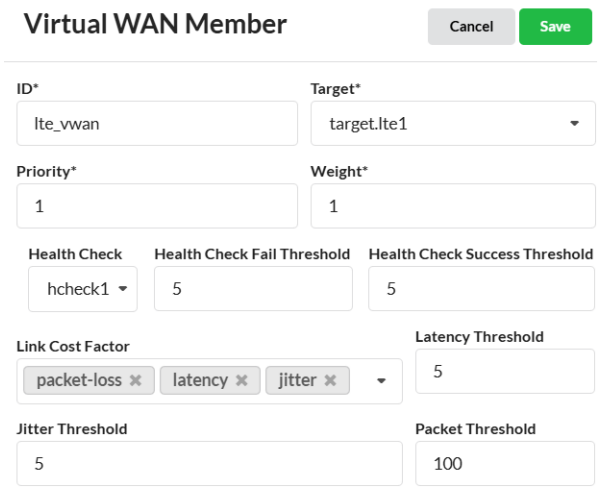
For more information, see Configure Virtual-WAN interface on page 48.

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:

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



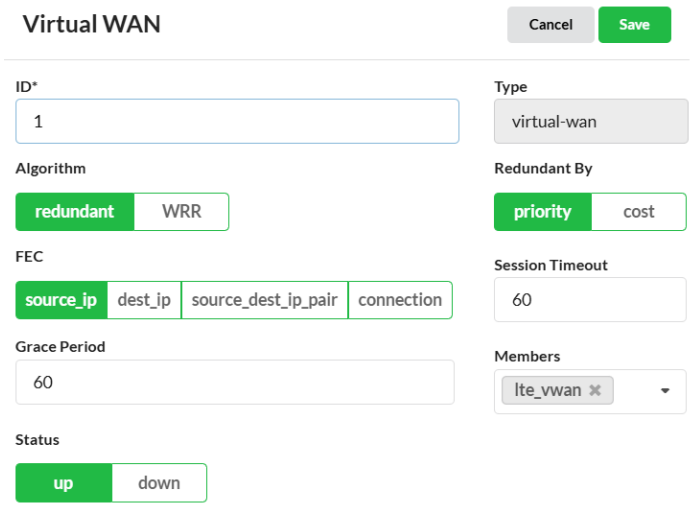
3. When you are finished, click *Save*.

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.



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 22
- Wireless WAN networks on page 23
- Virtual Access Points and SSID on page 24
- Radio profiles on page 25

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 22.

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.

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

Virtual Access Points and SSID

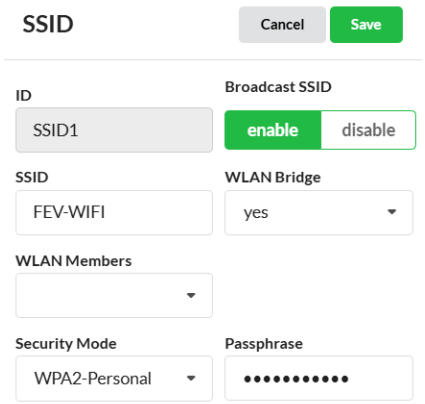
FortiExtender supports the creation of Virtual Access Points (VAPs), each representing a unique SSID. An SSID is the network name broadcast by the extender, allowing client devices to identify and connect to the wireless network.

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

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



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.

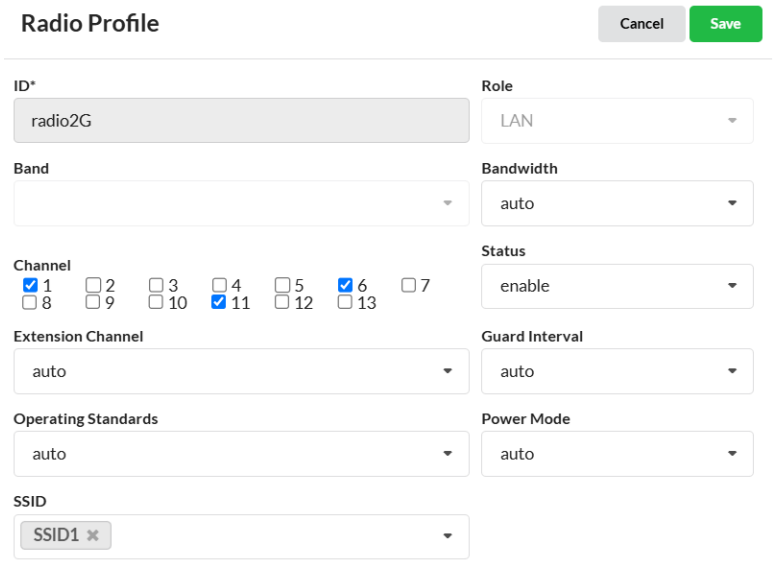
To configure radio profiles - CLI:

```
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.



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 polices and routes to control and direct traffic.

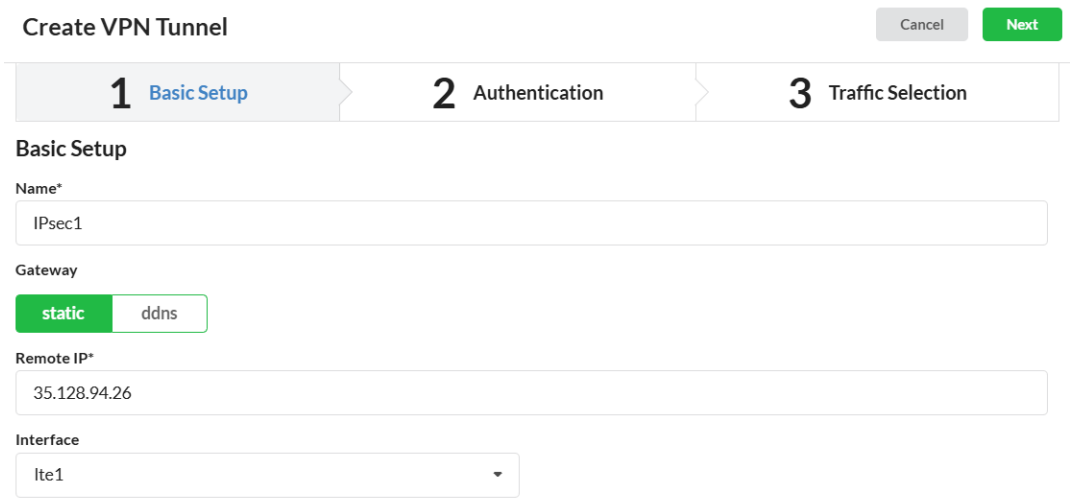
For more information about VPNs, see Configure VPN on page 94.

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.



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

Main LTE/5G features

FortiExtender offers the following main LTE/5G features:

- Cellular capabilities on page 29
- Supported wireless carriers on page 30
- SIM mapping on page 31
- Add a data plan and APN on page 31
- Global SIM with roaming on on page 32
- SIM-switch on page 32
- Get modem status on page 35
- Stopping data traffic on overaged LTE interface on page 36
- OBM management on page 36
- Multiple Packet Data Network (PDN) on page 37

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

For more information about adding a new carrier to the list of supported wireless carriers, see Add a new carrier profile on page 182

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 'rssi<=-100'	OFF	OFF	OFF	OFF
-90~-81	ON	OFF	OFF	OFF
-80~-71	ON	ON	OFF	OFF
-70~-61	ON	ON	ON	OFF
rssi>=-60	ON	ON	ON	ON

SIM-switch is a feature in data plan configuration which can be configured from 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. From the FortiExtender CLI, 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/adapter. Once you've logged into FortiExtender, you can access its console port using the following procedures:

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

```
# execute obm-console
Welcome to OBM Console - Serial Redirector.
```

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

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

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

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)

Multiple PDNs are not supported in IPv6 or in IPv4-IPv6 dual stack scenarios.

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).

To configure an interface - GUI:

1. From the FortiExtender GUI, go to *Networking* > *Interface*.
2. Select an interface and click *Edit*.
3. Configure the interface settings as needed.
4. When you are finished click Save.

To configure an interface - CLI:

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

CLI command	Description
`config system interface`	Enters system interface configuration mode.
`edit <interface_name>`	Specify or edit interface name (lan, lo, lte1 or wan).
`set type <type>`	Select the interface type: • `lan-switch`—LAN interface (Can be edited only). • `physical`—LAN interface (Can be edited only). • `lte`—LTE interface (Can be edited only). • `loopback`—Loopback interface (Can be edited only). • `tunnel`—Tunnel interface (Can be created, edited, or deleted). • `virtual-wan`—Virtual WAN interface (Can be created, edited, or deleted). • `vlan`–Vlan interface (Can be created, edited, or deleted) • `dummy`—Dummy interface (Can be created, edited, or deleted) • `capwap`–Capwap interface (Can edited only) • `vxlan`—Vxlan interface (Can edited only) • `aggregate`–Aggregate interface (Can edited only) • `switch`–Switch interface (Can edited only)
`set status {up | down}`	Specify the interface state: • `up`—Enabled.

CLI command	Description
	• down—Disabled.
set mode {static | dhcp}	Set the interface IP addressing mode: • static—If selected, FortiExtender will use a fixed IP address. See set ip <ip> below. • dhcp—If selected, FortiExtender will work in DHCP client mode.
set ip <ip>	(Applicable only when IP addressing mode is set to "static".) Specify an IPv4 address and subnet mask in the format: x.x.x.x/24
set gateway <gateway>	Set an IPv4 address for the router in the format: x.x.x.x
set mtu <mtu>	Set the interface's MTU value in the range of 512—1500.
allowaccess {ping | http | https | telnet}	Select the types of management traffic allowed to access the interface: • ping—PING access. • http—HTTP access. • https—HTTPS access. • telnet—TELNET access. • ssh—Secure Shell access. • snmp—SNMP access.
config ipv6	Configure the IPv6 interface settings. • set status {enable| disable} • set ip6-mode static • set autoconf {enable| disable} • set ip6-address <IPv6 prefix> • set ip6-gw <IPv6 Gateway> • set ip6-allowaccess {ping | http | telnet | ssh | https | snmp}

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 29.

Tunnel interface

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

Virtual-WAN interface

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

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

LAN interface configuration example:

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

WAN interface configuration example:

```
FX211E5919000009 # config system interface
FX211E5919000009 (interface) # edit wan
FX211E5919000009 (wan) # show
edit wan
    set type physical
    set status up
```

```
    set mode dhcp
    set mtu-override enable
    set mtu 1500
    set vrrp-virtual-mac enable
    config vrrp
        set status disable
    end
    set allowaccess
next

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

Access allowance

You can configure the physical, LTE, and tunnel interfaces 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.

```
config system interface
  edit <name>
    set type
    set allowaccess {option1}, {option2}, ...
  next
end
```

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:

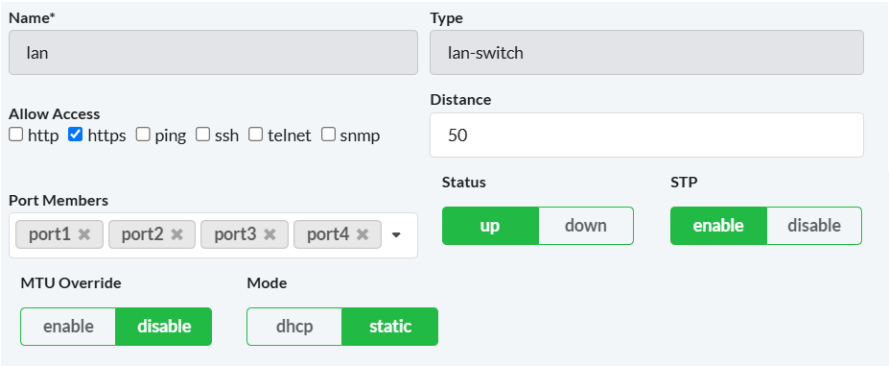
```
config system lan-switch
  config ports
    delete port4
  next
end
```

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.



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 117).

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
```

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:

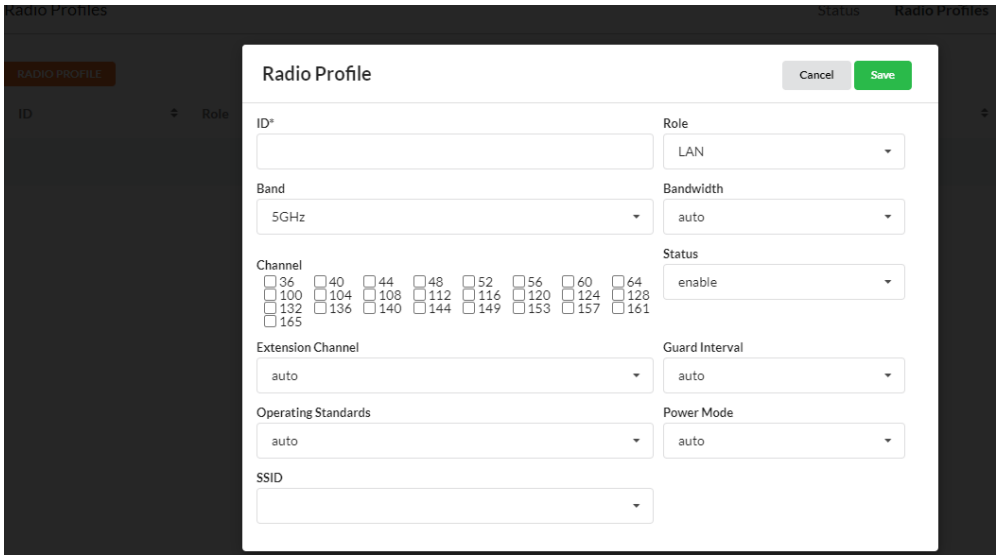
Scenario	DFS channel selection permission	
	FEV21xF	FBS10F
Fixed channel	Deny	Deny
Initial channel selection once the radio is up	Deny	Allow
Running time channel selection	Allow	Allow

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-profole
    edit <profile>
    set channel <choose from DFS channel list>
  next
end
```

IPv6

From an administrative point of view IPv6 works almost the same as IPv4 in FortiExtender. The primary difference is the use of IPv6 format for addresses. For an overview on IPv6, refer to the *FortiGate Administration Guide*.

IPv6 on FortiExtender does not support NAT66, NAT46, or NAT64.

Supported models

IPv6 is supported on the following FortiExtender models:

- FEXT-101G
- FEXT-211G
- FEXT-511G
- FEXT-511G-WIFI
- FEV-511G
- FER-511G

IPv6 address assignment

On a FortiExtender, an interface can use the following methods to obtain an IPv6 address:

Method	Overview
IPv6 static mode	• Manually configure IPv6 address.
IPv6 stateless address auto-configuration (SLAAC)	• Enables each network host to auto-configure a unique IPv6 address. • The lack of a state eliminates the need for a centralized server, thereby simplifying network management.

Static routing in IPv6

IPv6 static routing can be configured through the CLI. See Configure static routing on page 73.

Configuring IPv6

This section covers how to set up a basic IPv6 settings on the FortiExtender. Setting up IPv6 consists of the following steps:

1. Configure an IPv6 interface on page 54
2. Configure the IPv6 DNS on page 55
3. Create an IPv6 Address object on page 56

4. Configure the firewall policy on page 56

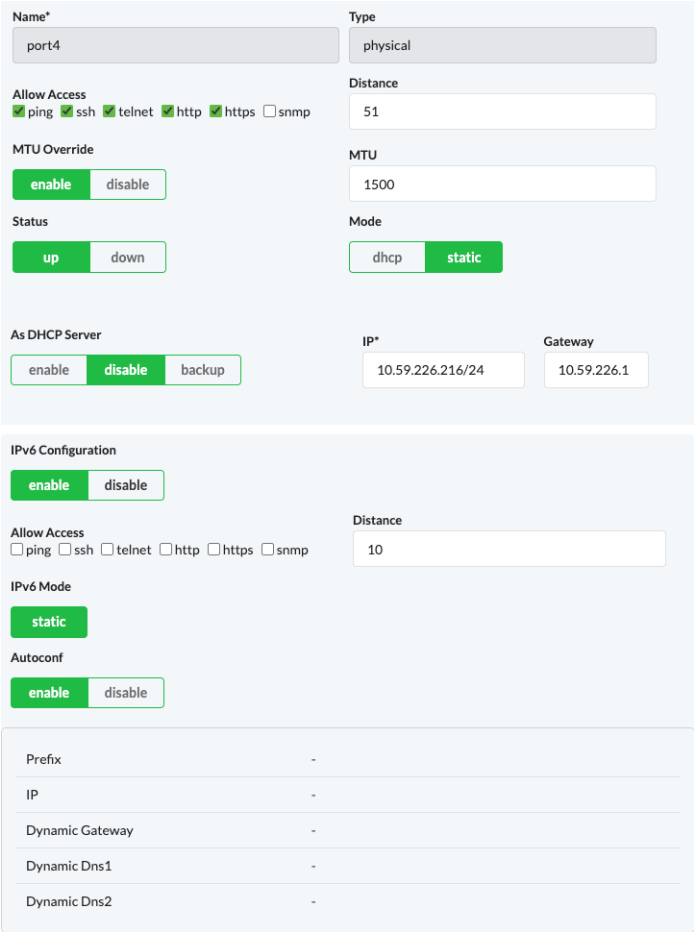
Configure an IPv6 interface

IPv6 is supported on the following types of interfaces:

- Wired Ethernet interface
- Switch interface
- LTE interface

To configure an interface - GUI:

1. From the FortiExtender GUI, go to *Networking* > *Interface*.
2. Select an interface and click *Edit*.
3. In *Allow Access*, select the IPv6 access options as needed (such as PING, HTTPS, and SSH).
4. In *Mode*, select *static*.
   Only static mode is supported, so the IPv6 address can be configured manually or through Autoconf (also known as SLAAC). For information on how to configure SLAAC, see Configure IPv6 SLAAC on an interface on page 58.



5. Click *Save*.

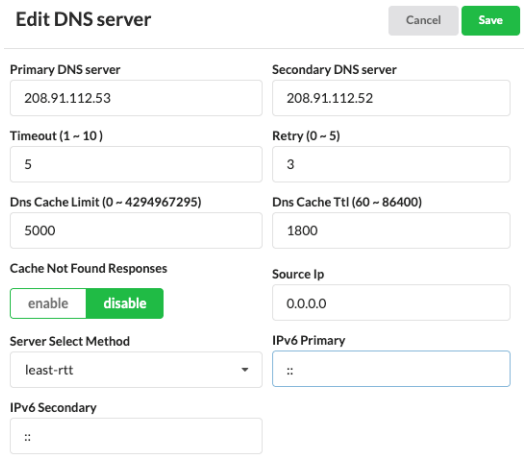
To configure an interface - CLI:

```
config system interface
  edit <interface name>
    config ipv6
      set status enable
      set ip6-mode static
      set autoconf disable
      set ip6-address <IPv6 prefix>
      set ip6-gw <IPv6 Gateway>
      set ip6-allowaccess {ping | http | telnet | ssh | https | snmp}
    end
  next
end
```

Configure the IPv6 DNS

To configure the IPv6 DNS - GUI:

1. From the FortiExtender GUI, go to *Networking* > *DNS* and then click *Edit*.
2. Configure the primary and secondary DNS servers as needed.



3. Click *Save*.

To configure the IPv6 DNS - CLI:

```
config system dns
  set ip6-primary <IPv6 Address>
  set ip6-secondary <IPv6 Address>
end
```

Create an IPv6 Address object

To configure an IPv6 Address object - GUI:

1. From the FortiExtender GUI, go to *Networking* > *Address* and then click *Create IPv6 Address*.
2. Enter a *Name* for the address object.

3. In the *Type* field, select one of the types.
4. Configure the remaining settings as required.
5. Click *Save*.

To configure an IPv6 Address object - CLI:

```
config network address6
  edit <name>
    set type <type>
    set subnet <ipv6 prefix>
  next
end
```

Configure the firewall policy

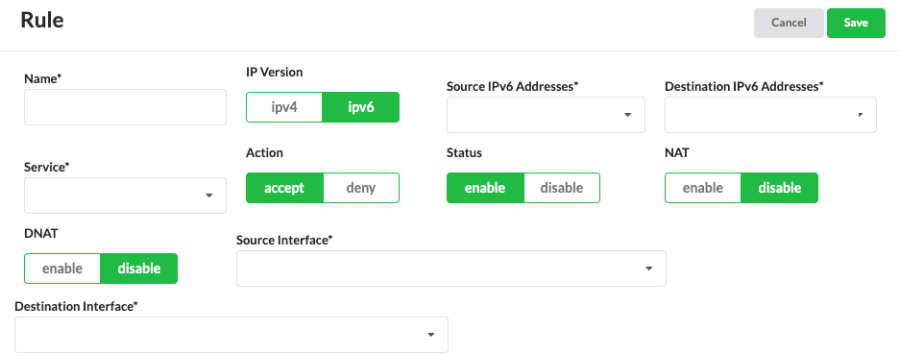
A firewall policy must be in place for any traffic that passes through a FortiExtender.

To create a firewall policy - GUI:

1. From the FortiExtender GUI, go to *Firewall* > *Policy* and click *Create Rule*.
2. Configure the following necessary settings:

Fields	Description
Name	Enter a nName for this policy.
IP Version	Select IPv4 or IPv6. In this example, select IPv6.
Source IPv6 Address	Enter the previously created IPv6 address object.
Destination IPv6 Address	Enter the previously created IPv6 address object.

Fields	Description
Action	Select if you want to accept or deny the policy.
Status	Enable or disable this rule.
NAT	Select if you want to enable or disable the Source NAT. In this example, select *disable*.
DNAT	Select if you want to enable or disable the Destination NAT. In this example, select *disable*.
Source Interface	Enter the incoming (ingress) interface.
Destination Interface	Enter the outgoing (egress) interface.



3. Click *Save*.

To create a firewall policy - CLI:

```
config firewall policy
  edit <name>
    set srcintf <Source Interface>
    set dstintf <Destination Interface>
    set srcaddr
    set dnat disable
    set dstaddr
    set srcaddr6 <IPv6 Address object>
    set dstaddr6 <IPv6 Address object>
    set action <accept | deny>
    set status <enable | disable>
    set service ALL
    set nat disable
  next
end
```

Configure IPv6 SLAAC on an interface

FortiExtender support stateless address autoconfiguration (SLAAC) addressing mode, enabling users to automatically acquire an IPv6 address, gateway, and DNS. FortiExtender can also work as a router server to send router advertisement (RA) messages to the client.

IPV6 SLAAC is only supported on the physical interface, switch interface, and LTE interface.

Router server configuration is not supported on the LTE interface.

To enable SLAAC on a supported interface - GUI

1. From the FortiExtender GUI, go to *Networking* > *Interface*.
2. Edit the interface you want to enable SLAAC on.
3. In *IPv6 Configuration*, select *enable*.
4. In *Autoconf*, select *enable*.

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

To enable SLAAC on a supported interface - CLI

1. From the FortiExtender CLI, configure the following:

```
config system interface
  edit lan
    config ipv6
      set status enable
      set ip6-mode static
      set autoconf enable
      set ip6-send-adv disable
      set ip6-allowaccess
      set distance 10
    end
  next
end
```

2. To verify your configurations, you can use the following commands to check the IPv6 address:

a. Check the system IPv6 interface:

```
# get system ipv6 interface
== [ lan ]
name: lan         mode: static      distance: 10          autoconf: enabled
prefix:  2002:db3:4:6::/64
ip:      2002:db3:4:6:4a3a:2ff:febb:432/64
gateway: fe80::8280:2cff:fe1a:56d8
dns:     8:7:8:7::
```

```
# get system interface-ipv6
== [ lan ]
name: lan             status: online/up/link up           type: switch          mac:
48:3a:02:bb:04:32   mode: static          mtu: 1500
                      ipv6: 2002:db3:4:6:4a3a:2ff:febb:432/64             gateway:
fe80::8280:2cff:fe1a:56d8                    dns: 8:7:8:7::
```

b. Check the default route:

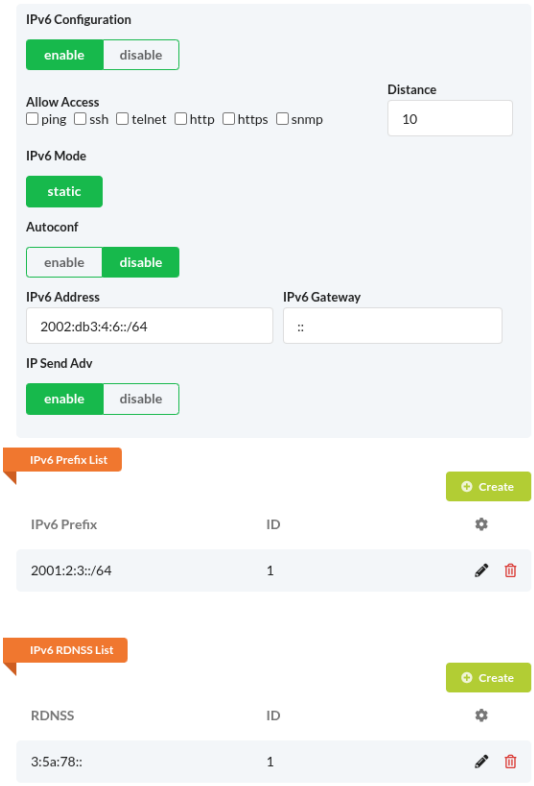
```
# get system ipv6 route
default via fe80::8280:2cff:fe1a:56d8 dev lan proto ra metric 10  expires 1793sec pref
medium
```

c. Check the interface IPv6 address

```
# get system ipv6 address lan
26: lan: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 2002:db3:4:6:4a3a:2ff:febb:432/64 scope global mngtmpaddr dynamic
       valid_lft 49sec preferred_lft 39sec
    inet6 fe80::4a3a:2ff:febb:432/64 scope link
       valid_lft forever preferred_lft forever
```

To enable a router server on a supported interface - GUI:

1. From the FortiExtender GUI, go to *Networking > Interface*.
2. Edit the interface you want to enable a router server on.
3. In *IPv6 Configuration*, select *enable*.
4. In *Autoconf*, select *disable*.
5. In *IP Send Adv*, select *enable*.
6. Click *Create* to add a prefix list and RDNSS list.



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

To enable a router server on a supported interface - CLI:

1. From the FortiExtender CLI, configure the following:

```
config system interface
  edit lan
    config ipv6
      set status enable
      set ip6-mode static
      set autoconf disable
      set ip6-send-adv enable
      set ip6-manage-flag disable
      set ip6-other-flag disable
      set ip6-max-interval 600
      set ip6-min-interval 198
      set ip6-adv-rio disable
      set ip6-address 2001:3:6:7::1/64
      set ip6-gw ::
      set ip6-allowaccess
      set distance 10
      config ip6-prefix-list
        edit 1
          set ip6-prefix 2001:3:6:7::/64
        next
      end
```

```
      config ip6-rdnss-list
        edit 1
          set ip6-rdnss 3:5a:78::
        next
      end
    end
  next
end
```

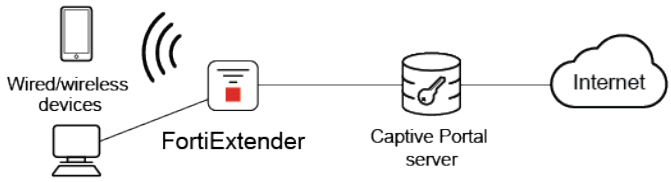
- You cannot enable `autoconf` and `ip6-send-adv` at the same time.
- When configuring `ip6-prefix`, it's better to configure using a /64 subnet so that the client can generate a SLAAC address.

Configure captive portals

Wi-Fi capable FortiExtender models support captive portals, which are used to enforce authentication before web resources can be accessed. Captive portal security provides an access point that initially appears open. Clients can connect to the access point with no security credentials, but any HTTP request returns the captive portal authentication page. Until the user enters valid credentials, no communication beyond the AP is permitted. After successfully authenticating, a user can access the requested URL and other web resources, as permitted by policies. The captive portal can also be configured to only allow access to members of specific user groups.

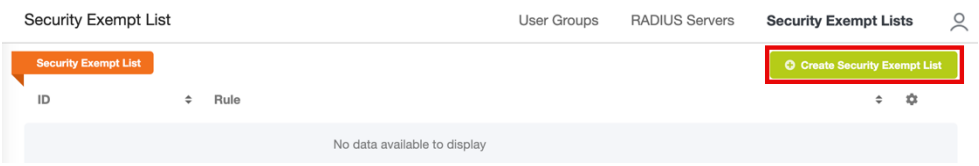
In general, all users on the interface are required to authenticate before accessing the internet, however, you can create security exemption lists for devices that are unable to authenticate, such as a printer that requires access to the internet for firmware upgrades.

FortiExtender captive portals are hosted on an external authentication server. They can be configured on either the switch or WiFi-LAN interface. The switch and WiFi-LAN interfaces may contain one or more VAPs as its member.

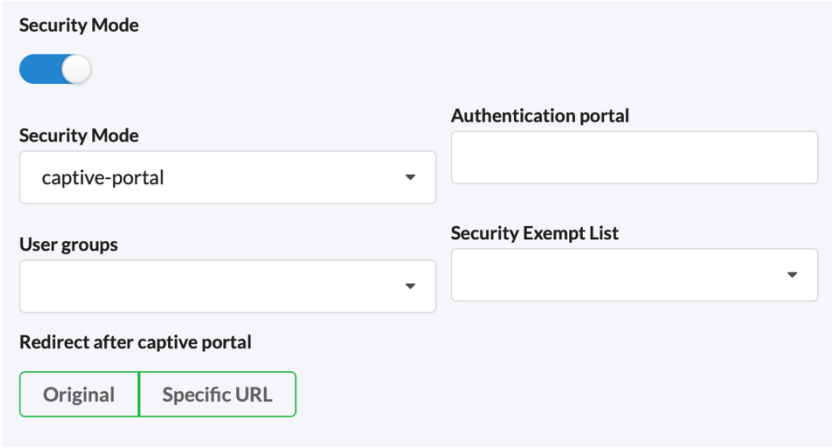


To configure a captive portal - GUI:

1. From the FortiExtender GUI, go to *User & Auth* > *User Groups* and click *Create User Group* to add a user group.
2. From *User & Auth* > *Security Exempt List*, click *Create Security Exempt List* to create a list of users exempt from the captive portal.



3. Go to *Networking* > *Interface* and edit the interface that the users connect to. The interface *Type* must be *WiFi LAN* or *Switch Interface*.



4. Configure the following fields:

1.	**Security Mode**	Enable *Security Mode*.
	Authentication Portal	Enter the FQDN or IP address of the external portal.
	User groups	Select the user groups that can authenticate with the captive portal.
	Security Exempt List	Select the security exempt list profiles you configured.
	Redirect after captive portal	Configure website redirection after successful captive portal authentication: • *Original Request*: redirect to the initially browsed to URL . • *Specific URL*: redirect to the specified URL.

To configure a captive portal - CLI:

1. From the FortiExtender CLI, add and configure user groups.

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

2. If necessary, create a security exemption list.

```
config user security-exempt-list
  edit <list>
    config rule
```

```
      edit 1
        set srcaddr <source(s)>
        set dstaddr <source(s)>
        set service <service(s)>
      next
   edit 2
        set srcaddr <source(s)>
        set dstaddr <source(s)>
        set service <service(s)>
      next
    end
  next
end
```

3. Configure captive portal authentication on a WiFi LAN or Switch interface and add the user group(s) and security exemption list(s).

```
config system interface
  edit <interface>
    set security-mode {none | captive-portal}
    set security-external-web <string>
    set security-groups <group(s)>
    set security-exempt-list <list>
    set security-redirect-url <string>
  next
end
```

Example captive portal configuration

1. Configure your FortiExtender in AP Mode (see Configure FortiExtender as a Wi-Fi AP on page 121 or Configure FortiExtender Wi-Fi APs as members of switch interface on page 129).

```
config wifi vap
  edit v1
    set ssid dengh-cap-fev511g
    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 OPEN
    end
  next
end
config wifi radio-profile
  edit r1
```

```
    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 v1
  next
end
```

2. Configure a RADIUS authentication server for your captive portal.

```
config user radius
  edit radius1
    set server demo.fortinet.com
    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
    set source-ip 0.0.0.0
  next
end
```

3. Configure a User Group and set the member to the RADIUS server you created.

```
config user group
  edit g1
    set member radius1
  next
end
```

4. Configure network address used in the security exempt list.

```
config network address
  edit lan
    set type ipmask
    set subnet 192.168.200.0/24
  next
  edit all
    set type ipmask
    set subnet 0.0.0.0/0
  next
```

```
  edit none
    set type ipmask
    set subnet 0.0.0.0/32
  next
  edit portal
    set type fqdn
    set fqdn demo.fortinet.com
  next
  edit ex1
    set type fqdn
    set fqdn www.example.com
  next
  edit ex2
    set type fqdn
    set fqdn login.example.com
  next
  edit star-ex
    set type ipmask
    set subnet 57.144.0.0/16
  next
  edit ex-cdn
    set type fqdn
    set fqdn static.xx.examplecdn.net
  next
end
```

5. Create a security exemption list and add your network addresses.

```
config user security-exempt-list
  edit captive-portal-exempt
    set description captive-portal-exempt portal exempt list
    config rule
      edit 1
        set srcaddr lan
        set dstaddr portal
        set service HTTP HTTPS
      next
      edit 3
        set srcaddr lan
        set dstaddr all
        set service DNS DNS_TCP
      next
      edit 2
        set srcaddr lan
        set dstaddr ex1 ex2 star-ex
        set service HTTP HTTPS
      next
    end
  next
end
```

6. Apply your captive portal configurations on either the wireless LAN interface or switch interface depending on which interface you configured your VAP on.

```
config system inferface
  edit lan
    set type switch
    set status up
    set mode static
    set ip 192.168.200.99/24
    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 http https ssh ping telnet
    set security-mode captive-portal
    set security-external-web https://demo.fortinet.com/portal
    set security-groups g1
    set security-exempt-list captive-portal-exempt
    set security-redirect-url
    config ipv6
      set status disable
      set autoconf disable
      set ip6-send-adv disable
      set ip6-address ::/0
      set ip6-gw ::
    end
  next
end
```

7. When a user from the permitted user group connects to the FortiExtender AP, they will be directed to the captive portal authentication page. After successfully authenticating, they will be redirected to their original URL.

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 70

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

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 - 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.

Example DHCP server configuration - CLI:

```
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>
```

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 71
- Service on page 71
- Target on page 71

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 73
- Configure Policy Based Routing on page 74
- Configure dynamic routing — OSPF on page 78
- Configure multicast routing on page 87

Configure static routing

You can configure IPv4 and IPv6 static routing with the following commands.

IPv4 static routing

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

Example static route configuration:

```
config router static
   edit 1
      set status enable
      set dst 0.0.0.0/0
      set gateway 192.168.2.1
      set distance 5
      set device lan
      set comment
   next
end
```

IPv6 static routing

CLI command	Description
`config router static6`	Enters static route configuration mode.
`edit <name>`	Specify the name of the static route.
`set status {enable | disable}`	Set the status of the static route: • `enable`—Enable the static route. • `disable`—Disable the static route.
`set dst <dst>`	Specify the destination IP address and netmask of the static route in the format: `x.x.x.x/x`
`set gateway <gateway>`	Specify the IP address of the gateway.
`set distance <distance>`	Specify the administrative distance. The range is 1–255. The default is 1.
`set device <device>`	Specify the name of the outgoing interface.
`set comment [comment]`	Enter a comment (optional).

```
config router static6
  edit <name>
    set status enable
    set dst <IPv6 Prefix>
    set gateway <IPv6 Address>
    set distance 10
    set device <interface>
    set comment
  next
end
```

Configure Policy Based Routing

You can configure Policy Based Routing (PBR) using router targets and router policies.

Router target

You can configure IPv4 and IPv6 router targets. For IPv6, use `config router target6`.

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
end
```

Router policy

You can configure IPv4 and IPv6 router policies. For IPv6, use `config router policy6`.

CLI Command	Description
`config router policy`	Configure router policies
`edit <name>`	Specify the name of the routing policy.
`set input-device <name1>`	Specify the incoming interface name.
`set srcaddr <name1>`	Source IP and mask for this policy based route rule.
`set dstaddr <name1>`	Destination IP and mask for this policy based route rule.
`set service <name1>, <name2>, …`	Service and service group names.
`set *target <name1>`	This PBR's out-going interface and next-hop.
`set status [enable | disable]`	Enable/disable this policy based on the routing rule.
`set comment{string}`	Optional comments.

Example PBR policy configuration:

```
config router policy
  edit 1
    set input-device lan
    set srcaddr all
    set dstaddr all
    set service ALL
    set target target.lte1
    set status enable
    set comment this is a test policy
  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
```

Parameter	Description	Type	Size	Default
status	Set the status of the OSPF.	option	-	disable
	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
	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>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td>
<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.
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 mtu-ignore is disabled, OSPF will detect mismatched MTUs, and OSPF adjacency is not established if MTU is mismatched.</td></tr>
</table>
</td><td></td><td></td><td></td></tr>
<tr><td>config redistribute</td><td>Redistribute configuration.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>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>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</td></tr>
</table>
</td></tr>
</table>
</td><td></td><td></td><td></td></tr>
</table>

Parameter	Description	Type	Size	Default

Option	Description

Option	Description
	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

`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`
	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, `10.0.0.0/24 le 30` will match 10.0.0.0/24 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:

```
ForitExtender# config router
   config prefix-list
      edit local-nets
         config rule
            edit 10
               set action permit
               set prefix 192.168.201.0/24 set ge 0
               set le 0
```

```
            next
        end
    next
    edit static-routes
       config rule
          edit 10
             set action deny
             set prefix 192.168.203.0/24 set ge 0
             set le 0
          next
          edit 20
             set action permit
             set prefix 192.168.202.0/24 set ge 0
             set le 0 next
    end
```

Step 2: Configuring route-map

CLI Command	Description

`config route-map`
`edit <route-map name>`
`config rule`
`edit <id>`
`set action [permit | deny]`
`set match-ip-address <prefix-list>`
	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
config router ospf config redistribute config [connected | static] set status [enable | disable] set metric-type [1 | 2] set metric <value> set route-map <route-map name>	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. • routemap—defined and configured on the route-map, see Configure route-map for details.

Example configuration:

```
ForitExtender# config router ospf
   config redistribute
      config connected
         set status enable
         set metric-type 2
         set metric 10
         set routemap redist-local-connected
   end
   config static
      set status enable
      set metric-type 2
      set metric 10
      set routemap redist-static
```

Verify OSPF configurations

Upon completing the OSPF configurations, you 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

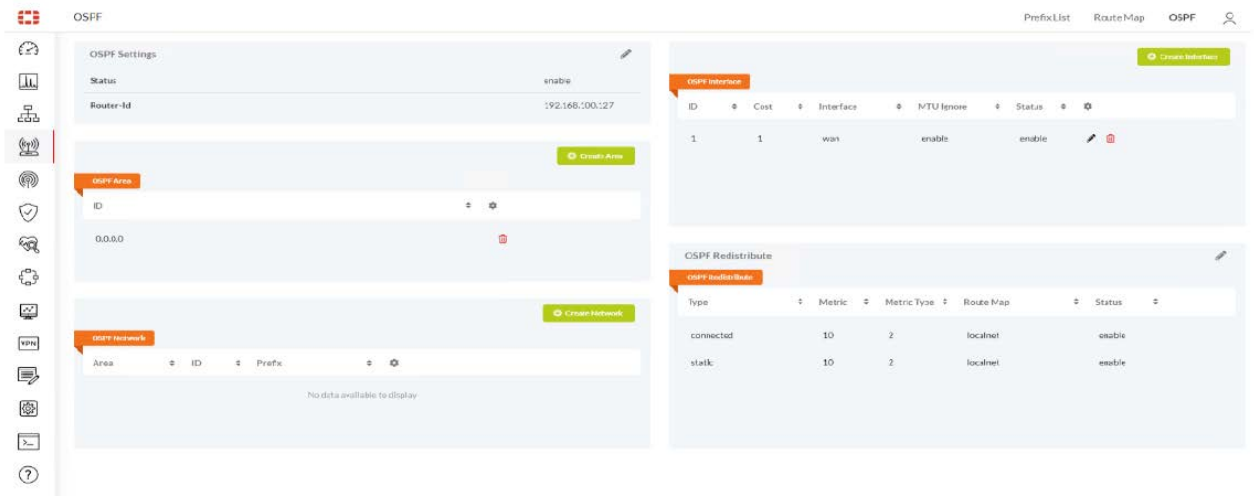
```
#get router info routing-table all
```

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
```

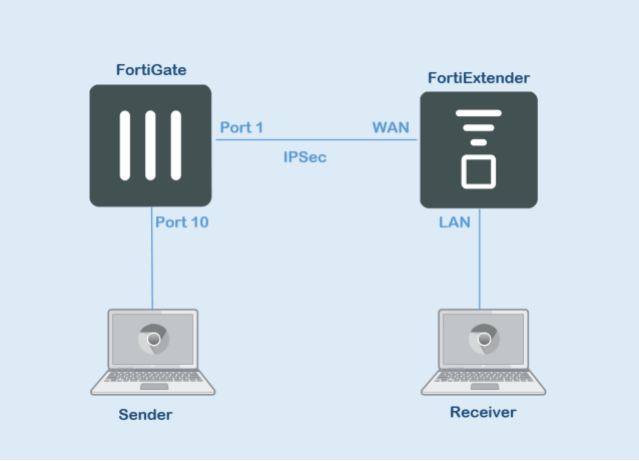
```
            edit 20
               set action deny
               set match-ip-address
            next
         end
      next
      edit redist-static
         config rule
            edit 20
               set action deny
               set match-ip-address
            next
            edit 10
               set action permit
               set match-ip-address static-routes
            next
      end

   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
```

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

A Firewall allows you to control network access based on Layer-3 or Layer-4 information. Also, Source Net Address Translation (SNAT) is provided.

Firewall configuration involves the following tasks:

- Configure address/subnet on page 88
- Configure protocol/port range on page 89
- Configure firewall policies on page 90

Configure address/subnet

You can configure IPv4 and IPv6 address/subnet to which you can apply firewall policies.

IPv4

CLI command	Description
`config network address`	Enters network IP address configuration mode.
`edit <name>`	Specify the name of the IP address configuration object.
`set type {ipmask | iprange}`	Select either address type: • `ipmask`—IPv4 address/mask in the format: `x.x.x.x/x` • `iprange`—IP addresses range.

IPv6

To configure an IPv6 Address object - GUI:

1. From the FortiExtender GUI, go to *Networking* > *Address* and then click *Create IPv6 Address*.
2. Enter a *Name* for the address object.

3. In the *Type* field, select one of the types.
4. Configure the remaining settings as required.
5. Click *Save*.

To configure an IPv6 Address object - CLI:

CLI command	Description
`config network address6`	Enters network IP address configuration mode.
`edit <name>`	Specify the name of the IP address configuration object.
`set type {ipmask | iprange}`	Select either address type: • `ipmask`—IPv6 address/mask. • `iprange`—IP addresses range.
`set subnet {ipv6-address}`	IP address and subnet mask.

Example IPv4 address/mask configurations:

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

Configure protocol/port range

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

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

Example protocol/port range configurations:

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

Configure firewall policies

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

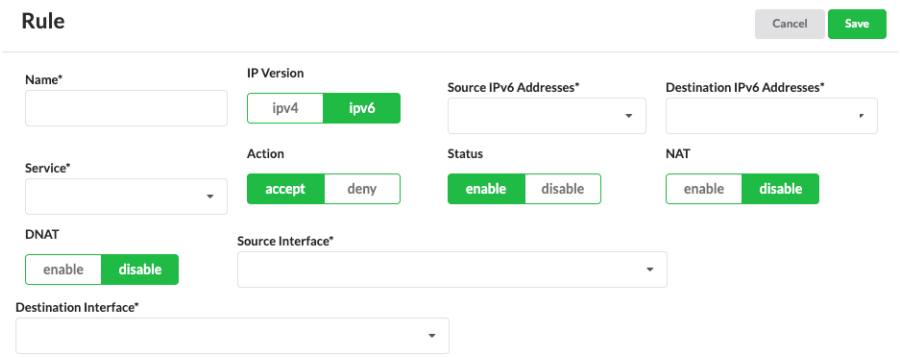
A firewall policy must be in place for any traffic that passes through a FortiExtender.

To create a firewall policy - GUI:

1. From the FortiExtender GUI, go to *Firewall* > *Policy* and click *Create Rule*.
2. Configure the following necessary settings:

Fields	Description
Name	The Name for this policy

Fields	Description
IP Version	IPv4 or IPv6.
Source IPv6 Address	Address object, which is created in above step
Destination IPv6 Address	Address object, which is created in above step
Action	Policy action
Status	Enable or disable
NAT	Source NAT, enable or disable.
DNAT	Destination NAT, enable or disable.
Source Interface	Incoming (ingress) interface
Destination Interface	Outgoing (egress) interface



3. Click *Save*.

To create a firewall policy - CLI:

CLI command	Description
`config firewall policy`	Enters firewall policy configuration mode.
`edit <name>`	Specify the name of the firewall configuration object.
`set srcintf`	Specify the ingress interface.
`set dstintf`	Specify the egress interface.
`set srcaddr`	Specify the source IP address, which can be either a single IP address or a range of IP addresses.
`set action {allow | deny}`	Select either of the following actions: • `allow`—Allow access. • `deny`—Deny access.

CLI command	Description
`set status {enable | disable}`	Set the status of the policy: • `enable`—Enable the policy. • `disable`—Disable the policy.
`set nat {enable | disable}`	Select an option for NAT: • `enable`—Enable NAT. • `disable`—Disable NAT.
`set srcaddr6`	Source IPv6 address.
`set dstaddr6`	Destination IPv6 address.

Example firewall policy configurations:

```
config firewall policy
  edit <name>
    set srcintf <Source Interface>
    set dstintf <Destination Interface>
    set srcaddr
    set dnat disable
    set dstaddr
    set srcaddr6 <IPv6 Address object>
    set dstaddr6 <IPv6 Address object>
    set action <accept | deny>
    set status <enable | disable>
    set service ALL
    set nat disable
  next
end
```

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

Move firewall policies

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

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

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

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

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

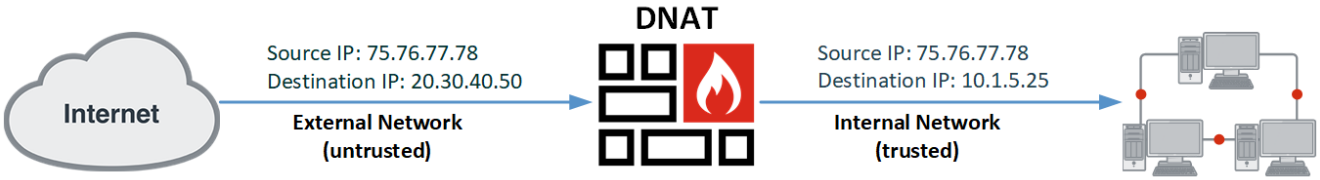
```
move filter1 after filter2
```

or

```
move filter2 before filter1
```

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.

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:

1. Configure phase-1 parameters
2. Configure phase-2 parameters
3. Configure firewall policies
4. Configure route (see System routing on page 73)

Configure phase-1 parameters

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.

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`	Diffie-Hellman (DH) key exchange in phase1 is used to negotiate and exchange private keys for phase2. Select one of the following DH groups: `1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, 30, 31, 32` **Note:** 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).
`*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`

CLI command	Description
*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.
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.

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. The DH groups in phase2 should be set to the same value as those for phase1, and PFS is recommended.
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:

Parameter	Description
	• subnet— IPv4 subnet • range —IPv4 range • ip —IPv4 IP • name — IPv4 network address name
src-subnet	Local proxy ID subnet. **Note:** This field is only available when src-addr-type is set to subnet.
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 polices to permit communications between the source and destination addresses.

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

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: Click *VPN* > *VPN Certificate* > *CA Certificate* > *Import New Certificate*.

Import a third-party Local certificate

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

Use third-party certificates for IKE authentication

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
```

DNS Service

FortiExtender running 7.2.0 and later 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.

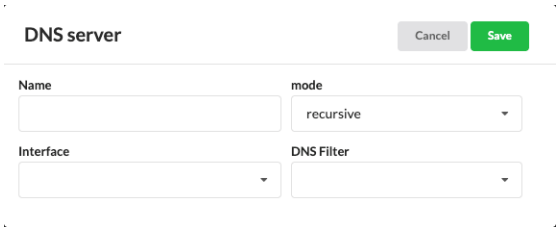
When DNS service is enabled on a specific interface, the FortiExtender listens for DNS query requests on that interface. Depending on the configuration, the DNS service on FortiExtender can work in three modes:

- **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.

Once you set up a DNS server, you can apply a DNS filter profile to control user access to web resources. For more information about DNS filtering, see DNS Filtering on page 109.

To enable DNS service on a specific interface - GUI:

1. From the FortiExtender GUI, go to *Networking* > *DNS Server* and click *Create DNS Service*.
2. Configure the DNS server for the interface you want.



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

To enable DNS service on a specific interface - CLI:

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

Parameter	Description
interface	Required. Specify the interface to enable the DNS service. Only one DNS service can

Parameter	Description
	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
dns-filter	Select a DNS category filter profile (see DNS Filtering on page 109).

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)

Parameter	Description
	• 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. **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
ttl	Default time-to-live value for the entries of this DNS zone. Note: The value ranges from 0 to 2147483647. The default is 86400. This filed 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.

Parameter	Description
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.
ttl	Time-to-live for this entry. **Note:** The value ranges from 0 to 2147483647. The default is 0. The field is NOT required.
hostname	Hostname of the host. **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)
```

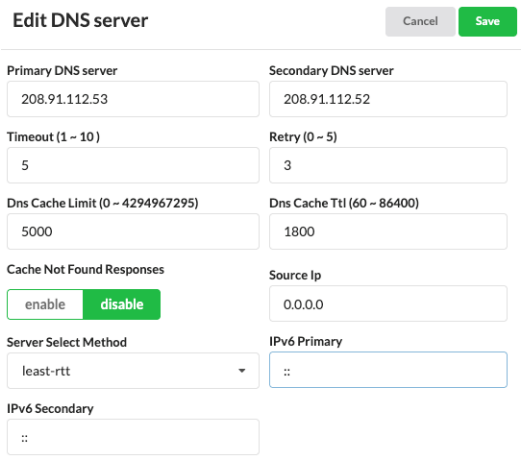
Configuring FortiExtender as a DNS proxy server

You can configure FortiExtender as a pure DNS proxy server which forwards DNS requests directly to the configured system DNS servers. Once configured, FortiExtender 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 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).

To configure DNS server parameters - GUI

1. From the FortiExtender GUI, go to *Networking* > *DNS*.
2. Click the *edit* button.
   The *Edit DNS* server window loads.



3. Configure the DNS server parameters as needed.
   You can configure IPv6 addresses in addition to IPv4 addresses.
4. When you are finished, click *Save*.

To configure DNS server parameters - CLI

1. From the FortiExtender CLI, you can configure the following FortiExtender system DNS parameters:

```
config system dns
  set primary 208.91.112.53
  set secondary 208.91.112.52
  set ip6-primary 2001:4860:4860::8888
  set ip6-secondary 2001:4860:4860::8844
  set timeout 5
  set retry 3
  set dns-cache-limit 5000
  set dns-cache-ttl 1800
  set cache-Tonotfound-responses disable
  set source-ip 0.0.0.0
  set server-select-method least-rtt
end
```

2. To verify your configurations, you can use the following command to check the DNS details:

```
# get system dns
primary                 : 208.91.112.53
secondary               : 208.91.112.52
IPV6 primary            : 2001:4860:4860::8888
IPV6 secondary          : 2001:4860:4860::8844
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        :
    lan:   8:7:8:7::
```

DNS Filtering

FortiExtender supports DNS category filtering to control user access to web resources. You can customize the default DNS filter profile or create your own, and then apply the profile to a DNS server on a FortiExtender interface.

You can also configure a DHCP server to point a user to a specific DNS server interface instead of the default system DNS server.

The following features are available in the FortiExtender DNS filter:

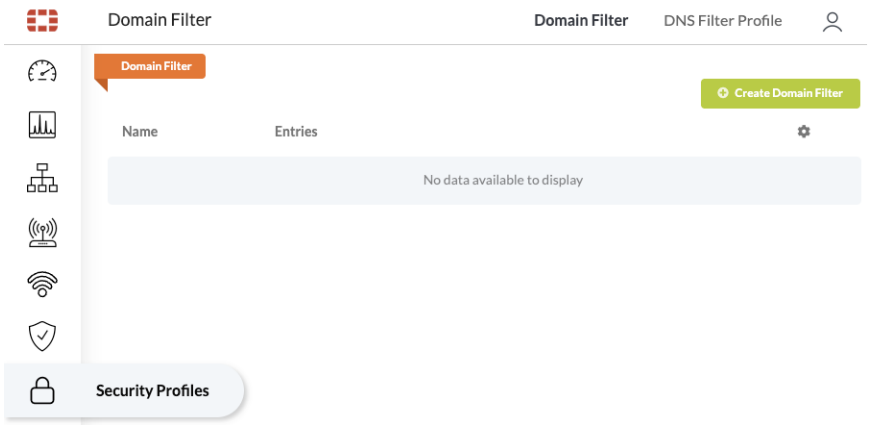
- **Botnet C&C domain blocking:** Blocks the DNS request for known botnet C&C domains.
  The botnet C&C domain is a domain list maintained by FortiGuard Service. The botnet C&C domain blocking feature can block the botnet website access at the DNS name resolving stage.
- **DNS safe search:** Enforces Google, Bing, and YouTube safe addresses for parental controls.
  The DNS safe search option helps avoid explicit and inappropriate results in the Google, Bing, DuckDuckGo, Qwant, and YouTube search engines. The FortiExtender responds with content filtered by the search engine.

  For individual search engine safe search specifications, refer to each company's respective documentation.

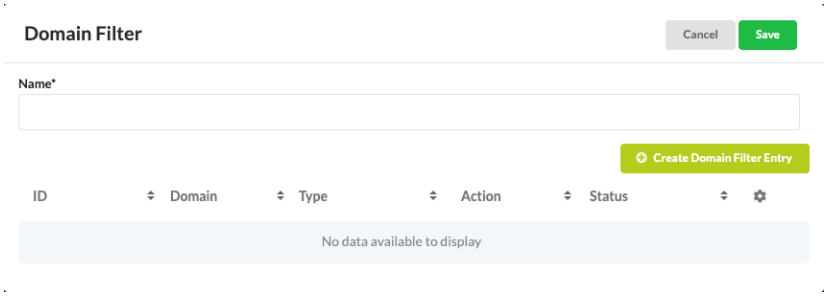
- **Domain filter:** Enables you to define your own domain list to block or allow.

To configure a DNS filter profile - GUI:

1. (Optional) From the FortiExtender GUI, go to *Security Profiles > Domain Filter*, to create a domain filter to apply to the DNS Profile.

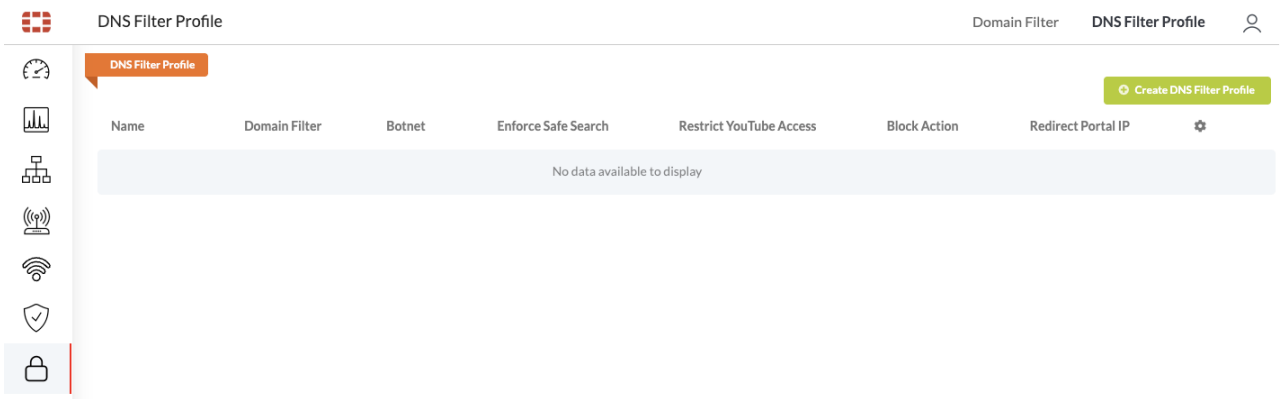


2. Click *Create Domain Filter* and configure the following:



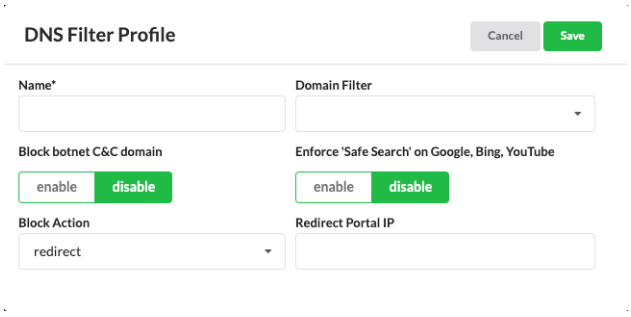
Name	Enter a name for a set of domain filter entries
Create Domain Filter Entry	Click to create individual entries for the filter
ID	Enter a name for the domain filter entry.
Domain	Enter a domain or Reg. Expression.
Type	Select the entry type: • *Simple*: Matches an exact string. • *Reg. Expression*: Matches using regex rules for advanced pattern matching. **Note:** If the domain string contains the character `?`, it can only be configured through the GUI. • *Wildcard*: Matches patterns using wildcards (e.g., *.example.com). **Note:** Only the * wildcard is supported.
Action	Select if you want to Block or Allow this entry. • *Block*: If the local domain filter action is set to block and an entry matches, then that DNS query is blocked or redirected. • *Allow*: If the local domain filter action is set to allow and an entry matches, it will directly return to the client DNS resolver.
Status	Enable/Disable this domain filter entry. • *Enable*: This domain filter takes effect. • *Disable*: This domain filter is disabled.

3. When you are finished, click *Save*.
4. From the FortiExtender GUI, go to *Security Profiles > DNS Filter Profile*.



5. Click *Create DNS Filter Profile* and configure the following:

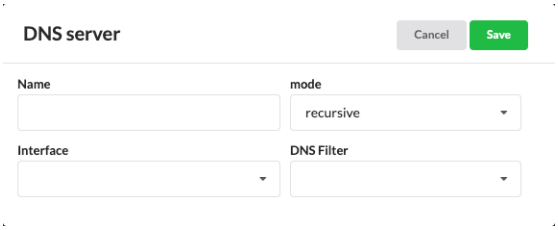
Name	Enter a unique name for the profile.
Domain Filter	Select a domain filter to apply to this profile.
Block botnet C&C domain	Enable to block botnet website access at the DNS name resolution stage.
Enforce 'Safe Search' on Google, Bing, YouTube	Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines.
Restrict YouTube Access	When *Enforce 'Safe Search' on Google, Bing, YouTube* is enabled, select either *Strict* or *Moderate* • *Strict*: Restricts YouTube access by responding to DNS resolutions with CNAME restrict.youtube.com. • *Moderate*: Restricts YouTube access by responding to DNS resolutions with CNAME restrictmoderate.youtube.com.
Block Action	Select what action is performed for blocked domains: • *Block*: The DNS request is blocked and a DNS response with NXDOMAIN is returned. • *Redirect*: A DNS response containing the portal IP address is returned, redirecting blocked domains to the SDNS portal. • *Block-SERVFAIL*: The DNS request is blocked, and a DNS response with SERVFAIL is returned.
Redirect Portal IP	Enter the IP address of the SDNS redirect portal



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

To apply a DNS filter profile to a DNS server - GUI:

1. From the FortiExtender GUI, go to *Networking* > *DNS Server* and click *Create DNS Service*.
2. Configure the DNS server for the interface you want and select the *DNS Filter* you previously created.

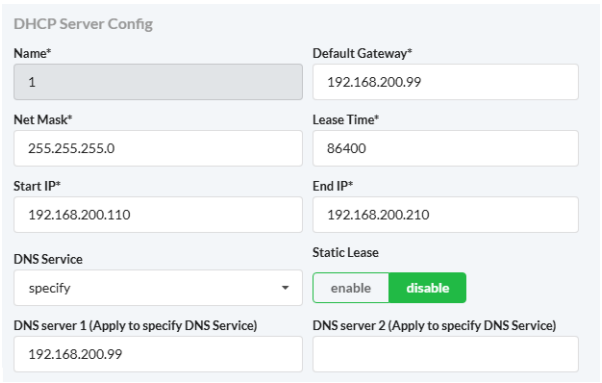


3. When you are finished, click *Save*.
   The DNS filter now applies to the FortiExtender interface.

To configure the DHCP server - GUI

You can also configure a DHCP server to point a user to a specific DNS server interface instead of the default system DNS server.

1. From the FortiExtender GUI, go to *Networking* > *Interface* and edit *LAN Switch*.
2. Under the *DHCP Server Config* section, enter set *DNS Service* to *specify*.
3. In *DNS server 1*, enter the IP address of the DNS server.



4. When you are finished, click *Save*.
   The DHCP server uses the specified DNS server interface instead of the system default.

To configure a DNS filter profile - CLI:

1. (Optional) Create a domain filter.

```
config dnsfilter domain-filter
  edit exampleFilter
    set comments example DNS filter
    config entries
      edit 1
        set domain www.example.com
        set type simple
        set action block
        set status enable
```

```
      next
    end
  next
end
```

2. Create a DNS filter profile and apply a domain filter, if needed.

```
config dnsfilter profile
  edit profile1
    config domain-filter
      set domain-filter-table exampleFilter
    end
    set block-action redirect
    set block-botnet enable
    set safe-search enable
    set youtube-restrict moderate
    set redirect-portal 0.0.0.0
  next
end
```

To apply a DNS filter profile to a DNS server - CLI:

1. Apply the DNS filter profile you created to the DNS server.

```
config system dns-server
  edit dnsserver1
    set interface lan
    set mode recursive
    set dns-filter profile1
  next
end
```

The DNS filter now applies to the FortiExtender interface.

To configure the DHCP server - CLI

You can also configure a DHCP server to point a user to a specific DNS server interface instead of the default system DNS server.

```
config system dhcpserver
  edit 1
    set status enable
    set lease-time 86400
    set dns-service specify
    set dns-server1 192.168.200.99
    set dns-server2
    set dns-server3
    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 192.168.200.110
    set end-ip 192.168.200.210
    set mtu 1500
    set vci_match disable
    set reserved-address disable
  next
end
```

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

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

- **Redundant:** 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. If the primary link (determined by priority) goes down, traffic is steered to the secondary link.

  If the algorithm were set to redundant mode, the priorities of the member interfaces (i.e., tunnel0 and tunnel1) must be different.
- **Weighted Round Robin (WRR):** In WRR mode, traffic is sent to each link member in a round-robin fashion based on the weight assigned to it. 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.

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`.

Use the following commands to configure an SD-WAN.

CLI command	Description
`config system interface`	Enters system interface configuration mode.
`edit <vwan_name>`	Specify the name of the SD-WAN interface.
`set type virtual-wan`	Set the interface type to virtual-wan.
`set status <status>`	Set the status of the interface: • `up`—Enable the interface. • `down`—Disable the interface.
`set FEC {source | dest | ip-pair | connection}`	Select a LLB metric to denote how to distribute traffic: • `source`—Traffic from the same source IP is forwarded to the same target. • `dest`—Traffic to the same destination IP is forwarded to the same target. • `ip-pair`—Traffic from the same source IP and to the same destination IP is forwarded to the same target. • `connection`—Traffic with the same 5 tuples (i.e., a source IP address/port number, destination IP address/port number and the protocol) is forwarded to the same target
`set algorithm {redundant | WRR}`	Select the LLB algorithm: • `redundant`—Targets work in primary-secondary mode. • `WRR`—Targets work in Weighted Round Robin mode.
`set grace-period`	Specify the grace period in seconds to delay fail-back.
`set session-timeout 60`	Specify the session timeout threshold in seconds. The default is 60. This is used to time out a VWAN session. A LLB session is created for each traffic stream. However, when a session times out, it is deleted.
`set members`	Add VWAN members to the VWAN interface.

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 interfce
        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 interfce
        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
`set target`	Specify the target to which traffic is forwarded.
`set priority`	Specify the priority of the link member. The valid value range is 1—7.
`set weight`	Specify the weight of the member.
`set health-check`	Specify the link health check of the VWAN.
`set health-check-fail-threshold`	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.
`set health-check-success-threshold`	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 a 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 120
- Configure FortiExtender as a Wi-Fi AP on page 121
- Configure FortiExtender Wi-Fi APs as members of switch interface on page 129.
- Configure FortiExtender as a Wi-Fi station on page 131

When FortiExtender is configured to operate in AP mode, you can configure Captive Portal authentication (see Configure captive portals on page 61).

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.

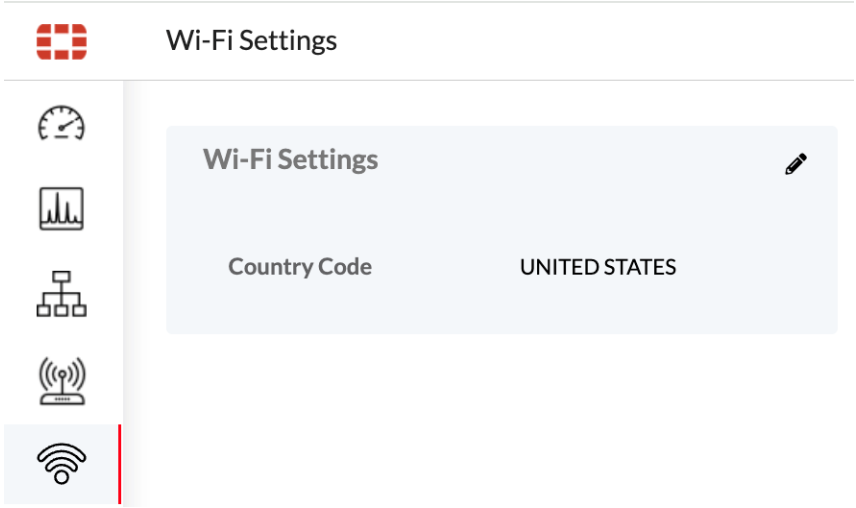
You can set the geographical location of your device using the FortiExtender software Console or GUI.

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) with `wlan-bridge` set to `yes`.

```
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:

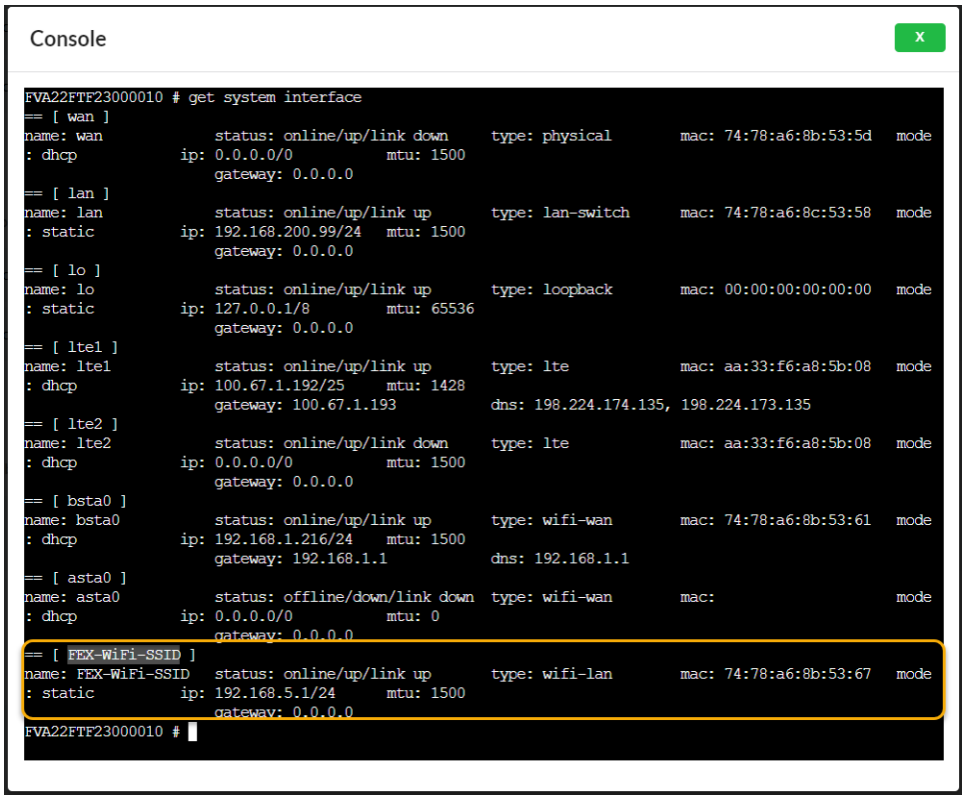
```
FXW51GS224000030 # config network address
FXW51GS224000030 (address) # edit FEX-WiFi-SSID
    set type ipmask
    set subnet 192.168.5.0/24
next
```

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

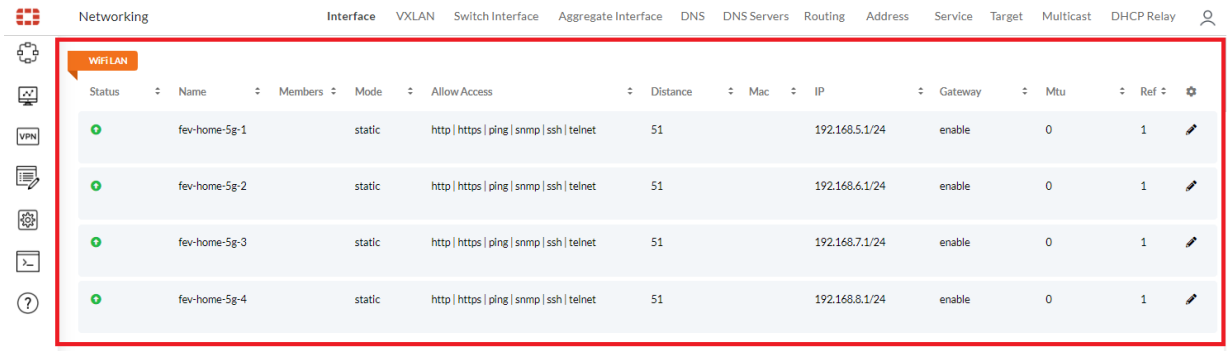
```
FXW51GS224000030 # config firewall policy
FXW51GS224000030 (policy) # edit FEX-WiFi-SSID
    set srcintf any
    set dstintf any
    set srcaddr FEX-WiFi-SSID
    set dnat disable
    set dstaddr all
    set action accept
    set status enable
    set service ALL
```

```
    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:

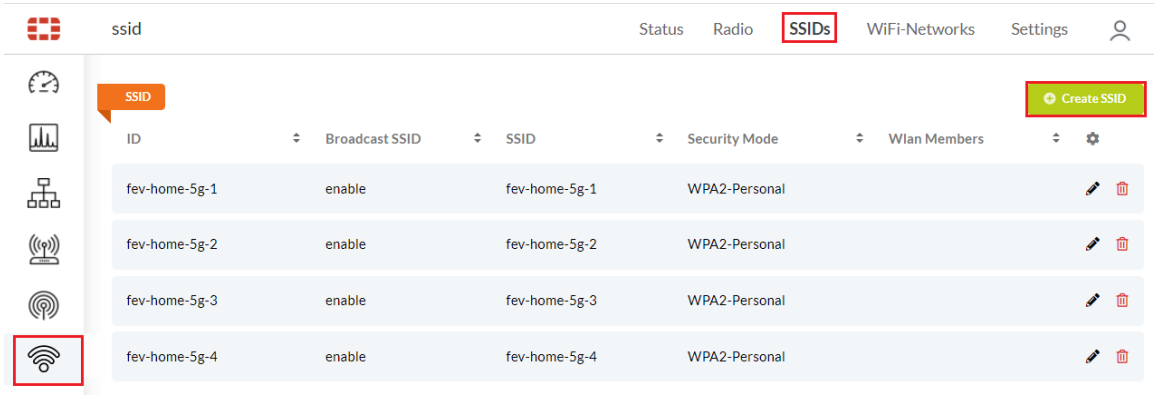


   c. Alternatively, you can check the status of the LAN interface using the *Networking* tab on the GUI, as shown in the following:

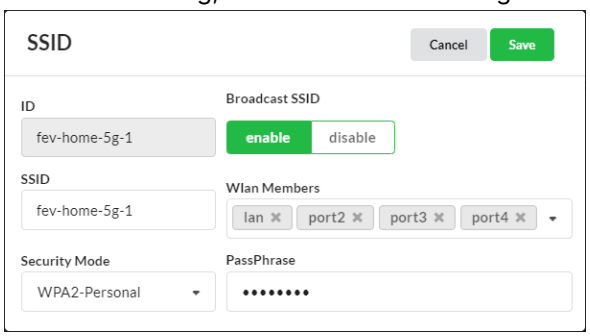


To configure FortiExtender in AP mode - GUI

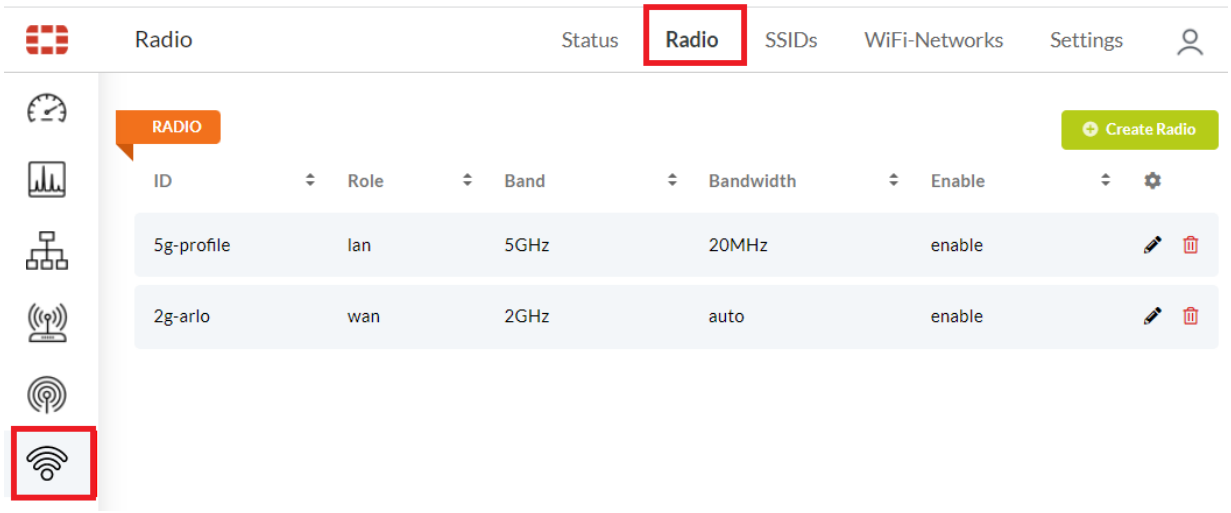
1. Create an SSID for the AP.
   a. Go to *WiFi* > *SSIDs* > *Create SSID*.



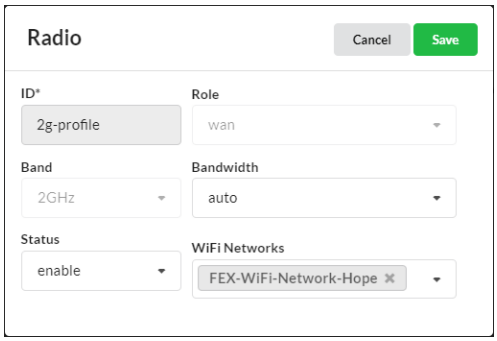
   b. In the SSID dialog, make the desired configurations or selections, as shown in the following:



   c. Click *Save*.
2. Associate the SSID with a Radio profile.
   a. Go to *WiFi* > *Radio* > *Create Radio*.



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

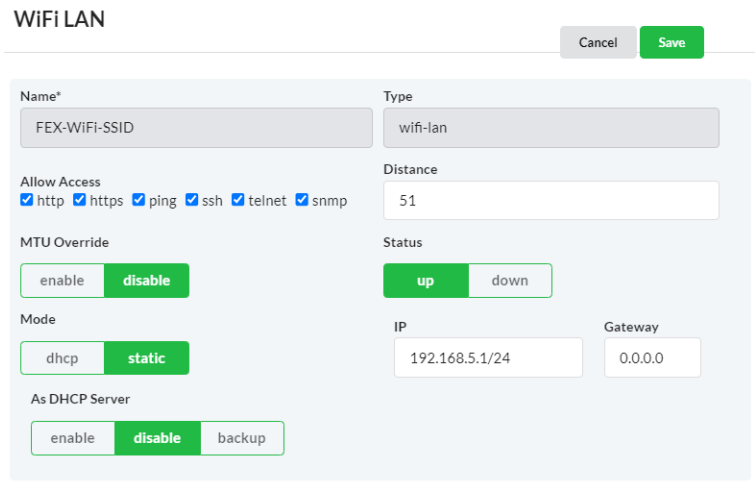


c. Click *Save*

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.



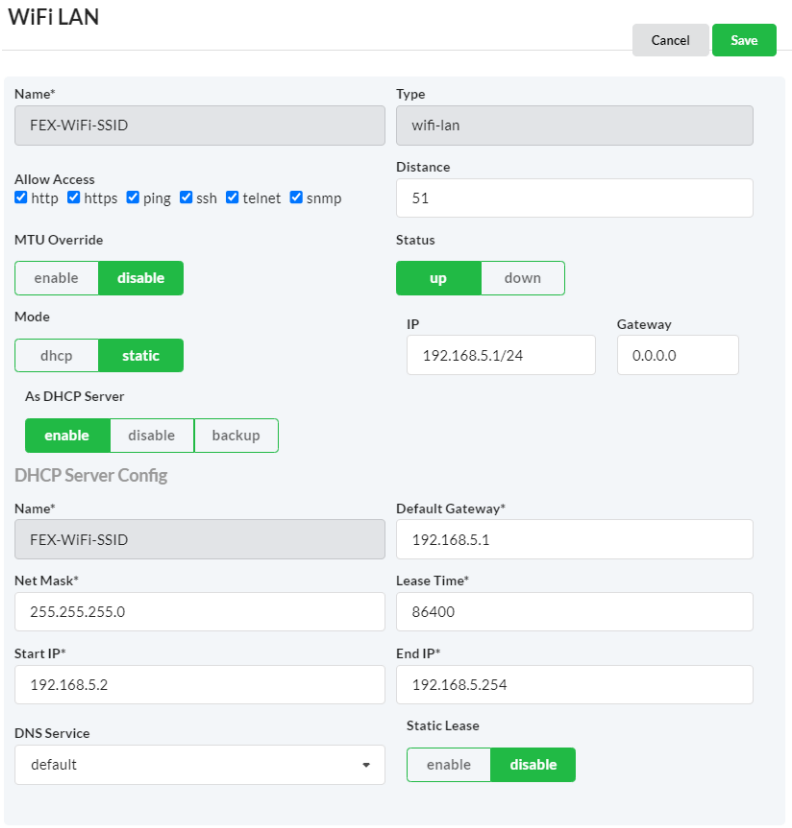
c. Click *OK*

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 the click *Edit*.

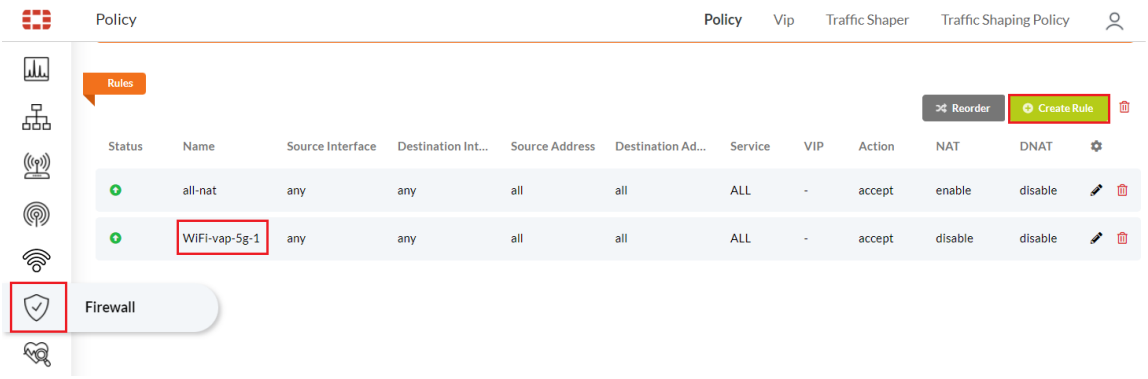
c. In the *WiFi LAN* dialog, make the desired configurations or selections.



d. Click *Save*.

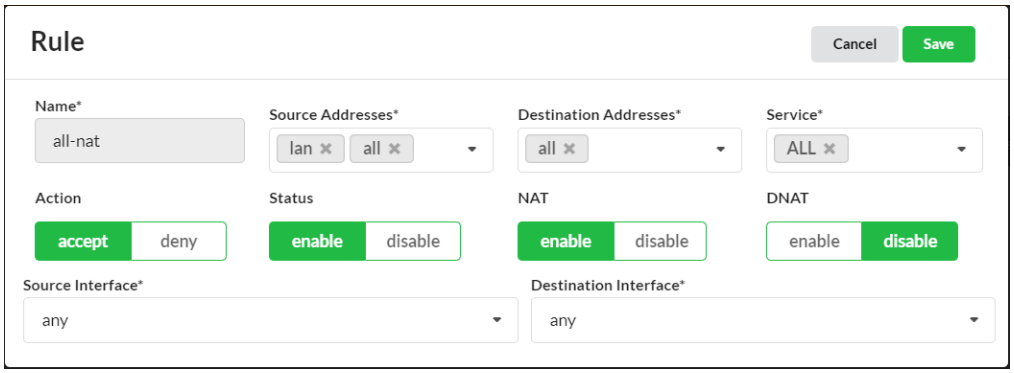
5. Configure a firewall policy for the VAP LAN interface. There are two methods of configuring.

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

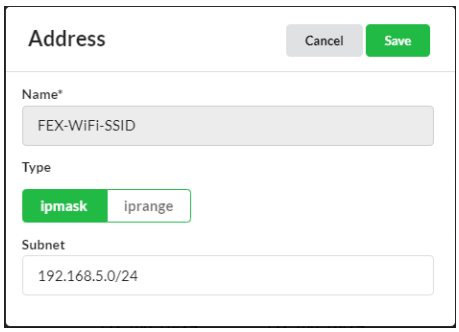


  - **ii.** Select *Create Rule*.

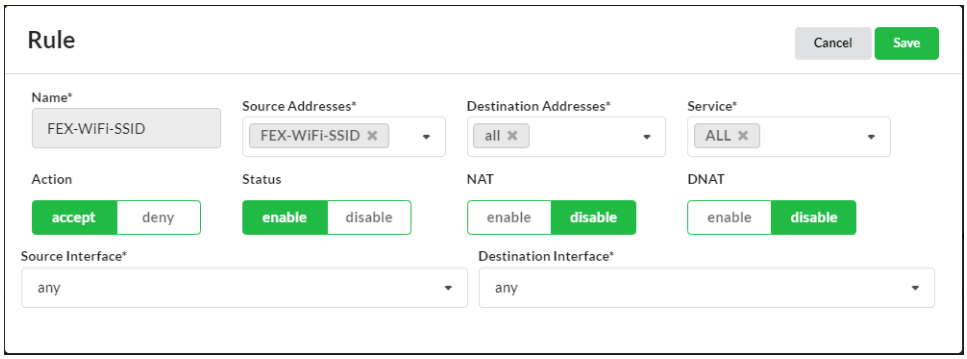
iii. In the *Rule* dialog, make the selections, and click *Save*.



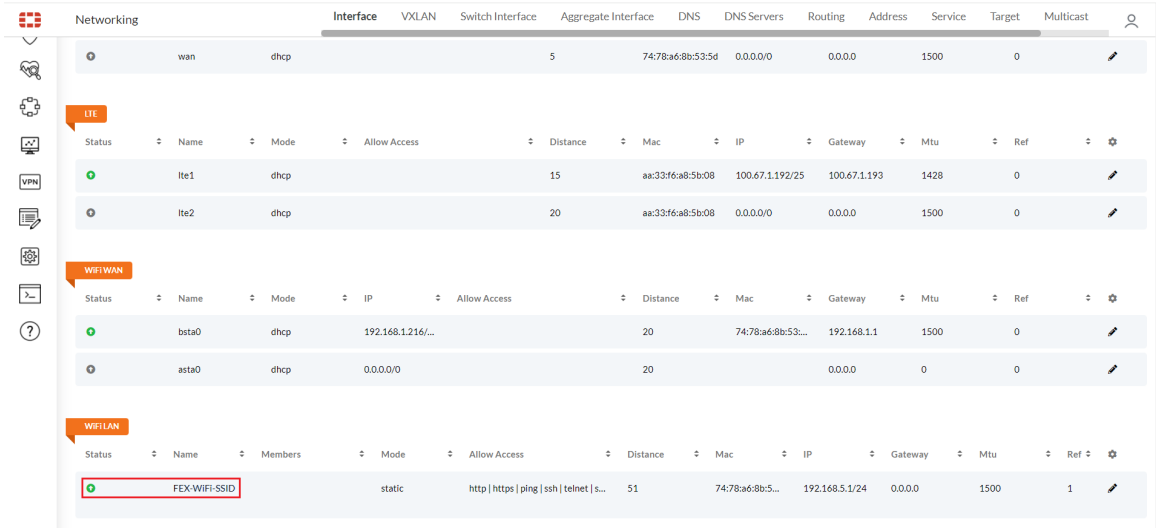
- Option 2: Add additional Firewall Policy to allow traffic via the Wi-Fi LAN interface.
  i. Add the IP address of the Wi-Fi LAN interface by selecting *Networking* > *Address* > *Create Address* from the main menu.



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



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 Wi-Fi APs as members of switch interface

The FortiExtender configuration schema for the system switch-interface supports adding Wi-Fi Virtual Access Points (VAPs) as members of a switch-interface. VAPs can be added as members of a switch-interface as long as they are *not* specified as a WLAN bridge. In so doing, the VAP shares DHCP servers and firewall policies with the switch-interface.

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

To add a FortiExtender Wi-Fi VAP as member of a switch interface:

1. From the FortiExtender, create a virtual access point (VAP), with `wlan-bridge` set to no.

```
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.

```
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.

```
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
vap3                vap3                aap1
```

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:

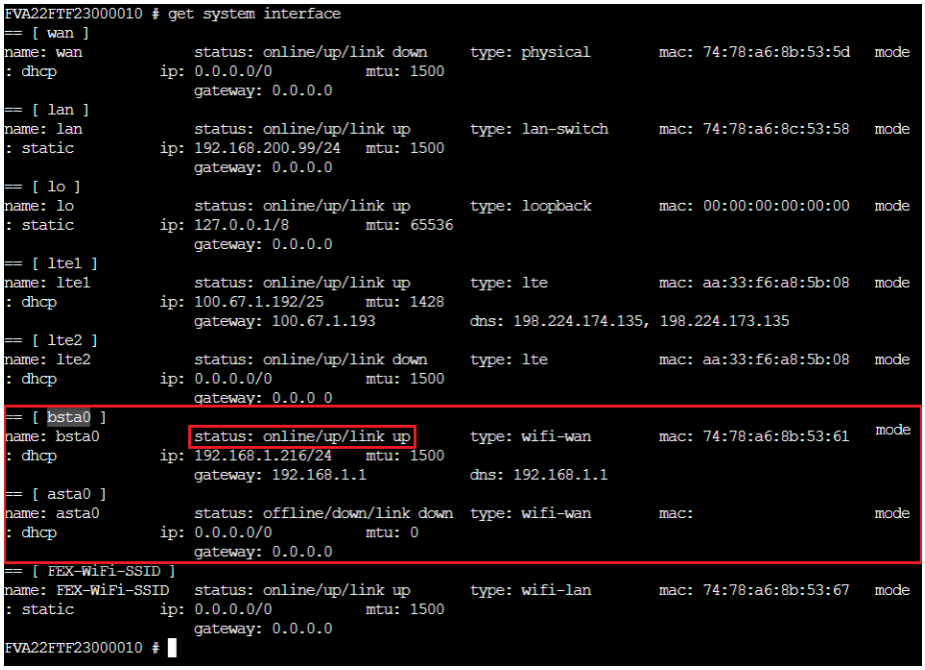
```
FXW51GS224000030 (FEX-WiFi-Network-Hope) <M> # show
edit FEX-WiFi-Network-Hope
    set ssid Hope
    set security-mode WPA2-Personal
    set pmf
    set passphrase ******
next
```

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
```

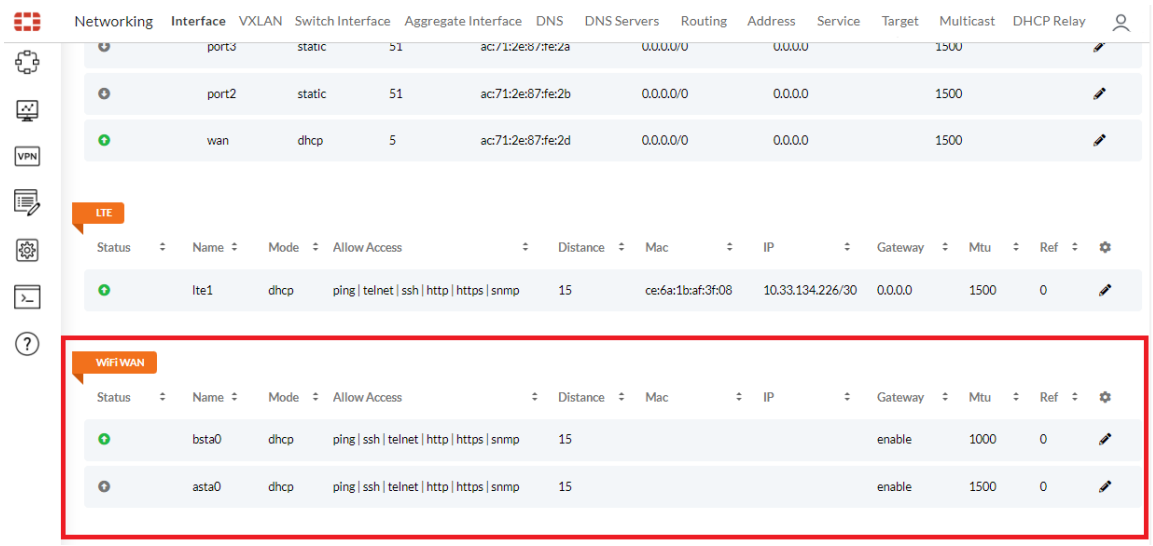
Because your FortiExtender is configured as a Wi-Fi station (in Step 1) which will be using services provided by an existing WAN, make sure that you set its `role` to `wan`.

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:



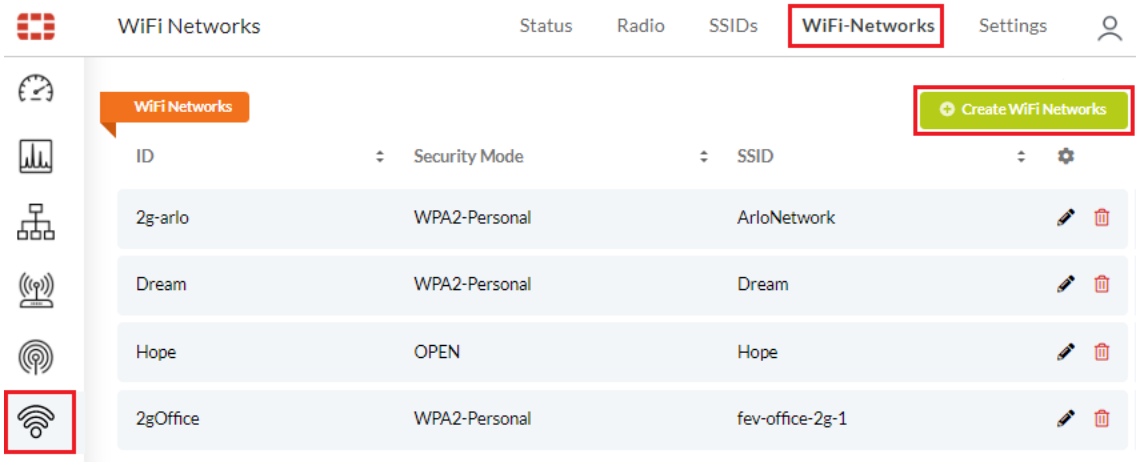
Some FortiExtender models have two embedded Wi-Fi interfaces: `asta0` and `bsta0`. `asta0` is for the 5 GHz band, and `bsta0` is for the 2.4 GHz band.

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

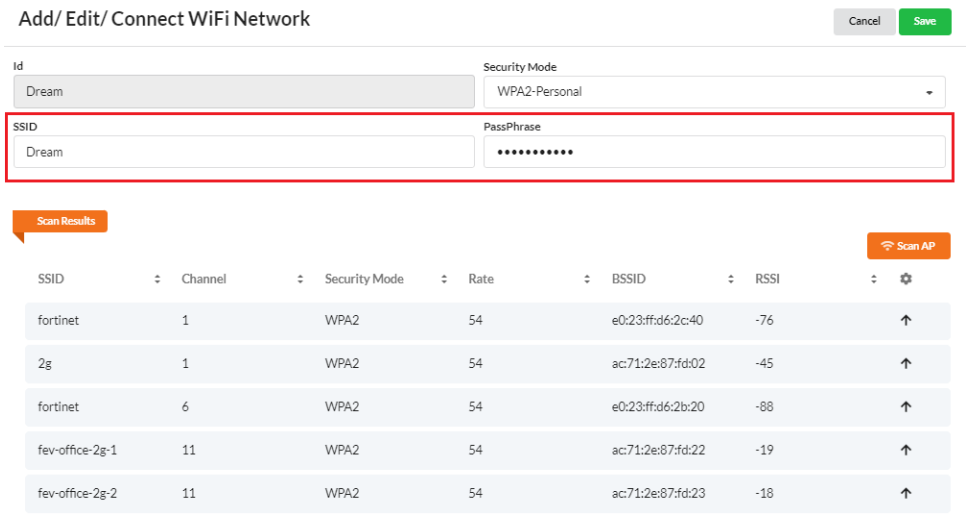


To configure FortiExtender as a Wi-Fi station - GUI:

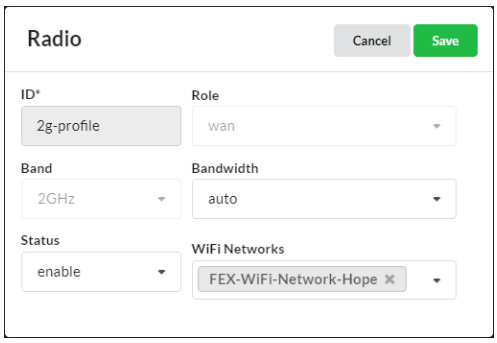
1. Create a Wi-Fi network (SSID).
   a. From the FortiExtender GUI, go to *WiFi* > *WiFi Networks* and click *Create WiFi Networks*.



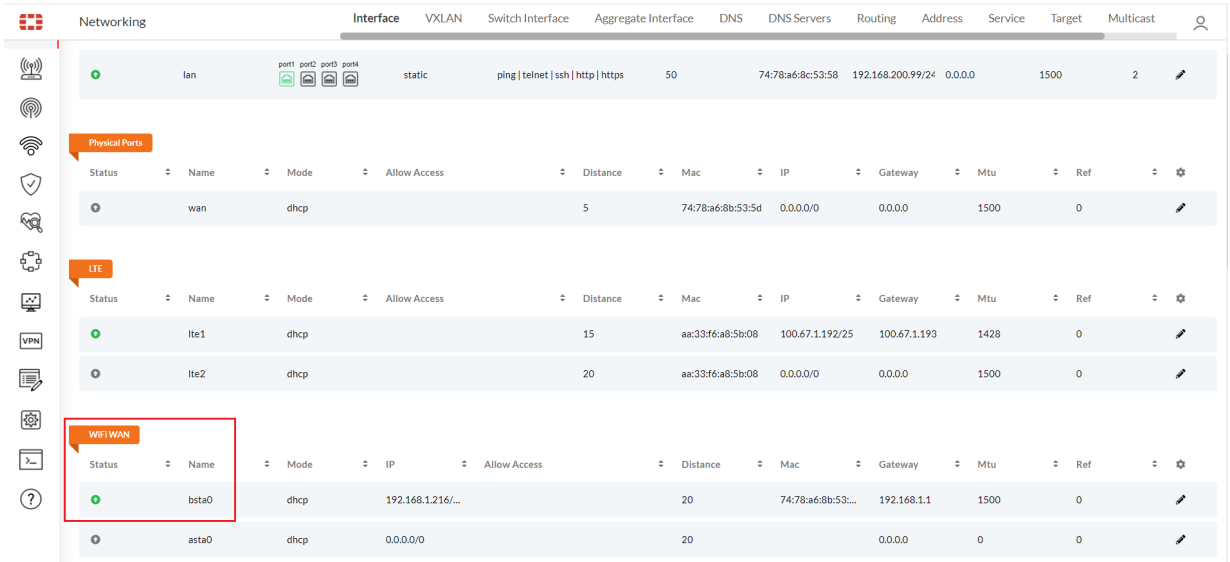
   b. In the *Add/Edit/Connect WiFi Network* dialog, create the Wi-Fi network with an SSID and password.



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*.



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



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 136
- Wired 802.1X authentication on page 140

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 fortinet.com
    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
    set source-ip 1.1.1.4
  next
end
```

2. Apply the RADIUS server table to a user group. You can apply multiple RADIUS server tables to a user group.

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

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. **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.

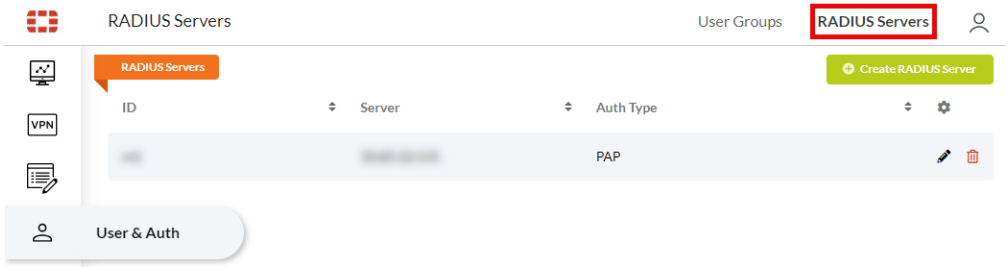
4. Verify that the RADIUS server connection is successful.

```
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

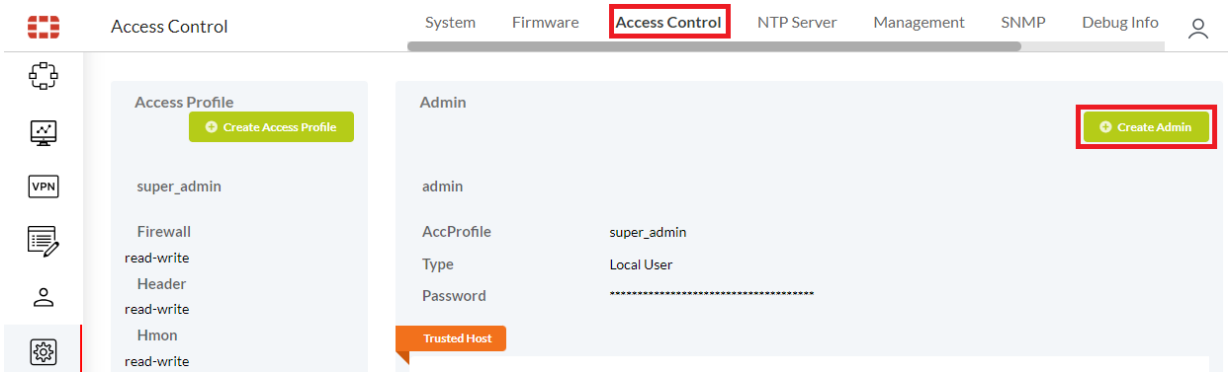
1. Configure the FortiExtender to access a RADIUS server.
   a. From the FortiExtender GUI, go to *User & Auth* and select the *RADIUS Servers* tab.



   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.

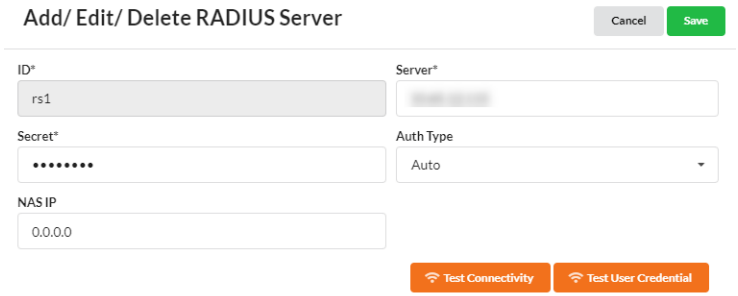
a. Go to *Settings* > *Access Control* and select *Create Admin* or edit an existing Admin profile.



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.



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
```

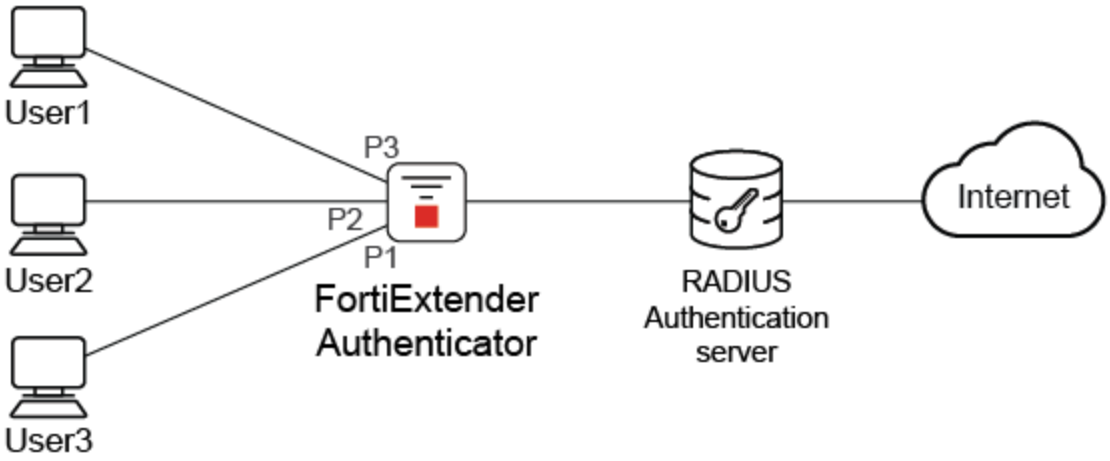
- Use the `get dnsproxy stats` command to check the statistics of DNS cache:

```
# 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	40 supplicants per FortiExtender.	GUI: Under the LAN Switch menu.

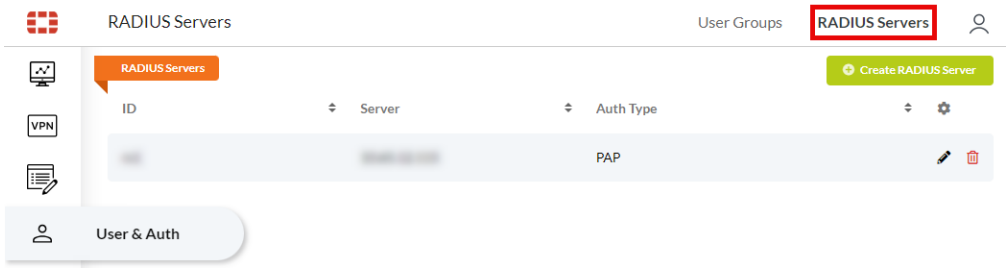
Platform	Models	Supplicant capacity	Configuration method
	FEV-212F-AM FEV-212F		CLI: Under `config system lan-switch`.
Branch	FBS-10F-WIFI FBS-20G FBS-20G-WIFI FER-511G FEXT-511G FEXT-511G-WIFI	8 supplicants for each port.	GUI: Under the Switch Interface menu. CLI: Under `config system switch-interface`.

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

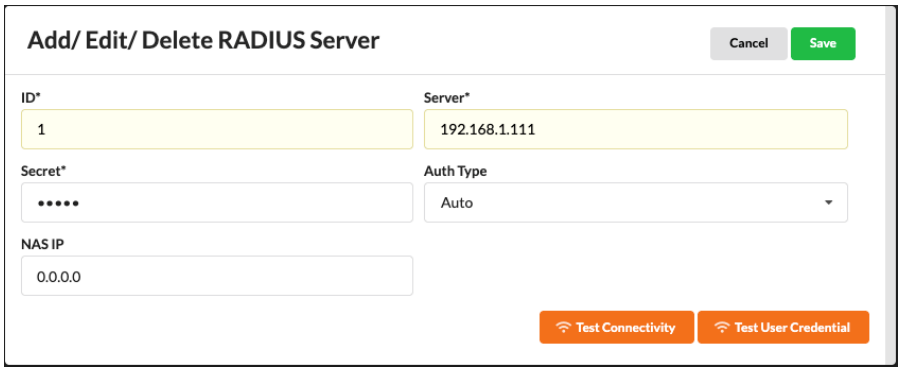
1. Configure a RADIUS User.
2. Configure a User Group.
3. Enable 802.1X authentication and assign the User Group to the appropriate interface depending on the FortiExtender platform type.
4. Optionally, disable 802.1X authentication on individual ports.

To configure a RADIUS User and User Group - GUI:

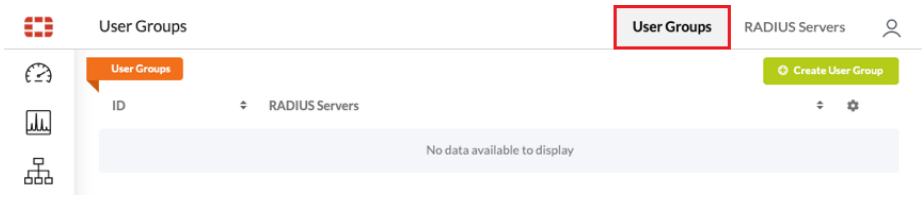
1. From the FortiExtender GUI, go to *User & Auth* and select the *RADIUS Servers* tab.



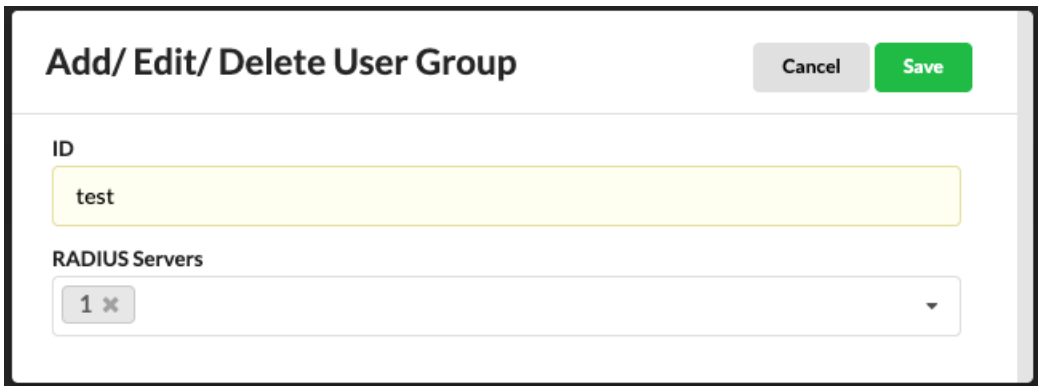
2. Click *Create RADIUS Server* and enter your RADIUS server information.



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.

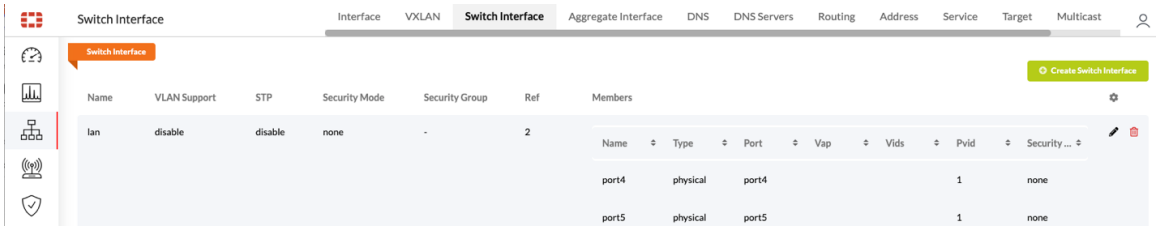


When you apply a user group to the wired 802.1X authentication, the RADIUS servers in this group are limited to four, with the first serving as the primary server and the rest as secondary servers.

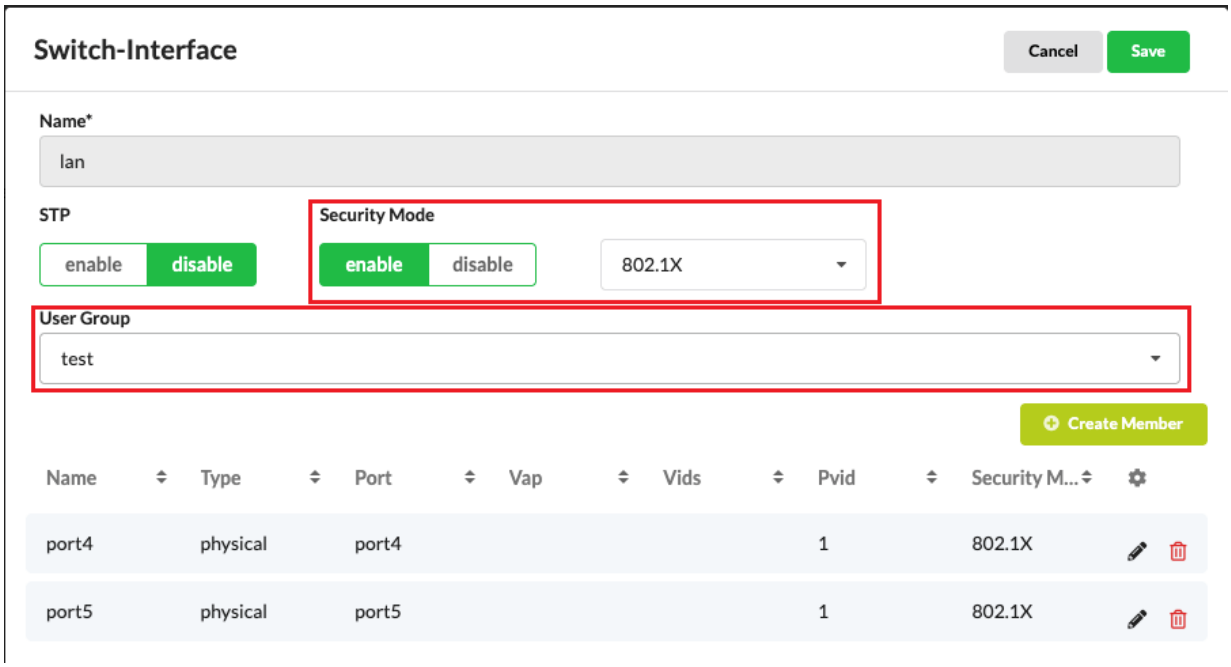
6. When you are finished, click *Save*.

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

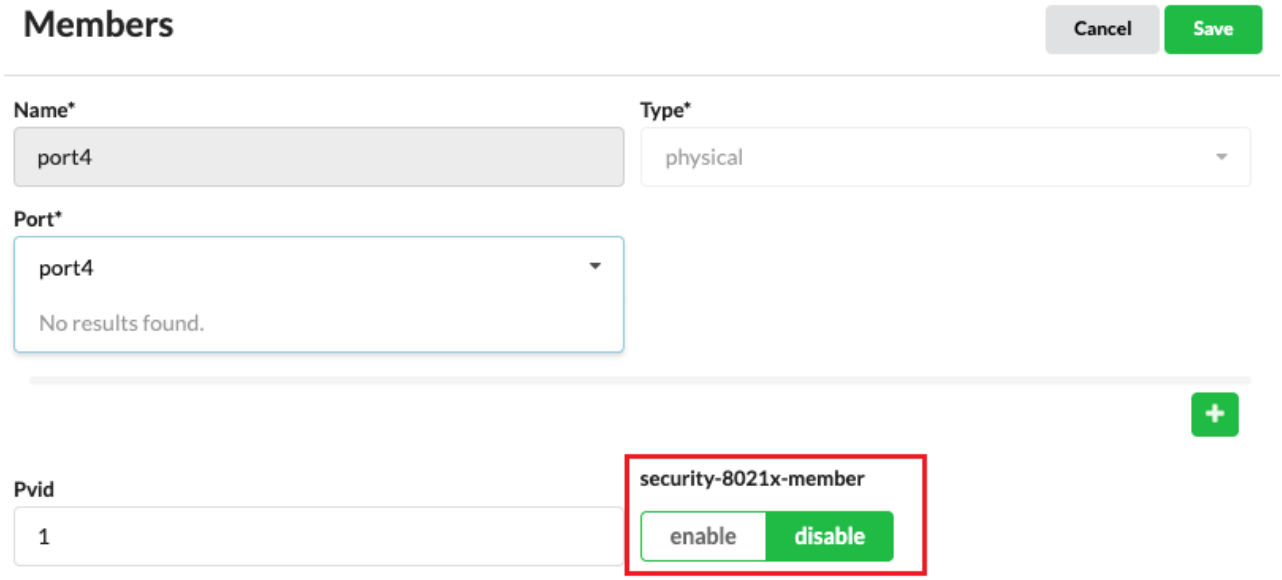
1. From the FortiExtender GUI, go to *Networking* and select the *Switch Interface* tab.



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



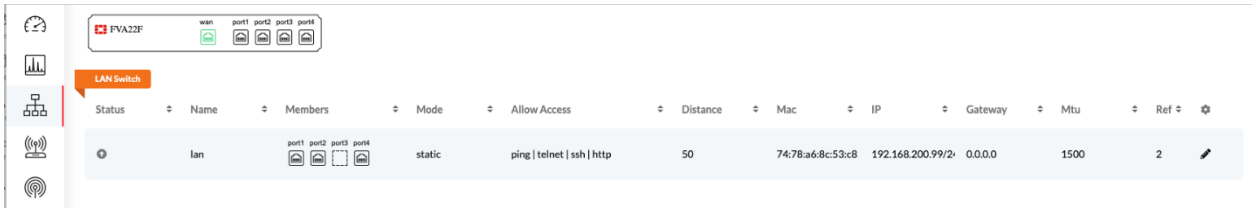
4. If you want to disable 802.1X authentication on a specific port, click *Edit* to edit that port and then disable *security-8021x-member*.



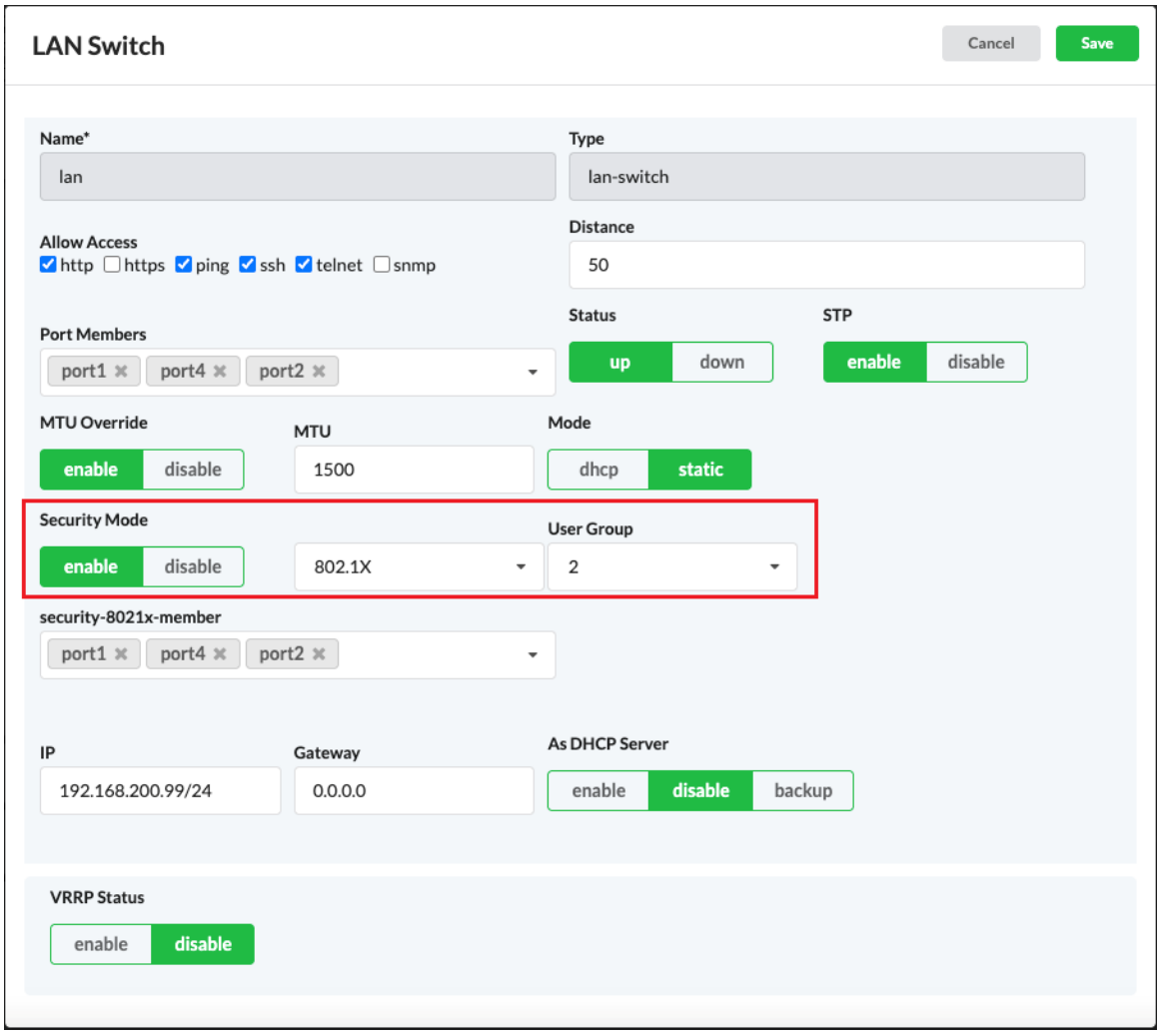
5. When you are finished, click *Save*.

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

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



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



   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 147
- Perform link health check on page 148
- Configure health monitoring on page 150

Monitor interface status

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

CLI Command	Description
`*set interface <interface_name>`	Specify the interface to be monitored.
`set interval`	Specify the monitoring interval in seconds. The valid range is 1–3600. The default is 30.
`set filter {rx_bytes | tx_bytes | rx_packets | tx_packets | rx_dropped | tx_dropped | rx_bps | tx_bps | rx_pps | tx_pps}`	Set the monitor filters on the interface: • `rx_bytes`—The number of bytes received. • `tx_bytes`—The number of bytes transmitted . • `rx_packets`—The number of packets received. • `tx_packets`—The number of packets transmitted. • `rx_dropped`—The number of incoming packets dropped. • `tx_dropped`—The number of outgoing packets dropped. • `rx_bps`—The number of bytes received per second. • `tx_bps`—The number of bytes transmitted per second. • `rx_pps`—The number of packets received per second. • `tx_pps`—The number of packets transmitted per second.

Example interface monitoring configuration:

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

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

You can monitor the aforementioned configuration using the following commands:

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

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

Perform link health check

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

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

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

Paramerter	Descriptions
`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.

Paramerter	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 interfce
        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 interfce
        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
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>
```

Logs

FortiExtender logs various system events in the Logs page. You can find logs for System, Controller, Configuration, LTE, VPN, Aggregate, VWAN, Backup, and Multicast events separated into their respective tabs.

FortiExtender logs are saved locally with a size limit of 2MB. Complete logs are stored with the debugging info and can be downloaded through the GUI or using TFTP (see Collect complete diagnostics information on page 197).

To view FortiExtender logs - GUI:

1. From the FortiExtender GUI, go to *Logs*, and select the log category type you want to view.
2. You can click on a logged event to see more details about it.

System management

This section covers the following system management related topics:

- Add trusted hosts on page 153
- Activate the default admin account on page 154
- Configuration backups and restore on page 155
- Multiple static access controller addresses or FQDN on page 157
- Get user session status and force log-out on page 158
- Upgrade OS firmware on page 159
- Upgrade modem firmware on page 160
- SMS notification on page 161
- Remote diagnostics via SMS on page 162
- Configure the system syslog on page 163
- Support for SNMP (read-only) and traps on page 164
- Get MIB2 interface statistics via SNMP on page 166
- Access other devices via SSH on page 167
- Entity certificates in FortiExtender on page 167
- Automation stitching in digital I/O ports on page 171
- Configure Bluetooth Low Energy on page 180

Add trusted hosts

You can add trusted hosts so that administrators of the hosts can connect to the FortiExtender device through 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:

```
config system admin
  edit admin
    set accprofile super_admin
    set password ENC $5$Ht4I..iMtoqzQdJn$tA/wEHn8yAs8Ap19pcBrYE6O92jEI9OnDSY6Y/ujJ9B
    set trusthost1 192.168.1.115
    set trusthost2
    set trusthost3 192.168.2.0/24
    set trusthost4
```

```
  next
end
```

Parameter	Description
edit <usernaem>	Specify the admin username.
set accprofile	Specify the access profile name.
set password	Specify the admin user password.
set trusthost1	Specify the IPv4 address or subnet address/netmask of the host from which the administrator connects to the device.
set trusthost2	See "trusthost1" above.
set trusthost3	See "trusthost1" above.
set trusthost4	See "trusthost1" above.
set trusthost5	See "trusthost1" above.
set trusthost6	See "trusthost1" above.
set trusthost7	See "trusthost1" above.
set trusthost8	See "trusthost1" above.
set trusthost9	See "trusthost1" above.
set trusthost10	See "trusthost1" above.

Activate the default admin account

In previous versions of FortiExtender, the admin user account may be hidden. You can activate and make the admin user account visible so that you can edit or remove it using the edit or delete configuration operations.

To activate the hidden default admin account:

```
config system admin
  edit admin
    set accprofile super_admin
    set password ENC $5$Ht4I..iMtoqzQdJn$tA/wEHn8yAs8Ap19pcBrYE6O92jEI9OnDSY6Y/ujJ9B
    set trusthost1
    set trusthost2
    set trusthost3
    ...
  next
end
```

Configuration backups and restore

Once you configure a FortiExtender, it is extremely important that you back up the configuration. In certain situations, you may need to reset the FortiExtender to factory defaults, which will erase the existing configuration. In these instances, you can use a backup file to restore your configurations.

FortiExtender configuration backups are saved in JSON format that can be encrypted using AES-256.

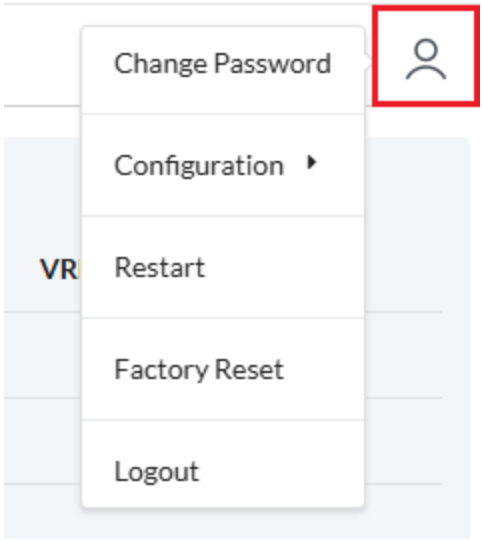
You can choose to secure the encrypted file by setting your own password, or by using the default password.

- If you set your own password, you must re-enter it when you restore the configuration.
- If you use the default password, FortiExtender automatically recognizes the configuration file.

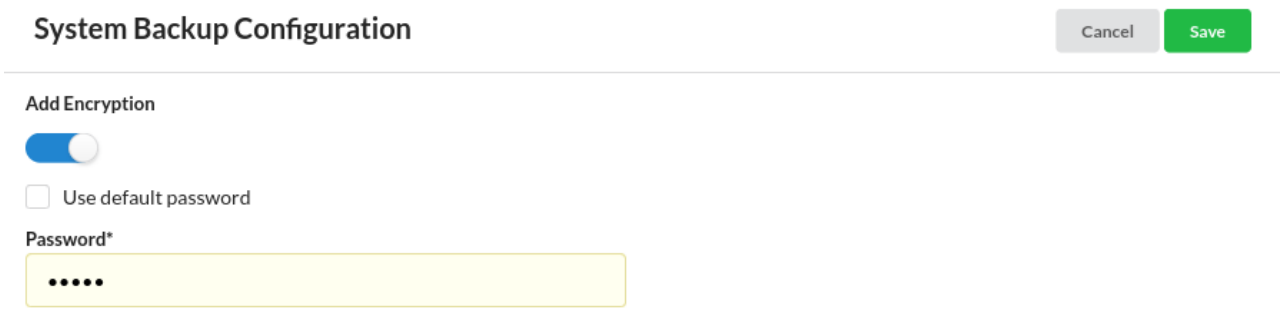
Once you create the configuration files, you can then restore your configurations by importing them back to FortiExtender.

To create a configuration backup - GUI

1. From the FortiExtender GUI, go to *Dashboard* and click the *Profile* icon.



2. Select *Configuration* > *Backup*.



3. Optionally, enable *Add Encryption* and select if you want to *Use default password* or enter your own *password*.

4. When you are finished, click *Save*.
   FortiExtender prompts you to save the configuration file.

To create a configuration backup - CLI

Enter the following command:

```
# execute config backup tftp [remote_file] [tftp_server] [encrypt] [encrypt_password]
```

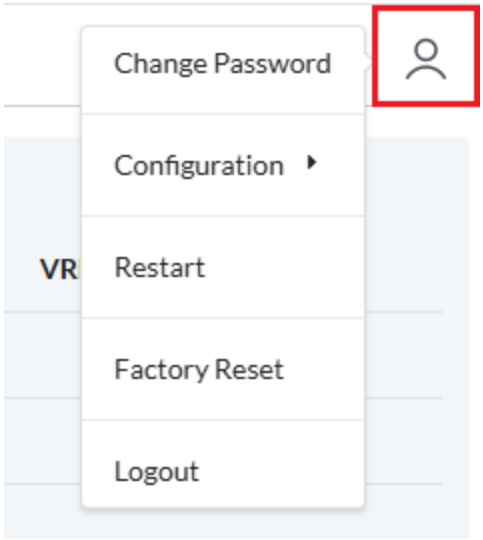
Note: `encrypt_password` is an optional field, but if you do not define a password, FortiExtender will use the default password option.

Example configuration backup command:

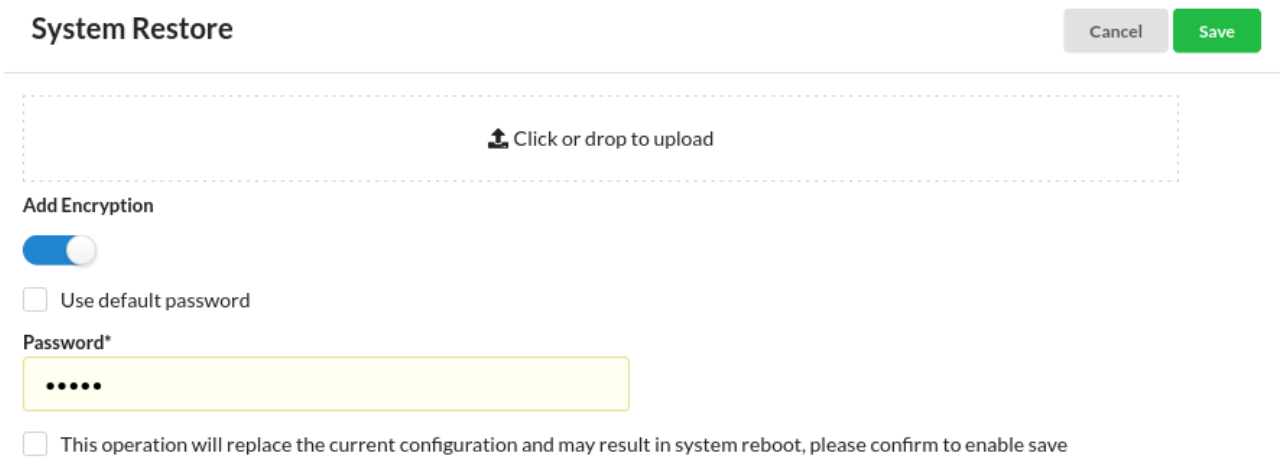
```
# execute config backup tftp fext_cfg 192.168.120.10 encrypt fortinet123
```

To restore a configuration backup - GUI

1. From the FortiExtender GUI, go to *Dashboard* and click the *Profile* icon.



2. Select *Configuration* > *Restore*.



3. Click or drop your saved configuration file to upload the image.
4. If the file is encrypted, enable *Add Encryption*.
5. Select which password you set.
   - If you used the default password, select *Use default password*.
   - If you set your own password, enter your password.
6. When you are finished, click *Save*.
   FortiExtender restores the configurations from the file, replacing your current configurations.

To restore a configuration backup - CLI

Enter the following command:

```
# config restore tftp [remote_file] [tftp_server] [encrypt] [decrypt_password]
```

Note: `encrypt_password` is an optional field, but if you do not define a password, FortiExtender will use the default password option.

Example configuration backup command:

```
# execute config restore tftp config_FXA11FTQ21000154_2025-08-26-18105_json_encrypted encrypt
```

Multiple static access controller addresses or FQDN

FortiExtender enables you to specify multiple access controllers while `ac-discovery-type` is static, and to specify the Fully Qualified Domain Name address (FQDN).

The `static-ac-ip-addr` in pre-7.0.2 releases has 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 in an FQDN string or IPv4-address string format.

If `static-ac-ip-addr` was specified in a pre-7.0.2 version of ForitExtender and upgraded to 7.0.2 or later, an entry "1" will be automatically generated and its `server` value will be the string configured in `static-ac-ip-addr` from the old version.

To configure multiple static access controller or FQDN:

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

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 users to log out:

```
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.

The FortiExtender firmware for 7.6.4 and later is digitally signed using a SHA-256 signature, which is verified before the upgrade process. If the firmware lacks the valid signature, the upgrade will be aborted. Downgrading to an earlier firmware is still supported.

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 not supported on models that use Quectel modems.

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 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 diagnosis is not supported on models that use Quectel modems.

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
    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.

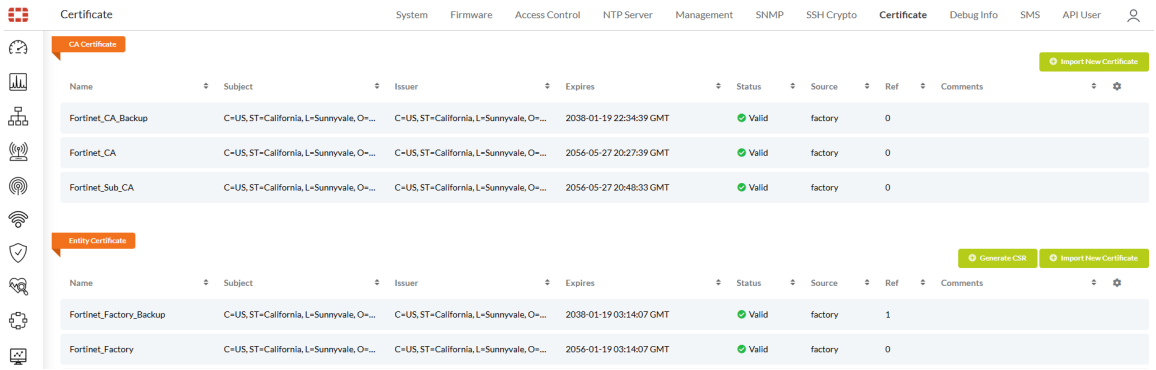
- If the certificate is approved, the CSR status changes from *pending* to *valid*.
- If the certificate is still pending approval after one minute, FortiExtender waits for twice the previous waiting time before checking again.
- If the waiting time exceeds 24 hours, the request is dropped. When a CSR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

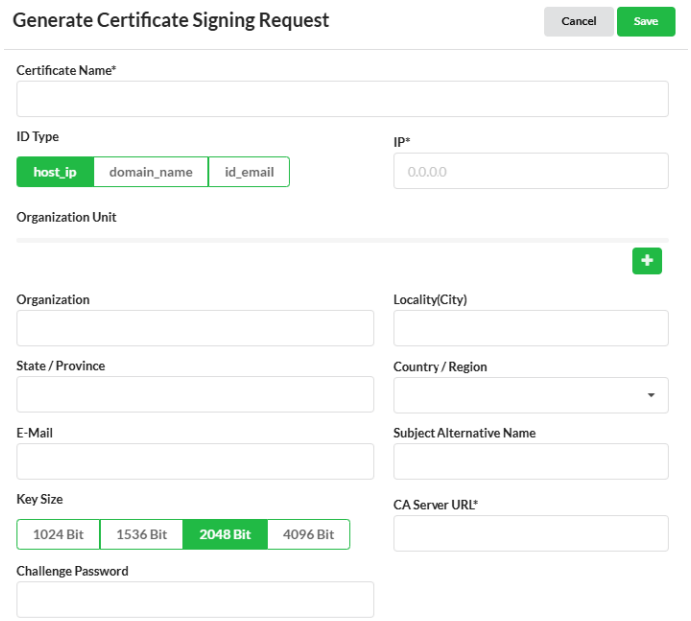
FortiExtender supports an *http* connection to the SCEP server.

To generate a CSR - GUI:

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



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



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	
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*.

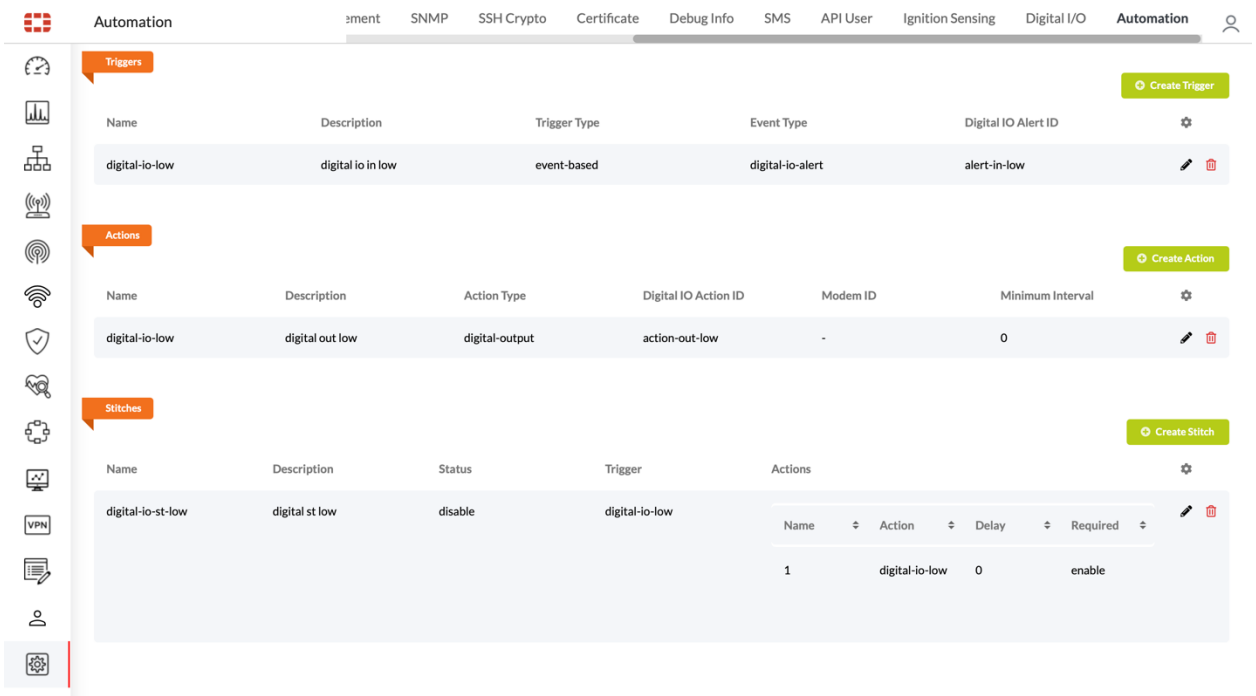
- The *trigger* is the condition or event on the FortiExtender that activates the action.
- The *action* is what the FortiExtender does in response to the trigger.

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.



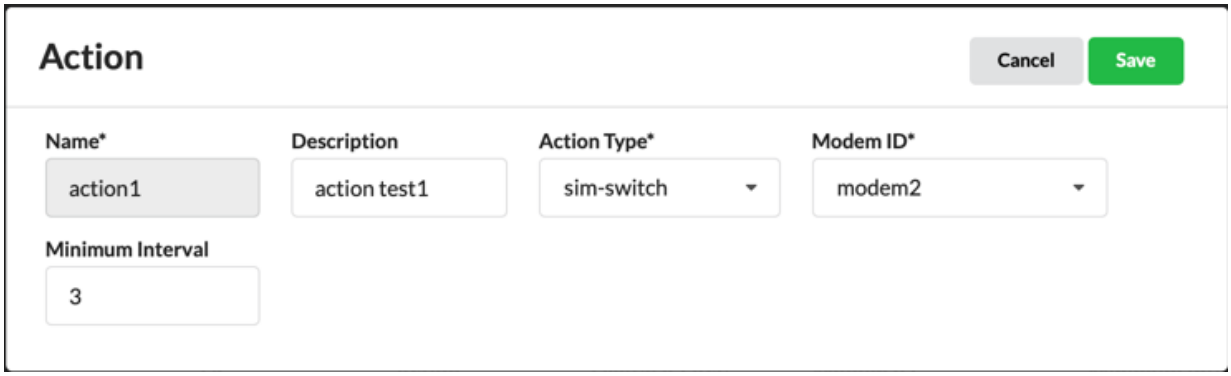
2. Automation stitches, actions, and triggers are configured in the separate dialogs. Click on each dialog to create either a trigger, action, or automation stitch.
   a. Click *Create Trigger* to create a trigger. To modify an existing trigger, click the edit icon.

i. Complete the following fields:

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

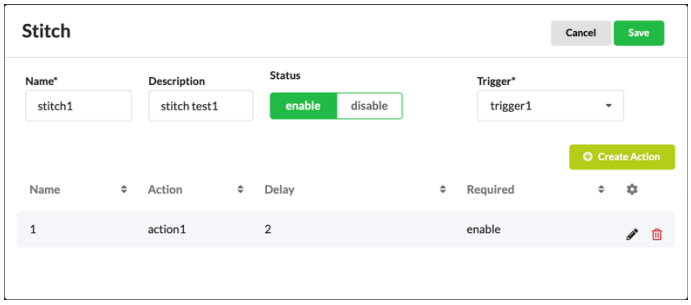


i. Complete the following fields:

Action fields	Description
Name	Enter a name for the automation action.
Description	Describe the automation action.
Action Type	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.
Digital IO Action ID	If *Action Type* is set to *digital-output*, you must configure a digital I/O action ID
Modem ID	If Action Type is set to *sim-switch* or *modem-reset*, you must configure a modem ID.
Minimum Interval	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.



i. Complete the following fields:

Stitch fields	Description
Name	Enter a name for the automation stitch.
Description	Describe the automation stitch.
Status	Enable or disable the automation stitch.
Trigger	Select the name of the trigger for this automation stitch.
Create Action	Click to create actions.
Name	Enter a name for the stitch action.
Action	Select the name of the action configuration for this automation stitch.
Delay	Set the delay before execution (in seconds)
Required	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 177).

```
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`.

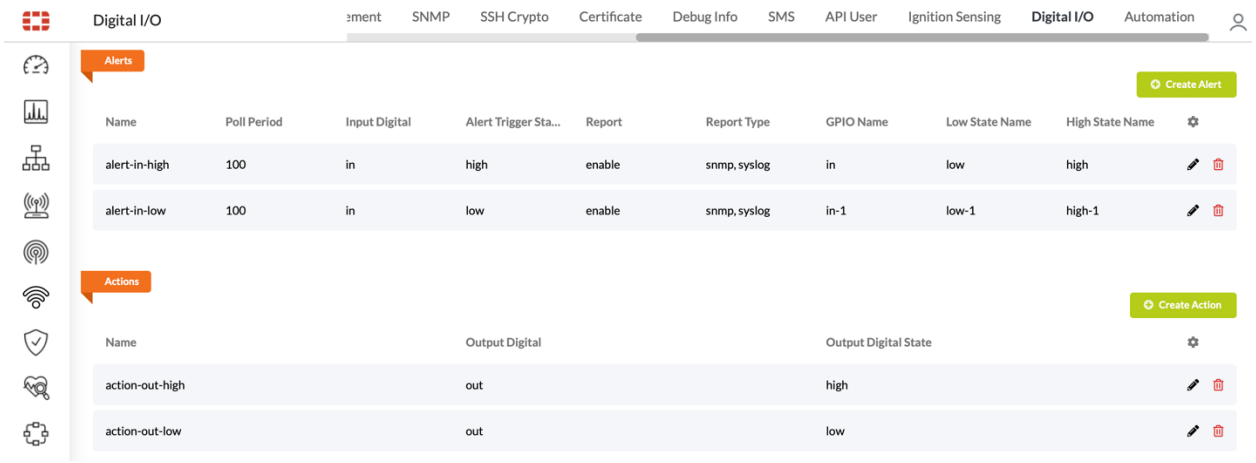
```
config system automation trigger
  edit digital-io-low
    set description digital io in low
    set trigger-type event-based
    set event-type digital-io-alert
    set digital-io-alert-id alert-in-low
  next
end
```

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

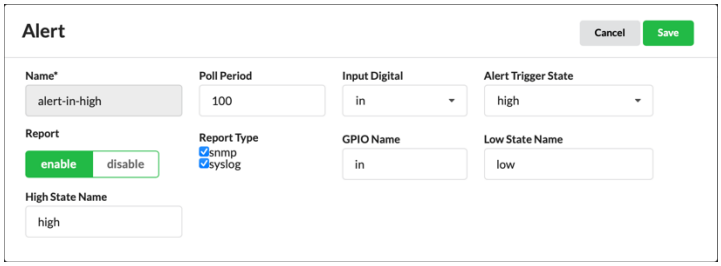
```
config system automation action
  edit digital-io-low
    set description digital out low
    set action-type digital-output
    set digital-io-action-id action-out-low
    set minimum-interval 0
  next
end
```

To configure digital I/O port functions - GUI:

1. From the FortiExtender GUI, go to *Setting* > *Digital I/O*.
   The FortiExtender Digital I/O tab loads.



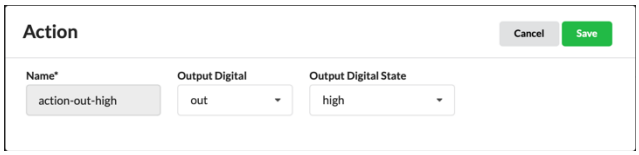
2. Digital I/O alerts and actions are configured in the separate dialogs. Click on each dialog to create either an alert or action.
   a. Click *Create Alert* to create an alert. To modify an existing alert, click the edit icon.



      i. Complete the following fields:

Stitch fields	Description
Name	Enter a name for the digital I/O alert.
Poll Period	The interval between general-purpose I/O (GPIO) status checks, in milliseconds.
Input Digital	Select a digital name
Alert Trigger State	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.
Report	Enable or disable reporting.
Report Type	Select a report type.
GPIO Name	The GPIO name that will be generated in the report log.
Low State Name	The low state name that will be generated in the report log.
High State Name	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.



i. Complete the following fields:

Stitch fields	Description
Name	Enter a name for the digital I/O action.
Output Digital	Select the name of the digital that will run the alert action on.
Output Digital State	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. The BLE interface can be used for initial provisioning through FortiExplorer Go, for diagnostics, or for recovery.

For more information on using FortiExplorer Go to provision a FortiExtender, refer to the FortiExplorer Go User Guide.

For specific instructions on enabling BLE for your device, refer to the QuickStart Guide that came with your FortiExtender. For most models, 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 the FortiExtender is in pairing mode, the device will "listen" for connection attempts for 90 seconds. If no pairing is completed during that interval, the BLE pairing window ends and the LED turns off.

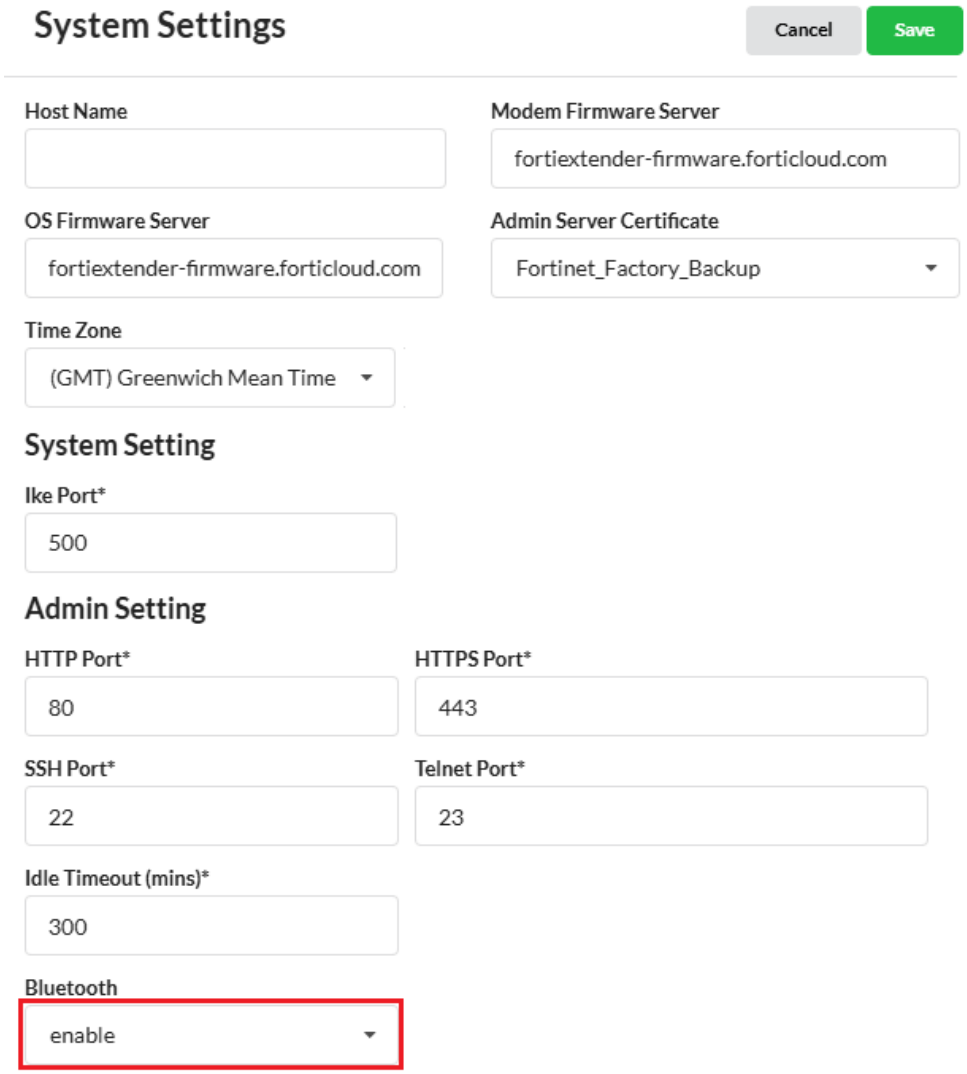
When BLE is active, any nearby device can attempt to connect. By default, the BLE interface is turned off to prevent unauthorized access.

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*.



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

To disable the FortiExtender BLE button - CLI:

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

LTE settings

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

- Add a new carrier profile on page 182
- Add a new operator/carrier on page 182
- Activate a SIM or eSIM on page 185
- Configure start session timeout on page 188
- Managing the SIM card IMSI number on page 189
- Set the default SIM on page 189
- Enable SIM-switch on page 191
- Dual modems on page 193
- Unlock SIM pin on page 194

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 from the FortiExtender:

```
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 1000000).
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 or eSIM

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` command runs 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:

From the FortiExtender CLI, configure the following:

```
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
```

Activate an eSIM

FortiExtender G-series models support eSIM, and requires an active internet service to download an eSIM profile to the FortiExtender. Fortinet recommends using a WAN connection to download as the FortiExtender modem cannot have an active connection while provisioning the eSIM.

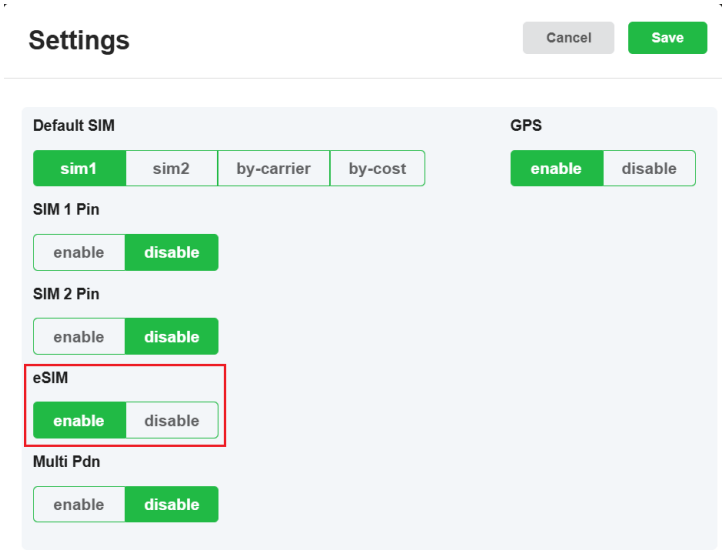
eSIM profiles need to be activated before use, and only one profile may be active at a time. Once the eSIM profile has been added and activated on the FortiExtender, it will replace any physical SIM in SIM slot 2, rendering SIM slot 2 unusable while the eSIM profile is active. Before an eSIM profile can be deleted from a device, it needs to be disabled first.

While FortiExtender supports adding up to four eSIM profiles, only one eSIM profile may be active at a time.

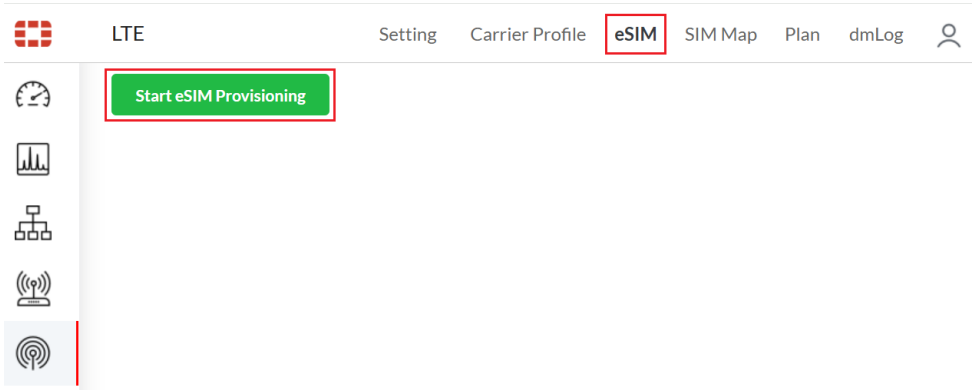
To activate eSIM functionality and download an eSIM profile - GUI:

When you purchase an eSIM, you should receive a URL beginning with LPA from the carrier. This URL is required when adding the eSIM profile.

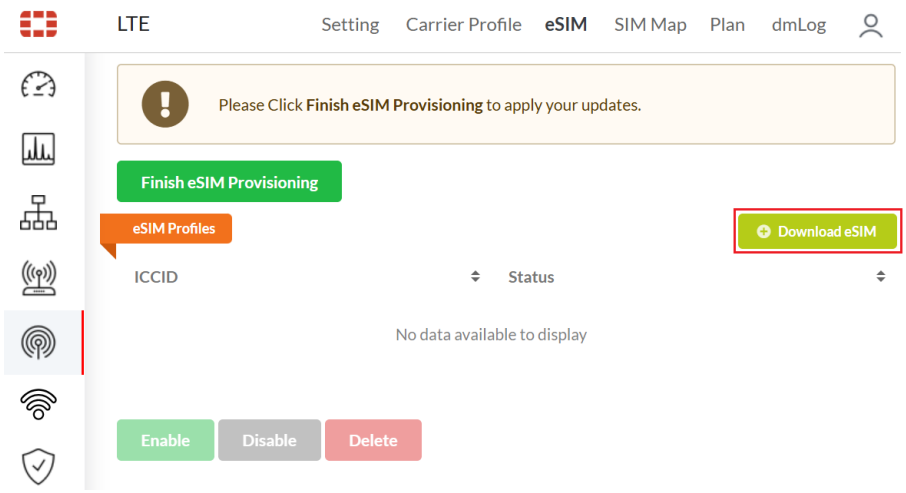
1. From the FortiExtender GUI, go to *LTE* and edit the LTE settings.
2. Within LTE settings, enable *eSIM*.



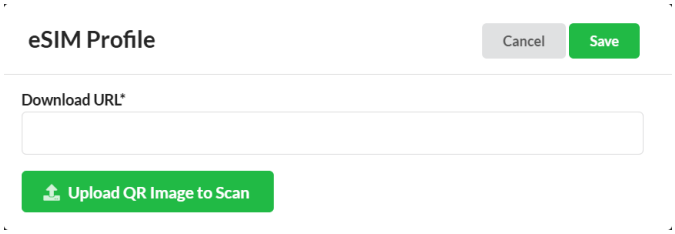
3. Save your changes and then refresh the page; the eSIM tab is available.
4. Navigate to *LTE > eSIM* and then click *Start eSIM Provisioning* to begin adding an eSIM profile.



5. Click *Download eSIM* to download the eSIM profile.



6. Enter the carrier-provided URL or upload a QR code, and then click *Save*.



The download process takes about 30 seconds.

7. Once the eSIM profile has been successfully downloaded, it is added to the list of eSIM profiles, which displays information about the SIM's ICCID and activation status.
8. If the eSIM has not been activated, select *ICCID* and then click *Enable*.
9. When you are finished, click *Finish eSIM Provisioning*.

Once the eSIM has been provisioned with a profile, you can configure the *Default SIM* as sim2 in the LTE modem settings to prioritize that eSIM.

You can configure SIM switching between the currently active eSIM profile and the SIM in the physical SIM slot 1. See Enable SIM-switch on page 191.

To activate eSIM functionality and download an eSIM profile - CLI:

1. From the FortiExtender CLI, set `esim` to `enable` on the modem you want to enable eSIM capability.

```
config lte setting
  config modem1
    set esim enable
  end
end
```

2. After enabling eSIM, you can use the following commands to configure the eSIM:

```
#execute modem modem1
sim1                    sim1 specific operations
sim2                    sim2 specific operations
esim-enable-access      enable access to esim chip
esim-disable-access     disable access to esim chip
esim-details            esim details
esim-display-profile    display stored esim profile numbers
esim-delete-profile     delete the esim with iccid
esim-disable-profile    disable the esim with iccid
esim-enable-profile     enable the esim with iccid
esim-download-profile   download the esim profile from the LPA server
```

- When provisioning your eSIM, you must begin with `execute modem modem1 esim-enable-access`.
- When using CLI commands to download the eSIM profile, you can only use the URL provided by the carrier.
- You can use `execute modem modem1 esim-details` to view the device's EID.
- When you are finished provisioning, you must end with `execute modem modem1 esim-disable-access`.

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
```

Managing the SIM card IMSI number

When a SIM card is activated, FortiExtender records the IMSI number of the card. You can then check the record or remove the IMSI number from the record.

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
```

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 select which default SIM to use. You can use the following criteria to set the default SIM:

- Set the default SIM by preferred carrier on page 190
- Set the default SIM by low cost on page 190
- Set the default SIM by SIM slot on page 190

Set the default SIM by preferred carrier

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

From the FortiExtender CLI, configure the following:

```
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`.

From the FortiExtender CLI, configure the following:

```
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 FortiExtender CLI commands:

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

Enable 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.

You can also force the FortiExtender to immediately switch the inactive SIM to the active SIM using an `execute` command.

You can configure SIM switching between the currently active eSIM profile and the SIM in the physical SIM slot 1. SIM-switch does not switch between eSIM profiles.

To enable SIM-switch:

From the FortiExtender CLI, configure the following:

```
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
```

Parameter	Description
by-disconnect	The SIM card switches when the active card gets disconnected according to the `disconnect-threshold` and `disconnect-period`.
by-signal	The SIM card switches when the signal strength gets weaker than the signal-threshold.
by-data-plan	The SIM card switches when `'capacity'` is overrun and `'overage'` is enabled.
disconnect-threshold	The number (1 —100) of disconnects for SIM switch to take place.
disconnect-period	The evaluation period (600 — 18000) in seconds for SIM switch.
switch-back	Enables switching back to the preferred SIM card.
switch-back-by-time	Switches over to the preferred SIM /carrier at a specified (UTC) time (HH:MM).

Parameter	Description
switch-back-by-timer	Switches over to the preferred SIM/carrier after a given time (3600-2147483647) in seconds.

To force an immediate SIM-switch:

You can immediately switch a modem's inactive SIM to the active SIM. From the FortiExtender CLI, enter the following command:

```
#execute sim-switch [modem1 | modem2]
```

The FortiExtender must have two SIMs for the command to work (or if eSIM is enabled, then an eSIM profile needs to be active). Modem2 is only available if the FortiExtender platform has two modems.

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 194
- Dual modems in NAT mode on page 194

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 39 for Virtual-WAN interface and System routing on page 73 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.

FortiExtender API

The FortiExtender REST API enables you to perform configuration and monitoring operations on a FortiExtender appliance or VM. The following types of REST APIs are supported:

- **Configuration APIs** that retrieve and modify CLI configuration items. For example, create or delete a firewall policy; view or change system settings.
- **Monitor APIs** that retrieve dynamic data and perform system/network operations. For example, restart or shut down a FortiExtender; backup or restore configuration settings.

FEXT-200F does not have any LTE APIs.

For instructions on generating and using an API token and to see the full FortiExtender API scheme, you will need a Fortinet Developer Network account.

Once you have an account, you can access the FortiExtender API documentation.

Troubleshooting, diagnostics, and debugging

For detailed troubleshooting information, refer to the FortiExtender Troubleshooting Guide.

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

- Diagnose from Telnet on page 197
- Collect complete diagnostics information on page 197

Diagnose from Telnet

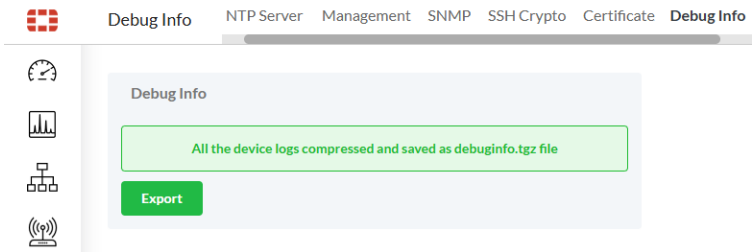
1. From the Windows Command prompt, type `cmd`.
2. Type `telnet [modem ip address]`. (The default IP address is 192.168.200.99/24.)
3. Enter your user name and password as required.
4. Enter the command you want.

Collect complete diagnostics information

FortiExtender 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.

To download diagnostics information - GUI:

1. From the FortiExtender GUI, go to *Settings* > *Debug Info*.



2. Click *Export*.
   All the device logs are compressed and saved as a *debuginfo.tgz* file.

To download diagnostics information - CLI:

Use the following command to collect all diagnostics information:

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

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.