



CLI Reference

FortiExtender 7.6.5



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 13, 2026

FortiExtender 7.6.5 CLI Reference

36-765-1236481-20260213

TABLE OF CONTENTS

Change Log	7
Introduction	8
Connect to the CLI	8
Console connection	8
SSH access	9
Enable SSH access to the CLI using a local console connection:	9
Access the FortiExtender CLI using SSH	10
CLI commands	12
Header	13
config version	13
Firewall	14
config firewall policy	14
config traffic-shaper	18
config shaping-policy	19
config vip	20
LTE	23
config lte setting	23
config carrier	30
config simmap	31
config plan	32
Router	36
config router policy	36
config router policy6	38
config router static	40
config router static6	42
config router target	43
config router target6	44
config multicast	45
config pim-sm-global	45
config rp-address	45
config interface	46
config OSPF	47
config area	48
config network	48
config ospf-interface	49
config redistribute	50
config prefix-list	51
config rule	52
config route-map	53
config rule	53
System	55
config system global	56

config system accprofile	57
config admin	60
config system bluetooth	63
config system management	63
config fortigate	64
config cloud	65
config system management local	66
config local-access	66
config fortigate-backup	67
config system interface	69
config VRRP	73
config ipv6	74
config system vxlan	78
config system aggregate-interface	79
config members	80
config pppoe-interface	81
config system dhcpserver	82
config reserved-address	85
config system dhcp6server	86
config dhcprelay	89
config dns	90
config dns-server	92
config dns-database	93
config dns-entry	94
config vwan-member	96
config sms-notification	99
config receiver	99
config alert	100
config sms-remote-diag	101
config allowed-user	102
config syslog	103
config remote-servers	104
config statistic-report	104
config virtual-wire-pair	107
config api-user	107
config ntp	108
config ntpserver	109
config settings	110
config system lan-switch	110
config system switch-interface	112
config system ipsec	114
config ssh-crypto	114
config system automation trigger	116
config system automation action	117
config system automation stitch	118
config system digital-io digital	120

config system digital-io alert	120
config system digital-io action	122
config system 802-1X-settings	123
config system ignition-sensing	123
config system obm-console	124
SNMP	126
config sysinfo	126
config community	126
config user	129
config hosts	130
HMON	132
config interface-monitoring	132
config hchk	132
VPN	136
config ipsec	136
config phase1-interface	136
config phase2-interface	141
config vpn certificate	146
config vpn certificate ca	146
config vpn certificate local	147
Network	149
config network address	149
config service	150
config service-custom	150
config network address6	151
Execute	153
execute interface dhcpclient-renew	153
execute obm-console	153
execute SSH username serverip	154
execute vpn certificate local generate rsa	154
execute sim-switch	155
execute modem	155
WiFi	157
config vap	157
config ap-security	160
config wifi-networks	162
config radio-profile	164
config wifi-general	167
User	169
config user group	169
config user radius	169
config user security-exempt-list	171
config rule	171
config user security-exempt-list6	172

config rule	172
DNS Filter	173
config dnsfilter domain-filter	173
config dnsfilter profile	174

Change Log

Date	Change Description
2026-02-13	Initial release.

Introduction

This *Reference Guide* discusses the CLI command syntax of FortiExtender. It introduces the commonly used commands with sample commands for reference.

Connect to the CLI

You can connect to the CLI through the FortiExtender or FortiCloud GUI.

To access the FortiExtender CLI via FortiCloud GUI, go to the device page of a deployed FortiExtender device and click the “>_Console” section to open a new instance of the FortiExtender console.

To access the FortiExtender CLI via the FortiExtender GUI, click the “>_” tab on the left side of the GUI.



You can open only one console per GUI access.

You can also access the FortiExtender CLI outside of the GUI using:

- Console connection — connect your computer directly to the console port of your FortiExtender.
- SSH access — connect your computer through any network interface attached to one of the network ports of your FortiExtender.

Console connection

You can directly connect to the CLI by connecting your management computer or console to the FortiExtender through its RJ-45 console port.

Direct console access to a FortiExtender device may be necessary if:

- You are installing the device for the first time, and it is not configured to connect to your network.
- You are restoring the firmware using a boot interruption. Network access to the CLI will not be available until after the boot process has completed, making direct console access the only option.

To connect to the FortiExtender console, you need a console cable to connect the console port on the FortiExtender to the communications port on a computer. Depending on your device, this may require:

- A USB to RJ-45 cable
- A DB-9 to RJ-45 cable (a DB-9-to-USB adapter may be used)
- A computer with an available communications port
- A terminal emulation software app

To connect to the CLI through a direct console connection:

1. Using the console cable, connect the FortiExtender console port to the serial communications (COM) port on your management computer.
2. Start a terminal emulation program on your management computer, select the COM port, and set the Baud speed to 115200 Bits per second.
3. Press Enter on the keyboard to connect to the CLI.
4. Log into the CLI using your username and password ("admin" by default; you will be prompted to create a new password upon your first login).

You can now enter CLI commands, including configuring access to the CLI via SSH.

SSH access

You can establish SSH access to the CLI by connecting your computer to the FortiExtender using one of its network ports, either directly using a peer connection between the two or through any intermediary network.

SSH must be enabled on the network interface that is associated with the physical network port that is being used.

If your computer is not connected either directly or through a switch to the FortiExtender, you must also configure the FortiExtender using a static route that can forward packets from the FortiExtender to the computer. This can be done using a local console connection or in the GUI.

To connect to the FortiExtender using SSH, you need:

- A computer with an available serial communications (COM) port and an RJ-45 port
- An appropriate console cable
- A network cable
- Terminal emulation software
- Prior configuration of the operating mode, network interface, and static route.

Enable SSH access to the CLI using a local console connection:

1. Using the network cable, connect the FortiExtender network port either directly to the network port on your computer or to a network through which your computer can reach the FortiExtender.
2. Note down the port number of the physical network port.
3. Using the direct console connection, connect and log into the CLI.
4. Enter the following command:

```
config system interface
  edit <interface_str>
```

```
        set allowaccess ssh
    next
```

where <interface_str> is the name of the network interface associated with the physical network port, such as port4.

5. Confirm the configuration using the following commands to show the interface settings:

```
config system interface
edit port4
show
For example:
FX511FTQ22002638 # config system interface
FX511FTQ22002638 (interface) # edit port4
FX511FTQ22002638 (port4) # show
edit port4
    set type physical
    set status up
    set mode static
    set ip
    set gateway
    set mtu-override disable
    set distance 51
    set vrrp-virtual-mac enable
config vrrp
    set status disable
end
    set allowaccess ssh
next
```

Access the FortiExtender CLI using SSH

Once the FortiExtender is configured to accept SSH connections, use an SSH client on your management computer to connect to the CLI.

The following instructions use PuTTY. The steps may vary in other terminal emulators.

To connect to the CLI using SSH:

1. On your management computer, start PuTTY.
2. In the Host Name (or IP address) field, enter the IP address of the FortiExtender network interface that you are connected to and has SSH access enabled.
3. Set the port number to 22, if it is not automatically set.
4. Set the connection type to SSH.
5. Click Open. The SSH client starts to connect to the FortiExtender.



The SSH client may display a warning if this is the first time that you are connecting to the FortiExtender and its SSH key is not yet recognized by the SSH client, or if you previously connected to the FortiExtender using a different IP address or SSH key. This is normal if the management computer is directly connected to the FortiExtender with no network hosts in between.

- 6.** Click Yes to accept the FortiExtender's SSH key.
The CLI will display the login prompt.
- 7.** Enter the administrator account name, such as admin, and press Enter.
- 8.** Enter the administrator account password and press Enter.
The CLI console shows the command prompt (the FortiExtender hostname followed by #). You can now enter CLI commands.

CLI commands

This *Reference Guide* introduces the syntax of the CLI commands to configure and manage a FortiExtender unit. The CLI syntax was created by processing the schema from FortiExtender models running FortiExtender OS version 7.2.0 and reformatting the resultant CLI output.

The commands cover the following topics:

- [Header on page 13](#)
- [Firewall on page 14](#)
- [LTE on page 23](#)
- [Router on page 36](#)
- [System on page 55](#)
- [SNMP on page 126](#)
- [HMON on page 132](#)
- [VPN on page 136](#)
- [Network on page 149](#)
- [Execute on page 153](#)



All CLI commands in this *Reference Guide* are based on FortiExtender 201E, a FortiExtender model that runs on the Sierra Modem EM7455.

Header

This section shows the syntax of the following command:

- [config version on page 13](#)

config version

Description: Configure header version settings.

```
config version
  set config {integer}
  set carrier {string}
  set simmap {integer}
  set certificate {integer}
unset
show
end
```

Sample command:

```
FX201E5919000057 (header) # show
config header
  config version
    set config 10517384
    set carrier FEM_06-22-1-2-AMEU|4a29ea
    set simmap 92e21b
    set certificate 3876258
  end
end
```

Parameter	Description	Type	Size	Default
config	Device configuration version.	integer	-	none
carrier	LTE carrier configuration version.	string	-	none
simmap	LTE SIM map configuration version.	string	-	none
certificate	VPN certificate version.	integer	-	none

Firewall

This section shows the syntax of the following commands:

- [config firewall policy on page 14](#)
- [config traffic-shaper on page 18](#)
- [config shaping-policy on page 19](#)
- [config vip on page 20](#)

config firewall policy

Description: Configure firewall policies.

```
config firewall policy
  edit <name>
    set *srcintf <name1>, <name2>, ...
    set *dstintf <name1>, <name2>, ...
    set *srcaddr <name1>, <name2>, ...
    set dnat [enable | disable]
    set *dstaddr <name1>, <name2>, ...
    set action [accept | deny]
    set status [enable | disable]
    set *service <name1>, <name2>, ...
    set nat [enable | disable]
    set srcaddr6 <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
  next
delete <name>
move <name1> [after | before] <name2>
end
purge
show
```

Sample command:

```
config firewall policy
  edit all-nat
    set srcintf any
    set dstintf any
    set srcaddr lan
    set dnat disable
    set dstaddr all
    set srcaddr6 any
```

```

set dstaddr6 any
set action accept
set status enable
set service ALL
set nat enable
next
end

```

Parameter	Description	Type	Size	Default														
srcintf	Incoming (ingress) interface.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the incoming interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the incoming interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the incoming interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the incoming interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the incoming interface.</td> </tr> <tr> <td>any</td> <td>Any port as the incoming interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the incoming interface.	lo	Loopback as the incoming interface.	lte1	LTE 1 as the incoming interface.	wan	WAN as the incoming interface.	port4	Port 4 as the incoming interface.	any	Any port as the incoming interface.			
Option	Description																	
lan	LAN as the incoming interface.																	
lo	Loopback as the incoming interface.																	
lte1	LTE 1 as the incoming interface.																	
wan	WAN as the incoming interface.																	
port4	Port 4 as the incoming interface.																	
any	Any port as the incoming interface.																	
dstintf	Outgoing (egress) interface.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the outgoing interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the outgoing interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the outgoing interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the outgoing interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the outgoing interface.</td> </tr> <tr> <td>any</td> <td>Any port as the outgoing interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the outgoing interface.	lo	Loopback as the outgoing interface.	lte1	LTE 1 as the outgoing interface.	wan	WAN as the outgoing interface.	port4	Port 4 as the outgoing interface.	any	Any port as the outgoing interface.			
Option	Description																	
lan	LAN as the outgoing interface.																	
lo	Loopback as the outgoing interface.																	
lte1	LTE 1 as the outgoing interface.																	
wan	WAN as the outgoing interface.																	
port4	Port 4 as the outgoing interface.																	
any	Any port as the outgoing interface.																	
srcaddr	Source address.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>all</td> <td>All network addresses.</td> </tr> <tr> <td>none</td> <td>None of the network addresses.</td> </tr> <tr> <td>lan-src</td> <td>LAN network address.</td> </tr> <tr> <td>wan-src</td> <td>WAN network address.</td> </tr> </tbody> </table>	Option	Description	all	All network addresses.	none	None of the network addresses.	lan-src	LAN network address.	wan-src	WAN network address.							
Option	Description																	
all	All network addresses.																	
none	None of the network addresses.																	
lan-src	LAN network address.																	
wan-src	WAN network address.																	
dnat	Destination NAT.	option	-	disable														

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable destination NAT.</td> </tr> <tr> <td>disable</td> <td>Disable destination NAT.</td> </tr> </tbody> </table>	Option	Description	enable	Enable destination NAT.	disable	Disable destination NAT.							
Option	Description													
enable	Enable destination NAT.													
disable	Disable destination NAT.													
dstaddr	Destination address.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>all</td> <td>All network addresses.</td> </tr> <tr> <td>none</td> <td>None of the network addresses.</td> </tr> <tr> <td>lan-src</td> <td>LAN network address.</td> </tr> <tr> <td>wan-src</td> <td>WAN network address.</td> </tr> </tbody> </table>	Option	Description	all	All network addresses.	none	None of the network addresses.	lan-src	LAN network address.	wan-src	WAN network address.			
Option	Description													
all	All network addresses.													
none	None of the network addresses.													
lan-src	LAN network address.													
wan-src	WAN network address.													
action	Policy action.	option	-	accept										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>accept</td> <td>Accept policy.</td> </tr> <tr> <td>deny</td> <td>Deny policy.</td> </tr> </tbody> </table>	Option	Description	accept	Accept policy.	deny	Deny policy.							
Option	Description													
accept	Accept policy.													
deny	Deny policy.													
status	Status of the policy.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable this policy.</td> </tr> <tr> <td>disable</td> <td>Disable this policy.</td> </tr> </tbody> </table>	Option	Description	enable	Enable this policy.	disable	Disable this policy.							
Option	Description													
enable	Enable this policy.													
disable	Disable this policy.													
service	Service/service group name.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ALL</td> <td>All services.</td> </tr> <tr> <td>HTTP</td> <td>HTTP service.</td> </tr> <tr> <td>etc</td> <td>Refer to config network service list.</td> </tr> </tbody> </table>	Option	Description	ALL	All services.	HTTP	HTTP service.	etc	Refer to config network service list.					
Option	Description													
ALL	All services.													
HTTP	HTTP service.													
etc	Refer to config network service list.													
nat	Source NAT.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable source NAT.</td> </tr> <tr> <td>disable</td> <td>Disable source NAT.</td> </tr> </tbody> </table>	Option	Description	enable	Enable source NAT.	disable	Disable source NAT.							
Option	Description													
enable	Enable source NAT.													
disable	Disable source NAT.													
srcaddr6	Source IPv6 address	option	-	none										

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>all</td> <td>All network addresses.</td> </tr> <tr> <td>none</td> <td>None of the network addresses.</td> </tr> <tr> <td>lan-src</td> <td>LAN network address.</td> </tr> <tr> <td>wan-src</td> <td>WAN network address.</td> </tr> </tbody> </table>	Option	Description	all	All network addresses.	none	None of the network addresses.	lan-src	LAN network address.	wan-src	WAN network address.			
Option	Description													
all	All network addresses.													
none	None of the network addresses.													
lan-src	LAN network address.													
wan-src	WAN network address.													
dstaddr6	Destination IPv6 address	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>all</td> <td>All network addresses.</td> </tr> <tr> <td>none</td> <td>None of the network addresses.</td> </tr> <tr> <td>lan-src</td> <td>LAN network address.</td> </tr> <tr> <td>wan-src</td> <td>WAN network address.</td> </tr> </tbody> </table>	Option	Description	all	All network addresses.	none	None of the network addresses.	lan-src	LAN network address.	wan-src	WAN network address.			
Option	Description													
all	All network addresses.													
none	None of the network addresses.													
lan-src	LAN network address.													
wan-src	WAN network address.													

```

FX201E5919000057 (policy) # move test2 after all-pass
FX201E5919000057 (policy) <M> # show
config firewall policy
  edit test1
    set srcintf lo
    set dstintf any
    set srcaddr all
    set dnat disable
    set dstaddr all
    set action accept
    set status enable
    set service AH
    set nat enable
  next
  edit all-pass
    set srcintf any
    set dstintf any
    set srcaddr all
    set dnat disable
    set dstaddr all
    set action accept
    set status enable
    set service ALL
    set nat enable
  next
  edit test2
    set srcintf any
    set dstintf lan
    set srcaddr all
    set dnat disable
  
```

```

    set dstaddr all
    set action accept
    set status disable
    set service ALL
    set nat enable
  next
end
FX201E5919000057 (policy) <M> # end

```

config traffic-shaper

Description: Configure firewall shapers.

```

config traffic-shaper
  edit <name>
    set max-bandwidth (1 - 16776000)
    set *bandwidth-unit [kbps | mbps | gbps]
  delete <name>
  purge
  show
end

```

Sample command:

```

FX201E5919000057 (traffic-shaper) # show
config firewall shaper traffic-shaper
  edit 1
    set max-bandwidth 34
    set bandwidth-unit kbps
  next
end

```

Parameter	Description	Type	Size	Default
max-bandwidth	Upper bandwidth limit enforced by the shaper.	integer	1 - 16776000	100
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for the shaper.	option	-	none
	Option	Description		
	kbps	Kilobits per second.		
	mbps	Megabits per second.		
	gbps	Gigabits per second.		

config shaping-policy

Description: Configure firewall shaping policies.

```
config shaping-policy
  edit <name>
    set status [enable | disable]
    set *dstintf <name1>, <name2>, ...
    set *traffic-shaper <name1>, <name2>, ...
  delete <name>
  purge
  show
end
```

Sample command:

```
FX201E5919000057 (shaping-policy) # show
config firewall shaping-policy
  edit 1_policy
    set status enable
    set dstintf wan
    set traffic-shaper 1
  next
end
```

Parameter	Description	Type	Size	Default
status	Status of the traffic shaping policy.	option	-	enable
	Option	Description		
	enable	Enable the policy.		
	disable	Disable the policy.		
dstintf	Outgoing (egress) interface.	option	-	none
	Option	Description		
	lan	LAN as the outgoing interface.		
	lo	Loopback as the outgoing interface.		
	lte1	LTE 1 as the outgoing interface.		
	wan	WAN as the outgoing interface.		
	port4	Port 4 as the outgoing interface.		
	any	Any port as the outgoing interface.		

Parameter	Description	Type	Size	Default
traffic-shaper	Traffic shaper to apply to traffic forwarded by the firewall policy.	option	-	none
	Option	Description		
	1	Refer to config traffic-shaper on page 18.		

config vip

Description: Configure firewall virtual IPs.

```

config vip
  edit <name >
    set comment [255]
    set *extip <name1>
    set *mappedip <name1>
    set *extintf <name1>, <name2>, ...
    set portforward [enable | disable]
    set *protocol <name1>, <name2>, ... *only accessible when portforward is enabled
    set *extport (1 - 65535) *only accessible when portforward is enabled
    set *mappedport (1 - 65535) *only accessible when portforward is enabled
    unset
    next
    show
    abort
    end
  delete <name >
  purge
  show
  end

```

Sample command:

```

FX201E5919000057 (vip) # show
  config firewall vip
    edit 1
      set comment this is a test vip
      set extip 10.153.24.44
      set mappedip 10.153.24.36
      set extintf any
      set portforward enable
      set protocol tcp
      set extport 25
      set mappedport 33
    next
  end

```

Parameter	Description	Type	Size	Default														
comment	Optional comments.	string	Up to 255 characters in length	none														
extip	IP address on the external interface to be mapped to an address on the destination network.	IPv4 address	-	none														
mappedip	IP address on the destination network to which the external IP address is mapped.	IPv4 address	-	none														
extintf	Interface connected to the source network that receives packets to be forwarded to the destination network.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the outgoing interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the outgoing interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the outgoing interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the outgoing interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the outgoing interface.</td> </tr> <tr> <td>any</td> <td>Any port as the outgoing interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the outgoing interface.	lo	Loopback as the outgoing interface.	lte1	LTE 1 as the outgoing interface.	wan	WAN as the outgoing interface.	port4	Port 4 as the outgoing interface.	any	Any port as the outgoing interface.			
Option	Description																	
lan	LAN as the outgoing interface.																	
lo	Loopback as the outgoing interface.																	
lte1	LTE 1 as the outgoing interface.																	
wan	WAN as the outgoing interface.																	
port4	Port 4 as the outgoing interface.																	
any	Any port as the outgoing interface.																	
portforward	Port forwarding.	option	-	disable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable port forwarding.</td> </tr> <tr> <td>disable</td> <td>Disable port forwarding.</td> </tr> </tbody> </table>	Option	Description	enable	Enable port forwarding.	disable	Disable port forwarding.											
Option	Description																	
enable	Enable port forwarding.																	
disable	Disable port forwarding.																	
protocol	Protocol to use when forwarding packets.	option	-	tcp														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>tcp</td> <td>TCP protocol.</td> </tr> <tr> <td>udp</td> <td>UDP Protocol.</td> </tr> <tr> <td>icmp</td> <td>ICMP protocol.</td> </tr> </tbody> </table>	Option	Description	tcp	TCP protocol.	udp	UDP Protocol.	icmp	ICMP protocol.									
Option	Description																	
tcp	TCP protocol.																	
udp	UDP Protocol.																	
icmp	ICMP protocol.																	
extport	Incoming port number to be mapped to a port number on the destination network.	number	1 - 65535	0														

Parameter	Description	Type	Size	Default
mappedport	Port number on the destination network to which the external port number is mapped.	number	1 - 65535	0

LTE

This section shows the syntax of the following commands:



These commands are NOT applicable to the FortiExtender 200F platform.

- [config lte setting on page 23](#)
- [config carrier on page 30](#)
- [config simmap on page 31](#)
- [config plan on page 32](#)

config lte setting

Description: Configure LTE modem settings.

```
config lte setting
  config controller-report
    set status [enable | disable]
    set interval (30 - 86400)
    set signal-threshold (10 - 50)
  end
  config modem1
    set pause-modem-manager [enable | disable]
    set default-sim [sim1 | sim2 | by-carrier | by-cost]
    set preferred-carrier {string}
    set esim [enable | disable]
    set session-down-detection (1 - 60)
    set gps [enable | disable]
    set sim1-pin [enable | disable]
    set sim1-pin-code {0, 4}
    set sim2-pin [enable | disable]
    set sim2-pin-code {0, 4}
    config auto-switch
      set by-disconnect [enable | disable]
      set by-signal [enable | disable]
      set by-data-plan [enable | disable]
      set by-health-monitor [enable | disable]
    config health-monitor
      set event <name>
      set fail-cnt (1 - 10)
      set recovery-cnt (1 - 10)
      set by-latency [enable |disable]
```

```
        set latency-threshold (0 - 10000000)
        set by-jitter [enable |disable]
        set jitter-threshold (0 - 10000000)
        set recover-by-reboot [enable | disable]
        set max-switches-allowed (1 - 20)
        set max-switches-interval (300 - 3600)
    end
    set disconnect-threshold (1 - 100)
    set disconnect-period (600 - 18000)
    set switch-back [by-timer | by-time ]
    set switch-back-time (HH:MM)
    set switch-back-timer (3600 - 2147483647)
end
end
config modem2
    set pause-modem-manager [enable | disable]
    set default-sim sim1 | sim2 | by-carrier | by-cost]
    set preferred-carrier {string}
    set session-down-detection (1 - 60)
    set gps [enable | disable]
    set sim1-pin [enable | disable]
    set sim1-pin-code {0, 4}
    set sim2-pin [enable | disable]
    set sim2-pin-code {0, 4}
    config auto-switch
        set by-disconnect [enable | disable]
        set by-signal [enable | disable]
        set by-data-plan [enable | disable]
        set by-health-monitor [enable | disable]
    config health-monitor
        set event <name>
        set fail-cnt (1 - 10)
        set recovery-cnt (1 - 10)
        set by-latency [enable |disable]
        set latency-threshold (0 - 10000000)
        set by-jitter [enable |disable]
        set jitter-threshold (0 - 10000000)
        set recover-by-reboot [enable | disable]
        set max-switches-allowed (1 - 20)
        set max-switches-interval (300 - 3600)
    end
    set disconnect-threshold (1 - 100)
    set disconnect-period (600 - 18000)
    set switch-back [by-timer | by-time ]
    set switch-back-time (HH:MM)
    set switch-back-timer (3600 - 2147483647)
end
end
set advanced [enable | disable]
config advanced-settings
    set sim-activation-delay (5 - 600)
    set force-ipv4 [enable | disable]
```

```
end
end
unset
show
```

Sample command:

```
config lte setting
  config controller-report
    set status enable
    set interval 300
    set signal-threshold 10
  end
  config modem1
    set pause-modem-manager 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 enable
      set by-signal disable
      set by-data-plan disable
      set by-health-monitor enable
      config health-monitor
        set event
        set fail-cnt 5
        set recovery-cnt 5
        set by-latency enable
        set latency-threshold 150
        set by-jitter enable
        set jitter-threshold 150
        set recover-by-reboot disable
      end
      set disconnect-threshold 3
      set disconnect-period 600
      set switch-back by-time by-timer
      set switch-back-time 00:01
      set switch-back-timer 86400
    end
  end
  set advanced enable
  config advanced-settings
    set sim-activation-delay 300
    set force-ipv4 disable
  end
end
```

Parameter	Description	Type	Size	Default										
status	Status of controller reporting.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable LTE controller report.</td> </tr> <tr> <td>disable</td> <td>Disable LTE controller report.</td> </tr> </tbody> </table>	Option	Description	enable	Enable LTE controller report.	disable	Disable LTE controller report.							
Option	Description													
enable	Enable LTE controller report.													
disable	Disable LTE controller report.													
interval	Reporting interval.	integer	30 - 86400	300										
signal-threshold	Signal threshold that needs to be reached before a report is sent.	integer	10 - 50	10										
Parameter	Description	Type	Size	Default										
pause-modem-manager	Delay the modem if the SIM needs a longer activation period.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable delayed modem activation.</td> </tr> <tr> <td>disable</td> <td>Disable delay of modem activation.</td> </tr> </tbody> </table>	Option	Description	enable	Enable delayed modem activation.	disable	Disable delay of modem activation.							
Option	Description													
enable	Enable delayed modem activation.													
disable	Disable delay of modem activation.													
default-sim	The first SIM card which the modem will try and connect with.	option	-	sim1										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>sim1</td> <td>SIM card in SIM slot 1.</td> </tr> <tr> <td>sim2</td> <td>SIM card in SIM slot 2.</td> </tr> <tr> <td>by-carrier</td> <td>SIM card from the carrier specified in preferred-carrier.</td> </tr> <tr> <td>by-cost</td> <td>SIM card whose plan has the lowest cost.</td> </tr> </tbody> </table>	Option	Description	sim1	SIM card in SIM slot 1.	sim2	SIM card in SIM slot 2.	by-carrier	SIM card from the carrier specified in preferred-carrier.	by-cost	SIM card whose plan has the lowest cost.			
Option	Description													
sim1	SIM card in SIM slot 1.													
sim2	SIM card in SIM slot 2.													
by-carrier	SIM card from the carrier specified in preferred-carrier.													
by-cost	SIM card whose plan has the lowest cost.													
preferred-carrier	Preferred carrier which the modem will try and connect with.	string	-	none										
esim	Enable or disable eSIM capabilities. Only available on supported platforms.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable eSIM capabilities.</td> </tr> <tr> <td>disable</td> <td>Disable eSIM capabilities.</td> </tr> </tbody> </table>	Option	Description	enable	Enable eSIM capabilities.	disable	Disable eSIM capabilities.							
Option	Description													
enable	Enable eSIM capabilities.													
disable	Disable eSIM capabilities.													
session-down-detection	Period to confirm a session has been disconnected.	integer	1 - 60	3										

Parameter	Description	Type	Size	Default						
gps	GPS location.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable GPS location.</td> </tr> <tr> <td>disable</td> <td>Disable GPS location.</td> </tr> </tbody> </table>	Option	Description	enable	Enable GPS location.	disable	Disable GPS location.			
Option	Description									
enable	Enable GPS location.									
disable	Disable GPS location.									
sim1-pin	Whether or not SIM 1 requires a pin code.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>SIM 1 requires a pin.</td> </tr> <tr> <td>disable</td> <td>SIM 1 does not require a pin.</td> </tr> </tbody> </table>	Option	Description	enable	SIM 1 requires a pin.	disable	SIM 1 does not require a pin.			
Option	Description									
enable	SIM 1 requires a pin.									
disable	SIM 1 does not require a pin.									
sim1-pin-code	The 4-digit pin code provided by the carrier.	integer		none						
sim2-pin	Whether or not SIM 2 requires a pin code.	option		disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>SIM 2 requires a pin.</td> </tr> <tr> <td>disable</td> <td>SIM 2 does not require a pin.</td> </tr> </tbody> </table>	Option	Description	enable	SIM 2 requires a pin.	disable	SIM 2 does not require a pin.			
Option	Description									
enable	SIM 2 requires a pin.									
disable	SIM 2 does not require a pin.									
sim2-pin-code	The 4-digit pin code provided by the carrier.	integer		none						
by-disconnect	SIM switching occurs based on disconnects.	option		disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable SIM switching based on disconnects.</td> </tr> <tr> <td>disable</td> <td>Disable SIM switching based on disconnects.</td> </tr> </tbody> </table>	Option	Description	enable	Enable SIM switching based on disconnects.	disable	Disable SIM switching based on disconnects.			
Option	Description									
enable	Enable SIM switching based on disconnects.									
disable	Disable SIM switching based on disconnects.									
disconnect-threshold	Number of disconnects that can happen before SIM switching is triggered.	integer	1 - 100	3						
disconnect-period	Evaluation period in seconds for SIM switching.	integer	600 - 18000	600						
by-signal	SIM switching occurs based on signal strength.	option		disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable SIM switching based on signal strength.</td> </tr> <tr> <td>disable</td> <td>Disable SIM switching based on signal strength.</td> </tr> </tbody> </table>	Option	Description	enable	Enable SIM switching based on signal strength.	disable	Disable SIM switching based on signal strength.			
Option	Description									
enable	Enable SIM switching based on signal strength.									
disable	Disable SIM switching based on signal strength.									
by-data-plan	SIM switching occurs when the data plan for the active SIM is used up.	option		disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable SIM switching based on data plan usage.</td> </tr> <tr> <td>disable</td> <td>Disable SIM switching based on data plan usage.</td> </tr> </tbody> </table>	Option	Description	enable	Enable SIM switching based on data plan usage.	disable	Disable SIM switching based on data plan usage.			
Option	Description									
enable	Enable SIM switching based on data plan usage.									
disable	Disable SIM switching based on data plan usage.									
by-health-monitor	Sim switching occurs based on health checks like Ping/RTT.	option		disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable SIM switching based on health checks.</td> </tr> <tr> <td>disable</td> <td>Disable SIM switching based on health checks.</td> </tr> </tbody> </table>	Option	Description	enable	Enable SIM switching based on health checks.	disable	Disable SIM switching based on health checks.			
Option	Description									
enable	Enable SIM switching based on health checks.									
disable	Disable SIM switching based on health checks.									
event	Hmon hchk member	string		none						
fail-cnt	Number of failures before the member is considered dead.	integer	1 - 10	5						
recovery-cnt	Number of successes before the member is considered alive.	integer	1 - 10	5						
by latency	Latency monitoring on the active SIM.	option		disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Decription</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable SIM switching based on latency.</td> </tr> <tr> <td>disable</td> <td>Disable SIM switching based on latency.</td> </tr> </tbody> </table>	Option	Decription	enable	Enable SIM switching based on latency.	disable	Disable SIM switching based on latency.			
Option	Decription									
enable	Enable SIM switching based on latency.									
disable	Disable SIM switching based on latency.									
latency-threshold	Latency in milliseconds for SLA to make decision.	integer	0 - 10000000	150						
by jitter	Jitter monitoring on the active SIM.	option		disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable SIM switching based on jitter.</td> </tr> <tr> <td>disable</td> <td>Disable SIM switching based on jitter.</td> </tr> </tbody> </table>	Option	Description	enable	Enable SIM switching based on jitter.	disable	Disable SIM switching based on jitter.			
Option	Description									
enable	Enable SIM switching based on jitter.									
disable	Disable SIM switching based on jitter.									

Parameter	Description	Type	Size	Default
recover-by-reboot	Reboot to recover the modem from excessive SIM switches.	option		disable
	Option	Description		
	enable	Enable device reboot after excessive SIM switching.		
	disable	Disable device reboot after excessive SIM switching.		
max-switches-allowed	Number of SIM switches allowed for a given duration.	integer	1 - 20	5
max-switches-interval	Duration to monitor SIM switches (in seconds).	integer	300 - 3600	1800
switch-back	Direct modem to switch back to a preferred SIM when the secondary SIM is active.	option		none
	Option	Description		
	by-time	Switch back at a specified time using the HH:MM format.		
	by-timer	Switch back after the specified duration is over.		
switch-back-time	Switch over to the preferred SIM/carrier at the specified UTC time in HH:MM format.	string		00:01
switch-back-timer	Switch over to the preferred SIM/carrier after the given duration.	integer	3600 - 2147483647	86400
Parameter	Description	Type	Size	Default
advanced	Advanced options for modem configuration.	option		disable
	Option	Description		
	enable	Enable advanced settings.		
	disable	Disable advanced settings.		
sim-activation-delay	Period for SIM card activation.	integer	5 - 600	300
force-ipv4	Reconfigure the modem to use IPv4; register to ISP with IPv4 only; plan/PDN must be IPv4 only.	option		disable

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Force the modem to use IPv4 only.</td> </tr> <tr> <td>disable</td> <td>Do not force the modem to use IPv4 only.</td> </tr> </tbody> </table>	Option	Description	enable	Force the modem to use IPv4 only.	disable	Do not force the modem to use IPv4 only.			
Option	Description									
enable	Force the modem to use IPv4 only.									
disable	Do not force the modem to use IPv4 only.									

config carrier

Description: Configure LTE carriers.

```
config carrier
  edit <name>
    set firmware {string}
    set pri {string}
    set default-profile [enable | disable]
  delete <name>
  purge
  show
end
```

Sample command:

```
config lte carrier
  edit AT&T
    set firmware SWI9X30C_02.33.03.00.cwe
    set pri SWI9X30C_02.33.03.00_GENERIC_002.072_001.nvu
    set default-profile disable
  next
end
FX511FTQ22002638 (carrier) # show
config lte carrier
  edit AT&T
    set firmware RM502QAEAR11A04M4G_01.001.01.001.zip
  next
```

Parameter	Description	Type	Size	Default
firmware	Mobile Country Code (the first three digits of the SIM card's IMSI).	integer	-	none
pri	Mobile Network Code (the two or three digits after the Mobile Country Code of the SIM card's IMSI, depending on the American or European standard).	integer	-	none

Parameter	Description	Type	Size	Default						
default-profile	Carrier of the SIM card.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>The default profile will be selected from the available PDP contexts (e.g., profile 3 for Verizon).</td> </tr> <tr> <td>disable</td> <td>The default profile will not be selected.</td> </tr> </tbody> </table>	Option	Description	enable	The default profile will be selected from the available PDP contexts (e.g., profile 3 for Verizon).	disable	The default profile will not be selected.			
Option	Description									
enable	The default profile will be selected from the available PDP contexts (e.g., profile 3 for Verizon).									
disable	The default profile will not be selected.									

config simmap

Description: Configure LTE SIM maps.

```

config lte simmap
  edit <name>
    set mcc {integer}
    set mnc {integer}
    set carrier <name1>
  next
delete <name>
purge
show
end
end

```

Sample command:

```

config lte simmap
  edit testsim
    set mcc 276
    set mnc 02
    set carrier Generic
  next
end

```

Parameter	Description	Type	Size	Default
mcc	Mobile Country Code (the first three digits of the SIM card's IMSI).	integer	-	none

Parameter	Description	Type	Size	Default
mnc	Mobile Network Code (the two or three digits after the Mobile Country Code of the SIM card's IMSI).	integer	-	none
carrier	Carrier of the SIM card.	string	-	none

config plan

Description: Configure LTE plans for SIM cards.

```

config lte plan
  edit <name>
    set modem [all | modem1 | modem2]
    set type [by-iccid | by-slot | by-carrier | by-default]
    set *carrier {string}
    set *slot [sim1 | sim2]
    set *iccid {integer}
    set apn {string}
    set auth [NONE | PAP | CHAP]
    set user {string}
    set pwd {string}
    set pdn [ipv4-only | ipv-only | ipv4-ipv6]
    set signal-threshold (-100 - -50)
    set signal-period (600 - 18000)
    set capacity (0 - 102400000)
    set monthly-fee (0 - 1000000)
    set billing-date (1 - 31)
    set overage [enable | disable]
    set preferred-subnet (0 - 32)
    set private-network [enable | disable]
    set session-dial-timeout (0 - 180)

  next
delete <name>
purge
show
end

```

Sample command:

```

config lte plan
  edit ATTPlan
    set modem modem1
    set type by-carrier
    set carrier AT&T

```

```

set apn broadband
set auth none
set user
set pwd
set pdn ipv4-only
set signal-threshold -100
set signal-period 3600
set capacity 1024
set monthly-fee 0
set billing-date 1
set overage disable
set preferred-subnet 0
set private-network disable
set session-dial-timeout 0
next
end

```

Parameter	Description	Type	Size	Default										
modem	Modem that will be using this plan.	option	-	all										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>all</td> <td>All modems in the device.</td> </tr> <tr> <td>modem1</td> <td>Only modem 1 will be used.</td> </tr> <tr> <td>modem2</td> <td>Only modem 2 will be used. (This option applies to devices with two modems.)</td> </tr> </tbody> </table>	Option	Description	all	All modems in the device.	modem1	Only modem 1 will be used.	modem2	Only modem 2 will be used. (This option applies to devices with two modems.)					
Option	Description													
all	All modems in the device.													
modem1	Only modem 1 will be used.													
modem2	Only modem 2 will be used. (This option applies to devices with two modems.)													
type	Method to assign the plan.	option	-	by-default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>by-carrier</td> <td>Assign the plan to the SIM card with the specified carrier.</td> </tr> <tr> <td>by-iccid</td> <td>Assign the plan to the SIM card with the specified iccid.</td> </tr> <tr> <td>by-slot</td> <td>Assign the plan to the SIM card in the specified SIM slot.</td> </tr> <tr> <td>by-default</td> <td>Assign the plan to the default SIM card as set in LTE settings.</td> </tr> </tbody> </table>	Option	Description	by-carrier	Assign the plan to the SIM card with the specified carrier.	by-iccid	Assign the plan to the SIM card with the specified iccid.	by-slot	Assign the plan to the SIM card in the specified SIM slot.	by-default	Assign the plan to the default SIM card as set in LTE settings.			
Option	Description													
by-carrier	Assign the plan to the SIM card with the specified carrier.													
by-iccid	Assign the plan to the SIM card with the specified iccid.													
by-slot	Assign the plan to the SIM card in the specified SIM slot.													
by-default	Assign the plan to the default SIM card as set in LTE settings.													
carrier	Carrier option if type is set to by-carrier.	string		none										
slot	SIM slot to which the plan is assigned.	option		sim1										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>sim1</td> <td>Assign the plan to the SIM card in SIM slot 1.</td> </tr> <tr> <td>sim2</td> <td>Assign the plan to the SIM card in SIM slot 2.</td> </tr> </tbody> </table>	Option	Description	sim1	Assign the plan to the SIM card in SIM slot 1.	sim2	Assign the plan to the SIM card in SIM slot 2.							
Option	Description													
sim1	Assign the plan to the SIM card in SIM slot 1.													
sim2	Assign the plan to the SIM card in SIM slot 2.													
iccid	The ICCID of the SIM card to which the plan is assigned.	integer	-	none										

Parameter	Description	Type	Size	Default								
apn	APN of the carrier.	string	-	none								
auth	Authentication method	option	-	NONE								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>NONE</td> <td>No authentication.</td> </tr> <tr> <td>PAP</td> <td>Password authentication protocol.</td> </tr> <tr> <td>CHAP</td> <td>Challenge-and-response authentication protocol.</td> </tr> </tbody> </table>	Option	Description	NONE	No authentication.	PAP	Password authentication protocol.	CHAP	Challenge-and-response authentication protocol.			
Option	Description											
NONE	No authentication.											
PAP	Password authentication protocol.											
CHAP	Challenge-and-response authentication protocol.											
user	username.	string	-	none								
pwd	password.	string	-	none								
pdn	Request Packet Data Network (PDN) IP address family.	option	-	ipv4-only								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Definition</th> </tr> </thead> <tbody> <tr> <td>ipv4-only</td> <td>Only the IPv4 protocol is used.</td> </tr> <tr> <td>ipv6-only</td> <td>Only the IPv6 protocol is used.</td> </tr> <tr> <td>ipv4-ipv6</td> <td>Both IPv4 and IPv6 are tried.</td> </tr> </tbody> </table>	Option	Definition	ipv4-only	Only the IPv4 protocol is used.	ipv6-only	Only the IPv6 protocol is used.	ipv4-ipv6	Both IPv4 and IPv6 are tried.			
Option	Definition											
ipv4-only	Only the IPv4 protocol is used.											
ipv6-only	Only the IPv6 protocol is used.											
ipv4-ipv6	Both IPv4 and IPv6 are tried.											
signal-threshold	SIM switch if signal drops below the set threshold.	integer	-100 - -50	-100								
signal-period	SIM switch if signal drops below the threshold for more than half of the set period.	integer	600 - 18000	3600								
capacity	The amount of data allotted to the SIM card's plan.	integer	0 - 10240000	0								
monthly-fee	The amount paid each month for the plan.	integer	0 - 1000000	0								
billing-date	The day of the month when the payment for the plan is renewed.	integer	1 - 31	1								
overage	Whether the SIM card can continue to use data once the allotted amount is used up.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable data usage over capacity.</td> </tr> <tr> <td>disable</td> <td>Disable data usage once the capacity has been reached.</td> </tr> </tbody> </table>	Option	Description	enable	Enable data usage over capacity.	disable	Disable data usage once the capacity has been reached.					
Option	Description											
enable	Enable data usage over capacity.											
disable	Disable data usage once the capacity has been reached.											
preferred-subnet	DHCP address netmask overwriting with modem assignment.	integer	0 - 32	0								

Parameter	Description	Type	Size	Default						
private-network	Whether the cellular modem forwards DHCP packets to the WAN/Internet through the LTE/5G model interface.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable DHCP traffic on port UDP 67 so cellular modems can forward them from the internal to the external side.</td> </tr> <tr> <td>disable</td> <td>Block DHCP traffic on port UDP 67, preventing them from passing from the internal to the external side.</td> </tr> </tbody> </table>	Option	Description	enable	Enable DHCP traffic on port UDP 67 so cellular modems can forward them from the internal to the external side.	disable	Block DHCP traffic on port UDP 67, preventing them from passing from the internal to the external side.			
Option	Description									
enable	Enable DHCP traffic on port UDP 67 so cellular modems can forward them from the internal to the external side.									
disable	Block DHCP traffic on port UDP 67, preventing them from passing from the internal to the external side.									
session-dial-timeout	Timeout value when dialing up a session.	integer	0 - 180	0						

Router

This section shows the syntax of the following commands:

- [config router policy on page 36](#)
- [config router static on page 40](#)
- [config router target on page 43](#)
- [config multicast on page 45](#)
- [config OSPF on page 47](#)
- [config prefix-list on page 51](#)
- [config route-map on page 53](#)

config router policy

Description: Configure router policies.

```
config router policy
  edit <name>
    set input-device <name1>
    set srcaddr <name1>
    set dstaddr <name1>
    set service <name1>, <name2>, ...
    set *target <name1>
    set status [enable | disable]
    set comment {string}
    unset
    next
    show
    abort
  end
delete <name>
purge
move <name1> [before | after] <name2>
show
end
```

Sample command:

```
FX201E5919000057 (policy) # show
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

```

Parameter	Description	Type	Size	Default
input-device	Incoming interface name.	option	-	none
	Option	Description		
	lan	LAN as the input device.		
	lo	Loopback as the input device.		
	lte1	LTE 1 as the input device.		
	wan	WAN as the input device.		
	port4	Port 4 as the input device.		
	port1	Port 1 as the input device.		
srcaddr	Source address.	option	-	none
	Option	Description		
	lan	LAN network address.		
	all	All the network addresses.		
	none	None of the network addresses.		
dstaddr	destination address.	option	-	none
	Option	Description		
	lan	LAN network address.		
	all	All the network addresses.		
	none	None of the network addresses.		
service	Service/service group names.	option	-	none
	Option	Description		
	ALL_ICMP	ICMP.		
	ALL	All.		
	etc	Refer to the different services in this command.		

Parameter	Description	Type	Size	Default														
target	The PBR's out-going interface and next-hop.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>target.lan</td> <td>LAN as the target.</td> </tr> <tr> <td>target.lo</td> <td>Loopback as the target.</td> </tr> <tr> <td>target.lte1</td> <td>LTE 1 as the target.</td> </tr> <tr> <td>target.wan</td> <td>WAN as the target.</td> </tr> <tr> <td>target.port4</td> <td>Port 4 as the target.</td> </tr> <tr> <td>target.Port1</td> <td>Port 1 as the target.</td> </tr> </tbody> </table>	Option	Description	target.lan	LAN as the target.	target.lo	Loopback as the target.	target.lte1	LTE 1 as the target.	target.wan	WAN as the target.	target.port4	Port 4 as the target.	target.Port1	Port 1 as the target.			
Option	Description																	
target.lan	LAN as the target.																	
target.lo	Loopback as the target.																	
target.lte1	LTE 1 as the target.																	
target.wan	WAN as the target.																	
target.port4	Port 4 as the target.																	
target.Port1	Port 1 as the target.																	
status	Status of the policy based the routing rule.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the policy.</td> </tr> <tr> <td>disable</td> <td>Disable the policy.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the policy.	disable	Disable the policy.											
Option	Description																	
enable	Enable the policy.																	
disable	Disable the policy.																	
comment	Comment on the policy.	string	1 - 255 characters in length	none														

config router policy6

Description: Configure IPv6 router policies.

```

config router policy6
  edit <name>
    set input-device <name1>
    set srcaddr <name1>
    set dstaddr <name1>
    set service <name1>, <name2>, ...
    set *target <name1>
    set status [enable | disable]
    set comment {string}
  unset
  next
  show
  abort
  end
  delete <name>
  purge

```

```

move <name1> [before | after] <name2>
show
end

```

Sample command:

```

config router policy6
  edit 1
    set input-device lan
    set srcaddr all
    set dstaddr all
    set service ALL
    set target target.wan
    set status enable
    set comment
  next
end

```

Parameter	Description	Type	Size	Default														
input-device	Incoming interface name.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the input device.</td> </tr> <tr> <td>lo</td> <td>Loopback as the input device.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the input device.</td> </tr> <tr> <td>wan</td> <td>WAN as the input device.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the input device.</td> </tr> <tr> <td>port1</td> <td>Port 1 as the input device.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the input device.	lo	Loopback as the input device.	lte1	LTE 1 as the input device.	wan	WAN as the input device.	port4	Port 4 as the input device.	port1	Port 1 as the input device.			
Option	Description																	
lan	LAN as the input device.																	
lo	Loopback as the input device.																	
lte1	LTE 1 as the input device.																	
wan	WAN as the input device.																	
port4	Port 4 as the input device.																	
port1	Port 1 as the input device.																	
srcaddr	Source address.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN network address.</td> </tr> <tr> <td>all</td> <td>All the network addresses.</td> </tr> <tr> <td>none</td> <td>None of the network addresses.</td> </tr> </tbody> </table>	Option	Description	lan	LAN network address.	all	All the network addresses.	none	None of the network addresses.									
Option	Description																	
lan	LAN network address.																	
all	All the network addresses.																	
none	None of the network addresses.																	
dstaddr	destination address.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN network address.</td> </tr> <tr> <td>all</td> <td>All the network addresses.</td> </tr> <tr> <td>none</td> <td>None of the network addresses.</td> </tr> </tbody> </table>	Option	Description	lan	LAN network address.	all	All the network addresses.	none	None of the network addresses.									
Option	Description																	
lan	LAN network address.																	
all	All the network addresses.																	
none	None of the network addresses.																	

Parameter	Description	Type	Size	Default														
service	Service/service group names.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ALL_ICMP</td> <td>ICMP.</td> </tr> <tr> <td>ALL</td> <td>All.</td> </tr> <tr> <td>etc</td> <td>Refer to the different services in this command.</td> </tr> </tbody> </table>	Option	Description	ALL_ICMP	ICMP.	ALL	All.	etc	Refer to the different services in this command.									
Option	Description																	
ALL_ICMP	ICMP.																	
ALL	All.																	
etc	Refer to the different services in this command.																	
target	The PBR's out-going interface and next-hop.	option	-	none														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>target.lan</td> <td>LAN as the target.</td> </tr> <tr> <td>target.lo</td> <td>Loopback as the target.</td> </tr> <tr> <td>target.lte1</td> <td>LTE 1 as the target.</td> </tr> <tr> <td>target.wan</td> <td>WAN as the target.</td> </tr> <tr> <td>target.port4</td> <td>Port 4 as the target.</td> </tr> <tr> <td>target.Port1</td> <td>Port 1 as the target.</td> </tr> </tbody> </table>	Option	Description	target.lan	LAN as the target.	target.lo	Loopback as the target.	target.lte1	LTE 1 as the target.	target.wan	WAN as the target.	target.port4	Port 4 as the target.	target.Port1	Port 1 as the target.			
Option	Description																	
target.lan	LAN as the target.																	
target.lo	Loopback as the target.																	
target.lte1	LTE 1 as the target.																	
target.wan	WAN as the target.																	
target.port4	Port 4 as the target.																	
target.Port1	Port 1 as the target.																	
status	Status of the policy based the routing rule.	option	-	enable														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the policy.</td> </tr> <tr> <td>disable</td> <td>Disable the policy.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the policy.	disable	Disable the policy.											
Option	Description																	
enable	Enable the policy.																	
disable	Disable the policy.																	
comment	Comment on the policy.	string	1 - 255 characters in length	none														

config router static

Description: Configure static routes.

```

config router static
  edit <name>
    set status [enable | disable]
    set dst {ipv4-address}
    set gateway {ipv4-address}
    set distance [1 - 255]
    set *device <name1>
    set comment {string}
  unset

```

```

    next
    show
    abort
    end
delete <name>
purge
show

```

Sample command:

```

FX201E5919000057 (static) # show
config router static
  edit 1
    set status enable
    set dst 10.124.23.0/24
    set gateway 192.168.200.99
    set distance 1
    set device wan
    set comment this is a sample static route
  next
end

```

Parameter	Description	Type	Size	Default
status	Status of the static route.	option	-	enable
	Option	Description		
	enable	Enable static route.		
	disable	Disable static route.		
dst	Destination IP and mask for the route.	Ipv4_ address/netmask-	-	none
gateway	Gateway IP for the route.	Ipv4_address	-	none
distance	Administrative distance. (This field is the metric of the route item. Set the value carefully and ensure that this route item matches your application scenario without affecting other route items.)	integer	1 - 255	1
device	Gateway outgoing interface or tunnel.	option	-	none
comment	Comment on the route. (Optional)	string	Up to 255 characters in length	none

config router static6

Description: Configure IPv6 static routes.

```

config router static
  edit <name>
    set status [enable | disable]
    set dst {ipv6-address}
    set gateway {ipv6-address}
    set distance [1 - 255]
    set *device <name1>
    set comment {string}
  unset
  next
  show
  abort
  end
delete <name>
purge
show

```

Sample command:

```

config router static6
  edit 1
    set status enable
    set dst 0::0/0
    set gateway 2001::3
    set distance 10
    set device wan
    set comment
  next
end

```

Parameter	Description	Type	Size	Default
status	Status of the static route.	option	-	enable
	Option	Description		
	enable	Enable static route.		
	disable	Disable static route.		
dst	Destination IP and mask for the route.	ipv6_ address/netmask-	-	none
gateway	Gateway IP for the route.	ipv6_address	-	none

Parameter	Description	Type	Size	Default
distance	Administrative distance. (This field is the metric of the route item. Set the value carefully and ensure that this route item matches your application scenario without affecting other route items.)	integer	1 - 255	1
device	Gateway outgoing interface or tunnel.	option	-	none
comment	Comment on the route. (Optional)	string	Up to 255 characters in length	none

config router target

Description: Configure router targets.

```

config router target
  edit <name>
    set *target <name1>
    set next-hop <name1>
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end

```

Sample command:

```

FX201E5919000057 # config router target
FX201E5919000057 (target) # show
config router target
  edit target.lo
    set interface lo
    set next-hop
  next

```

Parameter	Description	Type	Size	Default
interface	Target interface.	option		none

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the target interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the target interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the target interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the target interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the target interface.</td> </tr> <tr> <td>port1</td> <td>Port 1 as the target interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the target interface.	lo	Loopback as the target interface.	lte1	LTE 1 as the target interface.	wan	WAN as the target interface.	port4	Port 4 as the target interface.	port1	Port 1 as the target interface.			
Option	Description																	
lan	LAN as the target interface.																	
lo	Loopback as the target interface.																	
lte1	LTE 1 as the target interface.																	
wan	WAN as the target interface.																	
port4	Port 4 as the target interface.																	
port1	Port 1 as the target interface.																	
next-hop	Next-hop IP address in x.x.x.x format.	IPv4 address	-	none														

config router target6

Description: Configure IPv6 router targets.

```

config router target
  edit <name>
    set interface <name1>
    set next-hop <name1>
  unset
  next
  show
  abort
  end
delete <name>
purge
show
end

```

Sample command:

```

config router target6
  edit ip6.test
    set interface wan
    set next-hop 2001::100
  next
end

```

Parameter	Description	Type	Size	Default
interface	Target interface.	option		none

Parameter	Description	Type	Size	Default														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the target interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the target interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the target interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the target interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the target interface.</td> </tr> <tr> <td>port1</td> <td>Port 1 as the target interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the target interface.	lo	Loopback as the target interface.	lte1	LTE 1 as the target interface.	wan	WAN as the target interface.	port4	Port 4 as the target interface.	port1	Port 1 as the target interface.			
Option	Description																	
lan	LAN as the target interface.																	
lo	Loopback as the target interface.																	
lte1	LTE 1 as the target interface.																	
wan	WAN as the target interface.																	
port4	Port 4 as the target interface.																	
port1	Port 1 as the target interface.																	
next-hop	Next-hop IPv6 address.	IPv6 address	-	none														

config multicast

Description: Configure multicast router.

```
set join-prune-interval [1 - 65535]
set hello-interval [30 - 18724]
unset
```

- [config pim-sm-global on page 45](#)
- [config rp-address on page 45](#)
- [config interface on page 46](#)

config pim-sm-global

Description: Configure PIM sparse-mode interfaces.

config rp-address

Description: Configure static RP addresses.

```
config rp-address
  edit <rpaddressip>
    set *address <name1>
    set group <name1> *specified IPv4 subnet should be within 224.0.0.0/4 but not within
      232.0.0.0/8
    unset
  next
  show
  abort
  end
delete <rpaddressip>
```

```

    purge
    show
    end
show
end

```

config interface

Description: Configure Protocol Independent Multicast (PIM) interfaces.



There's no entry for the "set" command, although "set" is an available option.

```

config interface
  edit <name> *must be valid interface id in system interface list
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end
show
end

```

Sample command:

```

FX201E5919000057 (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 192.168.200.23
        set group 224.0.0.0/4
      next
    end
  end
config interface
end
end

```

Parameter	Description	Type	Size	Default
join-prune-interval	Interval (in seconds) between sending PIM join/prune messages.	integer	1 - 65535	60

Parameter	Description	Type	Size	Default
hello-interval	Interval (in seconds) between sending PIM hello messages .	integer	30 - 18724	30
address	RP router address.	IPv4 address	-	none
group	Groups to use this RP. (Note: The specified IPv4 subnet should be within 224.0.0.0/4, but not within 232.0.0.0/8.)	IPv4 address/netmask	-	224.0.0.0/4
interface	PIM interfaces.	string	-	none

config OSPF

Description: Configure OSPF settings.

```
config ospf
  set status [enable | disable]
  set router-id <name1>
  unset
```

Sample command:

```
config router ospf
  set status enable
  set router-id 192.168.100.127
```

Parameter	Description	Type	Size	Default						
status	Set the status of the OSPF:	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable OSPF</td> </tr> <tr> <td>disable</td> <td>Disable OSPF</td> </tr> </tbody> </table>	Option	Description	enable	Enable OSPF	disable	Disable OSPF			
Option	Description									
enable	Enable OSPF									
disable	Disable OSPF									
set 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 on page 48](#)
- [config network on page 48](#)
- [config ospf-interface on page 49](#)
- [config redistribute on page 50](#)

config area

Description: Configure OSPF area settings.

```
config area
  edit {ipv4-address}
    set
    unset
    next
    show
    abort
    end
  delete {ipv4-address}
  purge
  show
  end
```

Sample command:

```
config router ospf
  config area
    edit 0.0.0.0
```

Parameter	Description	Type	Size	Default
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

Description: Configure OSPF network settings.

```
config network
  edit <name>
    set *prefix {integer}
    set *area <name1>
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
```

```
end
```

Sample command:

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

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

config ospf-interface

Description: Configure OSPF interface settings.

```
config ospf-interface
edit <name>
set status [enable | disable]
set *interface <name1>
set mtu-ignore [enable | disable]
set cost [0 - 65535]
unset
next
show
abort
end
delete <name>
purge
```

```
show
end
```

Sample command:

```
config ospf-interface
edit 1
set status enable
set interface opaq
set mtu-ignore enable
set cost 5
end
```

Parameter	Description	Type	Size	Default
config ospf-interface	OSPF interface configuration.	option	-	none
status	Enable/Disable OSPF processing on the said interface.	option		-
	Option	Description		
	enable	Enable OSPF processing on the said interface.		
	disable	Disable OSPF processing on the said interface.		
set interface	Must be the VPN tunnel interface as OSPF is built over IPSEC VPN.			
set mtu-ignore	Prevents OSPF neighbor adjacency failure caused by mismatched MTUs.			
	Option	Description		
	enable	OSPF will stop detecting mismatched MTUs before forming OSPF adjacency		
	disable	OSPF will detect mismatched MTUs, and OSPF adjacency is not established if MTU is mismatched.		
set cost	Interface cost used to calculate the best path to reach other routers in the same area. 0 means auto-cost.	integer	0—65535	

config redistribute

Description: Configure redistribute settings.

```
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>

```

Sample command:

```

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
  end
end

```

Parameter	Description	Type	Size	Default
status	Enable/disable redistributing routes.			
set metric-type	Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).			E2
set metric	Used for the redistributed routes.	integer	1 - 16777214	10
set routemap	Route map name.			

config prefix-list

Description: Configure IPv4 prefix lists.

```

edit <name>
  set
  unset

```



The "set" command is available, but there are no settings to "set" or "unset".

- [config rule on page 52](#)

config rule

Description: Configure IPv4 prefix list rule.

```

config prefix-list
  config rule
    edit <name>
      set action [permit | deny]
      set *prefix {ipv4-subnet}
      set ge (0 - 32)
      set le (0 - 32)
      unset
      next
      show
      abort
      end
    delete <name>
  purge
  show
  end
  next
  show
  abort
  end
delete <name>
purge
show
end

```

Sample command:

```

FX201E5919000057 (prefix-list) # show
config router prefix-list
  edit 1
    config rule
      edit 1
        set action permit
        set prefix 192.168.200.0/24
        set ge 25
        set le 25
      next
    end
  next
end

```

Parameter	Description	Type	Size	Default
action	Action of the rule.	option	-	permit

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>permit</td> <td>Allow packets that match this rule.</td> </tr> <tr> <td>deny</td> <td>Deny packets that match this rule.</td> </tr> </tbody> </table>	Option	Description	permit	Allow packets that match this rule.	deny	Deny packets that match this rule.			
Option	Description									
permit	Allow packets that match this rule.									
deny	Deny packets that match this rule.									
prefix	IPv4 prefix to define the regular filter criteria.	IPv4 address/netmask	-	none						
ge	Minimum prefix length to be matched.	integer	0 - 32	none						
le	Maximum prefix length to be matched.	integer	0 - 32	none						

config route-map

Description: Configure route maps.

```
edit <name>
  set
  unset
```

- [config rule on page 53](#)

config rule

Description: Configure route map rule.

```
config rule
  edit <name>
    set action [permit | deny]
    set match-ip-address {ipv4-address}
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end
delete <name>
purge
show
end
show
end
```

Sample command:

```

FX201E5919000057 (route-map) # show
config router route-map
  edit 1
    config rule
      edit 1
        set action permit
        set match-ip-address 1
      next
    end
  next
end

```

Parameter	Description	Type	Size	Default						
action	Action of the rule.	option	-	permit						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>permit</td> <td>Allow packets that match this rule.</td> </tr> <tr> <td>deny</td> <td>Deny packets that match this rule.</td> </tr> </tbody> </table>				Option	Description	permit	Allow packets that match this rule.	deny	Deny packets that match this rule.
Option	Description									
permit	Allow packets that match this rule.									
deny	Deny packets that match this rule.									
match-ip-address	Match IP address permitted by the prefix-list.	string	-	none						

System

This section shows the syntax of the following commands:

- [config system global on page 56](#)
- [config system accprofile on page 57](#)
- [config admin on page 60](#)
- [config system bluetooth on page 63](#)
- [config system management on page 63](#)
- [config system interface on page 69](#)
- [config system dhcpserver on page 82](#)
- [config system dhcp6server on page 86](#)
- [config dhcprelay on page 89](#)
- [config dns on page 90](#)
- [config dns-server on page 92](#)
- [config dns-database on page 93](#)
- [config dns-entry on page 94](#)
- [config vwan-member on page 96](#)
- [config sms-notification on page 99](#)
- [config sms-remote-diag on page 101](#)
- [config syslog on page 103](#)
- [config virtual-wire-pair on page 107](#)
- [config api-user on page 107](#)
- [config ntp on page 108](#)
- [config settings on page 110](#)
- [config system lan-switch on page 110](#)
- [config system switch-interface on page 112](#)
- [config system ipsec on page 114](#)
- [config ssh-crypto on page 114](#)
- [config system automation trigger on page 116](#)
- [config system automation action on page 117](#)
- [config system automation stitch on page 118](#)
- [config system digital-io digital on page 120](#)
- [config system digital-io alert on page 120](#)
- [config system digital-io action on page 122](#)
- [config system 802-1X-settings on page 123](#)
- [config system ignition-sensing on page 123](#)
- [config system obm-console on page 124](#)

config system global

Description: Configure FortiExtender global settings.

```
config system global
  set hostname {string}
  set timezone [0 - 87]
  set auto-install-image [enable | disable]
  set default-image-file {string} *available when auto-install-image is enabled
  set mdm-fw-server {string}
  set os-fw-server {string}
  set admin-server-cert {string}
end
```

Sample command:

```
FX201E5919000057 (global) # show
config system global
  set hostname FX201E5919000057
  set timezone 80
  set auto-install-image disable
  set mdm-fw-server fortiextender-firmware.forticloud.com
  set os-fw-server fortiextender-firmware.forticloud.com
  set admin-server-cert my_fex_cert
end
```

Parameter	Description	Type	Size	Default
hostname	Device display name.	string	-	none
timezone	System timezone setting. (Note: Use the 'get timezone list' command to check the timezone ID.)	integer	0 - 87	80
auto-install-image	Automatically install image from USB.	option	-	disable
	Option	Description		
	enable	Enable auto-install-image.		
	disable	Disable auto-install-image.		
default-image-file	Image file from USB.	string	-	none

Parameter	Description	Type	Size	Default
mdm-fw-server	Cloud modem image upgrade URL.	string	-	fortiextender-firmware.forticloud.com
os-fw-server	Cloud OS image upgrade URL.	string	-	fortiextender-firmware.forticloud.com
admin-server-cert	Server certificate that the FortiExtender uses for HTTPS administrative connections.	string	-	Fortinet_Factory_Backup

config system accprofile

Description: Configure administration access profiles.

```

config system accprofile
  edit <name>
    set header [read-write | read | no-access]
    set firewall [read-write | read | no-access]
    set lte [read-write | read | no-access]
    set router [read-write | read | no-access]
    set dnsfilter [read-write | read | no-access]
    set system [read-write | read | no-access]
    set snmp [read-write | read | no-access]
    set hmon [read-write | read | no-access]
    set vpn [read-write | read | no-access]
    set network [read-write | read | no-access]
    set wifi [read-write | read | no-access]
    set user [read-write | read | no-access]
    unset
  next
  show
  abort
end
delete <name>
purge
show
end

```

Parameter	Description	Type	Size	Default
header	Header settings.	option	-	read
	Option	Description		
	read-write	Read-write access.		

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>read</td> <td>Read access.</td> </tr> <tr> <td>no-access</td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	read	Read access.	no-access	No access.					
Option	Description											
read	Read access.											
no-access	No access.											
firewall	Firewall configuration.	option	-	read								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>read-write</td> <td>Read-write access.</td> </tr> <tr> <td>read</td> <td>Read access.</td> </tr> <tr> <td>no-access</td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	read-write	Read-write access.	read	Read access.	no-access	No access.			
Option	Description											
read-write	Read-write access.											
read	Read access.											
no-access	No access.											
lte	LTE configuration.	option	-	read								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>read-write</td> <td>Read-write access.</td> </tr> <tr> <td>read</td> <td>Read access.</td> </tr> <tr> <td>no-access</td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	read-write	Read-write access.	read	Read access.	no-access	No access.			
Option	Description											
read-write	Read-write access.											
read	Read access.											
no-access	No access.											
router	Router configuration.	option	-	read								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>read-write</td> <td>Read-write access.</td> </tr> <tr> <td>read</td> <td>Read access.</td> </tr> <tr> <td>no-access</td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	read-write	Read-write access.	read	Read access.	no-access	No access.			
Option	Description											
read-write	Read-write access.											
read	Read access.											
no-access	No access.											
dnsfilter	DNS filter configuration.	option	-	read								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>read-write</td> <td>Read-write access.</td> </tr> <tr> <td>read</td> <td>Read access.</td> </tr> <tr> <td>no-access</td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	read-write	Read-write access.	read	Read access.	no-access	No access.			
Option	Description											
read-write	Read-write access.											
read	Read access.											
no-access	No access.											
system	System configuration.	option	-	read								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>read-write</td> <td>Read-write access.</td> </tr> <tr> <td>read</td> <td>Read access.</td> </tr> <tr> <td>no-access</td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	read-write	Read-write access.	read	Read access.	no-access	No access.			
Option	Description											
read-write	Read-write access.											
read	Read access.											
no-access	No access.											

Parameter	Description	Type	Size	Default
snmp	SNMP configuration.	option	-	read
	Option	Description		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		
hmon	Health monitor configuration.	option	-	read
	Option	Description		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		
vpn	VPN configuration.	option	-	read
	Option	Description		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		
network	Network configuration.	option	-	read
	Option	Description		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		
wifi	Wi-Fi configuration (on Wi-Fi capable models only)	option	-	read
	Option	Description		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		
user	User configuration.	option	-	read

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>read-write</td> <td>Read-write access.</td> </tr> <tr> <td>read</td> <td>Read access.</td> </tr> <tr> <td>no-access</td> <td>No access.</td> </tr> </tbody> </table>	Option	Description	read-write	Read-write access.	read	Read access.	no-access	No access.			
Option	Description											
read-write	Read-write access.											
read	Read access.											
no-access	No access.											

config admin

Description: Configure user access.

```

config admin
  edit <name>
    set *accprofile <name1>
    set remote-auth {enable | disable}
    set wildcard {enable | disable}
    set *password {string}
    set remote-group {group name}
    set trusthost1 {ipv4-address}
    set trusthost2 {ipv4-address}
    set trusthost3 {ipv4-address}
    set trusthost4 {ipv4-address}
    set trusthost5 {ipv4-address}
    set trusthost6 {ipv4-address}
    set trusthost7 {ipv4-address}
    set trusthost8 {ipv4-address}
    set trusthost9 {ipv4-address}
    set trusthost10 {ipv4-address}
  next
end

```

Sample command:

```

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 192.168.200.110/24
    set trusthost2
    set trusthost3
    set trusthost4

```

```

set trusthost5
set trusthost6
set trusthost7
set trusthost8
set trusthost9
set trusthost10
next
end

```

Parameter	Description	Typy	Size	Default
accprofile	Access profile.	string	-	none
remote-auth	Enable/disable authentication using a remote RADIUS server	option	-	disable
wildcard	<p>Enable/disable wildcard RADIUS authentication</p> <p>Note: If <code>wildcard</code> 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.</p> <p>Only one wildcard remote account is allowed to exist under <code>system admin</code>.</p>	option	-	disable
password	<p>Admin user password</p> <p>Note: If <code>wildcard</code> is enabled, you cannot set a password.</p>	string	-	none
remote-group	<p>Enter the FortiExtender user group name you want to use for remote authentication.</p> <p>Note: If <code>remote-auth</code> is enabled, <code>remote-group</code> becomes mandatory. Otherwise <code>remote-group</code> is hidden.</p> <p>If <code>remote-auth</code> is enabled but <code>wildcard</code> 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.</p>	option	-	none
trusthost1	Address or subnet address and netmask from which the	IPv4 address	-	none

Parameter	Description	Typy	Size	Default
Trusthost2	administrator can connect to the device. Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost3	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost4	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost5	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost6	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost7	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost8	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost9	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost10	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none

config system bluetooth

Description: Configure Bluetooth settings on BLE capable FortiExtenders.

```
config system bluetooth
  set status {enable | disable}
end
```

Sample command:

```
config system bluetooth
  set status enable
end
```

Parameter	Description	Type	Size	Default						
status	Enable or disable the Bluetooth button on applicable FortiExtender models.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the Bluetooth button. The Bluetooth button can be triggered to provide Bluetooth functionality.</td> </tr> <tr> <td>disable</td> <td>Disable the Bluetooth button. Pressing the Bluetooth button will not trigger anything.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the Bluetooth button. The Bluetooth button can be triggered to provide Bluetooth functionality.	disable	Disable the Bluetooth button. Pressing the Bluetooth button will not trigger anything.			
Option	Description									
enable	Enable the Bluetooth button. The Bluetooth button can be triggered to provide Bluetooth functionality.									
disable	Disable the Bluetooth button. Pressing the Bluetooth button will not trigger anything.									

config system management

Description: Configure Extender management settings.

```
config system management
  set discovery-type [auto | fortigate | cloud | local]
unset
```

Sample command

```
set discovery-type fortigate
```

Parameter	Description	Type	Size	Default
discovery-type	AC discovery type.	option	-	auto

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>Automatic.</td> </tr> <tr> <td>fortigate</td> <td>FortiGate.</td> </tr> <tr> <td>cloud</td> <td>FortiExtender Cloud.</td> </tr> <tr> <td>local</td> <td>Local.</td> </tr> </tbody> </table>	Option	Description	auto	Automatic.	fortigate	FortiGate.	cloud	FortiExtender Cloud.	local	Local.			
Option	Description													
auto	Automatic.													
fortigate	FortiGate.													
cloud	FortiExtender Cloud.													
local	Local.													

- [config fortigate on page 64](#)
- [config cloud on page 65](#)
- [config system management local on page 66](#)
- [config local-access on page 66](#)
- [config fortigate-backup on page 67](#)

config fortigate

Description: Configure FortiGate settings.

```

set ac-discovery-type [static | broadcast]
  config static-ac-addr *only accessible when ac-discovery-type is static
    edit <name>
      set server <name>
    next
  end
set ac-ctl-port [1024 - 49150]
set ac-data-port [1024 - 49150]
set discovery-intf <name1>
set ingress-intf <name1>
unset
show
end

```

Parameter	Description	Type	Size	Default						
ac-discovery-type	The method that the device uses to discover the AC, i.e., FortiGate.	option	-	broadcast						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>broadcast</td> <td>Broadcast.</td> </tr> <tr> <td>static</td> <td>Static IP address.</td> </tr> </tbody> </table>	Option	Description	broadcast	Broadcast.	static	Static IP address.			
Option	Description									
broadcast	Broadcast.									
static	Static IP address.									
server	IP address or hostname of the AC server.	string	-	none						
ac-ctl-port	CAPWAP control port of the AC	integer	1024 - 49150	5246						

Parameter	Description	Type	Size	Default										
	server.													
ac-data-port	CAPWAP data port of the AC server.	integer	1024 - 49150	5246										
discovery-intf	The physical port from which FortiExtender sends broadcast packets in search for FortiGate.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the discovery interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the discovery interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the discovery interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the discovery interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the discovery interface.	lte1	LTE 1 as the discovery interface.	wan	WAN as the discovery interface.	port4	Port 4 as the discovery interface.			
Option	Description													
lan	LAN as the discovery interface.													
lte1	LTE 1 as the discovery interface.													
wan	WAN as the discovery interface.													
port4	Port 4 as the discovery interface.													

config cloud

Description: Configure Cloud settings.

```

config cloud
  set dispatcher {string}
  set dispatcher-port {integer}
  set mode [ip-passthrough | nat]
  set proxy [enable | disable]
  set proxy-server {ipv4-address} *available when proxy is enabled
  set proxy-port [1 - 65535] *available when proxy is enabled
  unset
  show
end

```

Parameter	Description	Type	Size	Default						
dispatcher	Cloud dispatch URL.	string	-	fortiextender-dispatch.forticloud.com						
dispatcher-port	Cloud dispatch port.	integer	0 - 9223372036854775807	443						
mode	Networking mode.	option	-	nat						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>nat</td> <td>NAT.</td> </tr> <tr> <td>ip-passthrough</td> <td>IP-passthrough.</td> </tr> </tbody> </table>	Option	Description	nat	NAT.	ip-passthrough	IP-passthrough.			
Option	Description									
nat	NAT.									
ip-passthrough	IP-passthrough.									
proxy	Status of proxy connection.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable proxy.</td> </tr> <tr> <td>disable</td> <td>Disable proxy.</td> </tr> </tbody> </table>	Option	Description	enable	Enable proxy.	disable	Disable proxy.			
Option	Description									
enable	Enable proxy.									
disable	Disable proxy.									
proxy-server	Proxy server IP address.	IPv4 address	-	none						
proxy-port	Socks5 proxy port.	integer	1 - 65535	1080						

config system management local

Description: Configure local settings.

```
config system management local
  set mode [ip-passthrough | nat]
  set modem-offload [disable | enable]
  unset
  show
end
```

Parameter	Description	Type	Size	Default						
mode	Networking mode.	option	-	nat						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>nat</td> <td>NAT.</td> </tr> <tr> <td>ip-passthrough</td> <td>IP-passthrough.</td> </tr> </tbody> </table>	Option	Description	nat	NAT.	ip-passthrough	IP-passthrough.			
Option	Description									
nat	NAT.									
ip-passthrough	IP-passthrough.									
modem-offload	Enable/disable LTE/5G traffic offload This feature takes effect when FortiExtender is working in local mode with NAT enabled.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable LTE/5G traffic offload.</td> </tr> <tr> <td>disable</td> <td>Disable LTE/5G traffic offload.</td> </tr> </tbody> </table>	Option	Description	enable	Enable LTE/5G traffic offload.	disable	Disable LTE/5G traffic offload.			
Option	Description									
enable	Enable LTE/5G traffic offload.									
disable	Disable LTE/5G traffic offload.									

config local-access

Description: Configure administrative access settings.

```

config local-access
  set http [1 - 65535]
  set https [1 - 65535]
  set ssh [1 - 65535]
  set telnet [1 - 65535]
  set idle-timeout [1 - 480]
unset
show
end

```

Parameter	Description	Type	Size	Default
http	HTTP port number.	integer	1 - 65535	80
https	HTTPS port number.	integer	1 - 65535	443
ssh	SSH port number.	integer	1 - 65535	22
telnet	Telnet port number.	integer	1 - 65535	23
idle-timeout	The number of minutes before an idle administrator session times out.	integer	1 - 480	5

config fortigate-backup

Description: Configure backup feature.

```

config fortigate-backup
  set vrrp-interface <name1>
  set status [enable | disable]
unset
show
end
show
end

```

Parameter	Description	Type	Size	Default
vrrp-interface	VRRP interface.	option	-	none
	Option	Description		
	lan	LAN as vrrp-interface.		
	lo	Loopback as vrrp-interface.		
	lte1	LTE 1 as vrrp-interface.		
	wan	WAN as vrrp-interface.		

Parameter	Description	Type	Size	Default
status	Status of the VRRP interface.	option	-	disable
	Option	Description		
	enable	Enable the VRRP interface.		
	disable	Disable the VRRP interface.		

Sample command:

```

FX201E5919000057 (management) # show
config system management
  set discovery-type auto
  config fortigate
    set ac-discovery-type static
    edit 1
      set server 10.107.41.66
    next
  set ac-ctl-port 5246
  set ac-data-port 25246
  set discovery-intf lan
  set ingress-intf
end

config cloud
  set dispatcher fortiextender-dispatch.forticloud.com
  set dispatcher-port 443
  set mode nat
  set proxy enable
  set proxy-server 10.107.34.22
  set proxy-port 3453
end

config local
  set mode nat
end

config local-access
  set http 80
  set https 443
  set ssh 22
  set telnet 23
  set idle-timeout 5
end

config fortigate-backup
  set vrrp-interface wan
  set status enable

```

```
end
end
```

config system interface

Description: Configure system interface settings.

```
config system interface
  edit <name>
    set *type [loopback | virtual-wan | vlan | capwap | dummy]
    set status [up| down]
    set mode [static | dhcp]
    set ip {ipv4-address}
    set gateway {ipv4-address}
    set mtu-override [enable | disable]
    set mtu [512-1500] *available when mtu-override is set to enable
    set distance [1 - 512]
    set vrrp-virtual-mac [enable | disable]
    set allowaccess {option1}, {option2}, ...
    set security-mode [none|captive-portal]
    set security-external-web {string}
    set security-groups <name1>, <name2>, ...
    set security-exempt-list {string}
    set security-exempt-list6 {string}
    set security-redirect-url {string}
    set defaultgw [enable | disable] *available when mode is set to dhcp
    set dns-server-override [enable | disable] *available when mode is set to dhcp
    set redundant-by [priority | cost] *available when type is set to virtual-wan
    set algorithm [redundant | WRR] *available when type is set to virtual-wan
    set FEC [source_ip | dest_ip | source_dest_ip_pair | connection] *available when type is set
to virtual-wan
    set session-timeout [0 - 86400] *available when type is set to virtual-wan
    set grace-period [0 - 10000000] *available when type is set to virtual-wan
    set members <name1>, <name2>, ...*available when type is set to virtual-wan
    set rid [1 | 2] *available when type is set to capwap
    set *vid [1 - 4089] *available when type is set to vlan
    set *ingress-intf <name1>
  unset
```

Parameter	Description	Type	Size	Default
type	Interface type.	option	-	none
	Option	Description		
	loopback	Loopback interface.		

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>virtual-wan</td> <td>Virtual-WAN interface.</td> </tr> <tr> <td>vlan</td> <td>VLAN interface.</td> </tr> <tr> <td>capwap</td> <td>CAPWAP interface.</td> </tr> <tr> <td>dummy</td> <td>Dummy interface.</td> </tr> </tbody> </table>	Option	Description	virtual-wan	Virtual-WAN interface.	vlan	VLAN interface.	capwap	CAPWAP interface.	dummy	Dummy interface.			
Option	Description													
virtual-wan	Virtual-WAN interface.													
vlan	VLAN interface.													
capwap	CAPWAP interface.													
dummy	Dummy interface.													
status	Interface status.	option	-	up										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>up</td> <td>Bring the interface up.</td> </tr> <tr> <td>down</td> <td>Bring the interface down.</td> </tr> </tbody> </table>	Option	Description	up	Bring the interface up.	down	Bring the interface down.							
Option	Description													
up	Bring the interface up.													
down	Bring the interface down.													
mode	Addressing mode.	option	-	static										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>static</td> <td>Static mode.</td> </tr> <tr> <td>dhcp</td> <td>DHCP mode.</td> </tr> </tbody> </table>	Option	Description	static	Static mode.	dhcp	DHCP mode.							
Option	Description													
static	Static mode.													
dhcp	DHCP mode.													
ip	Interface IP address and subnet mask (in x.x.x.x/24 format).	IPv4 address	-	none										
gateway	Interface's connected gateway.	string	-	none										
mtu-override	Status of MTU override.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable MTU override.</td> </tr> <tr> <td>disable</td> <td>Disable MTU override.</td> </tr> </tbody> </table>	Option	Description	enable	Enable MTU override.	disable	Disable MTU override.							
Option	Description													
enable	Enable MTU override.													
disable	Disable MTU override.													
mtu	MTU value for the interface.	integer	512 - 1500	1500										
distance	Route metric of the interface gateway.	integer	1 - 512	5										
vrrp-virtual-mac	Use of virtual MAC for VRRP.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable VRRP virtual MAC.</td> </tr> <tr> <td>disable</td> <td>Disable VRRP virtual MAC.</td> </tr> </tbody> </table>	Option	Description	enable	Enable VRRP virtual MAC.	disable	Disable VRRP virtual MAC.							
Option	Description													
enable	Enable VRRP virtual MAC.													
disable	Disable VRRP virtual MAC.													
allowaccess	Types of management access allowed to this interface.	option	-	none										

Parameter	Description	Type	Size	Default						
security-mode	Turn on captive portal authentication for this interface.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>none</td> <td>No security option.</td> </tr> <tr> <td>captive-portal</td> <td>Captive portal authentication.</td> </tr> </tbody> </table>	Option	Description	none	No security option.	captive-portal	Captive portal authentication.			
Option	Description									
none	No security option.									
captive-portal	Captive portal authentication.									
security-external-web	URL of external authentication web server.	string	Maximum length: 255	-						
security-groups	Names of user groups that can authenticate with the captive portal.	option	-	-						
security-exempt-list	Name of security-exempt-list.	option	-	-						
security-exempt-list6	Name of security-exempt-list6.	option	-	-						
security-redirect-url	URL redirection after disclaimer/authentication.	string	Maximum length: 255	-						
defaultgw	Ability to get the gateway IP from the DHCP server.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable getting the gateway IP from the DHCP server.</td> </tr> <tr> <td>disable</td> <td>Disable getting the gateway IP from the DHCP server.</td> </tr> </tbody> </table>	Option	Description	enable	Enable getting the gateway IP from the DHCP server.	disable	Disable getting the gateway IP from the DHCP server.			
Option	Description									
enable	Enable getting the gateway IP from the DHCP server.									
disable	Disable getting the gateway IP from the DHCP server.									
dns-server-override	Use DNS acquired by DHCP.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable DNS server override.</td> </tr> <tr> <td>disable</td> <td>Disable DNS server override.</td> </tr> </tbody> </table>	Option	Description	enable	Enable DNS server override.	disable	Disable DNS server override.			
Option	Description									
enable	Enable DNS server override.									
disable	Disable DNS server override.									
redundant-by	Use of the benchmark for redundant algorithm.	option	-	priority						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>priority</td> <td>Redundant by priority.</td> </tr> <tr> <td>cost</td> <td>Redundant by cost.</td> </tr> </tbody> </table>	Option	Description	priority	Redundant by priority.	cost	Redundant by cost.			
Option	Description									
priority	Redundant by priority.									
cost	Redundant by cost.									
algorithm	LLB algorithm.	option	-	redundant						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>redundant</td> <td>Redundant as algorithm.</td> </tr> <tr> <td>WRR</td> <td>WRR as algorithm.</td> </tr> </tbody> </table>	Option	Description	redundant	Redundant as algorithm.	WRR	WRR as algorithm.									
Option	Description															
redundant	Redundant as algorithm.															
WRR	WRR as algorithm.															
FEC	Forward equivalence class.	option	-	source_ip												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>source_ip</td> <td>Forward equivalence class by source IP.</td> </tr> <tr> <td>dest_ip</td> <td>Forward equivalence class by destination IP.</td> </tr> <tr> <td>source_dest_ip_pair</td> <td>Forward equivalence class by source and destination IP pair.</td> </tr> <tr> <td>connection</td> <td>Forward equivalence class by connection.</td> </tr> </tbody> </table>	Option	Description	source_ip	Forward equivalence class by source IP.	dest_ip	Forward equivalence class by destination IP.	source_dest_ip_pair	Forward equivalence class by source and destination IP pair.	connection	Forward equivalence class by connection.					
Option	Description															
source_ip	Forward equivalence class by source IP.															
dest_ip	Forward equivalence class by destination IP.															
source_dest_ip_pair	Forward equivalence class by source and destination IP pair.															
connection	Forward equivalence class by connection.															
session-timeout	FEC session timeout in seconds.	integer	0 - 86400	60												
grace-period	Grace period measured in seconds before failback.	integer	0 - 10000000	0												
members	Link members of virtual WAN.	option	-	none												
rid	CAPWAP virtual interface ID.	integer	1, 2	1												
vid	VLAN ID.	integer	1 - 4089	0												
ingress-intf	CAPWAP or VLAN interface's parent interface.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the ingress interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the ingress interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the ingress interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the ingress interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the ingress interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the ingress interface.	lo	Loopback as the ingress interface.	lte1	LTE 1 as the ingress interface.	wan	WAN as the ingress interface.	port4	Port 4 as the ingress interface.			
Option	Description															
lan	LAN as the ingress interface.															
lo	Loopback as the ingress interface.															
lte1	LTE 1 as the ingress interface.															
wan	WAN as the ingress interface.															
port4	Port 4 as the ingress interface.															
Sfp-dsl	sfp-dsl status	option	-	disable												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable sfp-dsl.</td> </tr> <tr> <td>disable</td> <td>Disable sfp-dsl.</td> </tr> </tbody> </table>	Option	Description	enable	Enable sfp-dsl.	disable	Disable sfp-dsl.									
Option	Description															
enable	Enable sfp-dsl.															
disable	Disable sfp-dsl.															
Autodect	Enable/disable sfp-dsl auto-detect.	option	-	enable												
Phy-mode	DSL physical mode.	option	-	vdsl												

Parameter	Description	Type	Size	Default
	Option	Description		
	Vdsl			
	Adsl			

- [config VRRP on page 73](#)
- [config ipv6 on page 74](#)

config VRRP

Description: Configure the VRRP settings.

```

config system interface
  edit <name>
    config vrrp
      set status [enable | disable]
      set version [2]
      set *ip {ipv4-address}
      set *id [1 - 255]
      set priority [1 - 255]
      set adv-interval [1 - 255]
      set start-time [1 - 255]
      set preempt [enable | disable]
    unset
  show
end
next
show
abort
end
delete <name>
purge
show
end

```

Sample command:

```

FX201E5919000057 (interface) # show
config system interface
  edit wan
    set type physical
    set status up
    set mode dhcp
    set mtu-override enable
    set mtu 1500
    set distance 5

```

```

set vrrp-virtual-mac disable
config vrrp
    set status enable
    set version 2
    set ip 192.168.100.25
    set id 5
    set priority 1
    set adv-interval 23
    set start-time 33
    set preempt enable
end
set allowaccess http https ping snmp ssh telnet
set defaultgw enable
set dns-server-override enable
next
end

```

Parameter	Description	Type	Size	Default
status	Status of the VRRP configuration.	option	-	disable
	Option	Description		
	enable	Enable the VRRP configuration.		
	disable	Disable VRRP configuration.		
version	VRRP version.	integer	2	2
ip	IP address of the virtual router.	IPv4 address	-	none
id	ID of the virtual router.	integer	1 - 255	0
priority	Priority of the virtual router.	integer	1 - 255	100
adv-interval	Advertisement interval.	integer	1 - 255	1
start-time	Start-up time.	integer	1 - 255	1
preempt	Preempt mode.	option	-	disable
	Option	Description		
	enable	Enable preempt mode.		
	disable	Disable preempt mode.		

config ipv6

Description: Configure the IPv6 interface settings.

```
config system interface
edit <name>
  config ipv6
    set status [enable | disable]
    set ip6-mode [static | dhcp | pppoe | delegated]
    set autoconf [enable | disable]
    set ip6-send-adv [enable | disable]
    set ip6-manage-flag [enable | disable]
    set ip6-other-flag [enable | disable]
    set ip6-max-interval <4-1800>
    set ip6-min-interval <3-1350>
    set ip6-address {ipv6-address}
    set ip6-adv-rio [enable | disable]
    set ip6-route-pref [low | medium | high]
    set ip6-gw {ipv6-address}
    set ip6-upstream-interface [option1 | ...]
    set ip6-allowaccess [http | https | ping | snmp | ssh]
    set distance {number}
    config ip6-prefix-list
      edit <name>
        set ip6-prefix {ipv6-address}
      next
    end
    config ip6-rdnss-list
      edit <name>
        set ip6-rdnss {ipv6-address}
      next
    end
  end
end
next
end
```

Sample command:

```
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::/64
    set ip6-gw ::
    set ip6-allowaccess http https ping snmp ssh
    set distance 10
  config ip6-prefix-list
```

```

edit 1
  set ip6-prefix 2001:2:3::/64
next
end
config ip6-rdnss-list
  edit 1
    set ip6-rdnss 3:5a:78::
  next
end
end
next
end

```

Parameter	Description	Type	Size	Default										
status	Status of the interface.	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the</td> </tr> <tr> <td>disable</td> <td>Disable</td> </tr> </tbody> </table>	Option	Description	enable	Enable the	disable	Disable							
Option	Description													
enable	Enable the													
disable	Disable													
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>static</td> <td>Static setting.</td> </tr> <tr> <td>dhcp</td> <td>DHCPv6 client mode.</td> </tr> <tr> <td>pppoe</td> <td>IPv6 over PPPoE mode.</td> </tr> <tr> <td>delegated</td> <td>IPv6 address with delegated prefix.</td> </tr> </tbody> </table>	Option	Description	static	Static setting.	dhcp	DHCPv6 client mode.	pppoe	IPv6 over PPPoE mode.	delegated	IPv6 address with delegated prefix.			
Option	Description													
static	Static setting.													
dhcp	DHCPv6 client mode.													
pppoe	IPv6 over PPPoE mode.													
delegated	IPv6 address with delegated prefix.													
autoconf	Enable/disable address auto config.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable auto-configuration.</td> </tr> <tr> <td>disable</td> <td>Disable auto-configuration.</td> </tr> </tbody> </table>	Option	Description	enable	Enable auto-configuration.	disable	Disable auto-configuration.							
Option	Description													
enable	Enable auto-configuration.													
disable	Disable auto-configuration.													
ip6-send-adv	Enable/disable sending router advertisement (RA) messages about the interface.	option	-	disable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable sending RA messages about this interface.</td> </tr> <tr> <td>disable</td> <td>Disable sending RA messages about this interface.</td> </tr> </tbody> </table>	Option	Description	enable	Enable sending RA messages about this interface.	disable	Disable sending RA messages about this interface.							
Option	Description													
enable	Enable sending RA messages about this interface.													
disable	Disable sending RA messages about this interface.													
ip6-manage-flag	Specify whether to set an M-flag	option		disable										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the M-flag.</td> </tr> <tr> <td>disable</td> <td>Disable the M-flag.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the M-flag.	disable	Disable the M-flag.					
Option	Description											
enable	Enable the M-flag.											
disable	Disable the M-flag.											
ip6-other-flag	Specify whether to set an O-flag.	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the O-flag.</td> </tr> <tr> <td>disable</td> <td>Disable the O-flag.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the O-flag.	disable	Disable the O-flag.					
Option	Description											
enable	Enable the O-flag.											
disable	Disable the O-flag.											
ip6-max-interval	Specify maximum RA sending interval.	integer	4-1800	600								
ip6-min-interval	Specify minimum RA sending interval.	integer	3-1350	600								
ip6-address	Primary IPv6 address prefix.	IPv6-prefix	-	::/0								
ip6-adv-rio	Specify whether to enable router information option	option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable router information option.</td> </tr> <tr> <td>disable</td> <td>Disable router information option.</td> </tr> </tbody> </table>	Option	Description	enable	Enable router information option.	disable	Disable router information option.					
Option	Description											
enable	Enable router information option.											
disable	Disable router information option.											
ip6-route-pref	Specify router preference level. This option is hidden when ip6-adv-rio disabled.	option	-	medium								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>low</td> <td>Set the router preference level to low.</td> </tr> <tr> <td>medium</td> <td>Set the router preference level to medium.</td> </tr> <tr> <td>high</td> <td>Set the router preference level to high.</td> </tr> </tbody> </table>	Option	Description	low	Set the router preference level to low.	medium	Set the router preference level to medium.	high	Set the router preference level to high.			
Option	Description											
low	Set the router preference level to low.											
medium	Set the router preference level to medium.											
high	Set the router preference level to high.											
ip6-upstream-interface	Specify the IPv6 interface name providing delegated information. This option is available when ip6-mode is set to delegate.	option	-	-								
ip6-gw	IPv6 Gateway. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.	string	ipv6-address	::								
ip6-allowaccess	Allow management access to the interface.	option	-									

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>http</td> <td>HTTP access.</td> </tr> <tr> <td>https</td> <td>HTTPS access.</td> </tr> <tr> <td>ping</td> <td>PING access.</td> </tr> <tr> <td>snmp</td> <td>SNMP access.</td> </tr> <tr> <td>ssh</td> <td>SSH access.</td> </tr> </tbody> </table>	Option	Description	http	HTTP access.	https	HTTPS access.	ping	PING access.	snmp	SNMP access.	ssh	SSH access.			
Option	Description															
http	HTTP access.															
https	HTTPS access.															
ping	PING access.															
snmp	SNMP access.															
ssh	SSH access.															
distance	Route metric of the interface gateway.	number	1-255	10												
ip6-prefix-list	Specify the RA prefix info. You can create multiple prefixes.	table	-	null												
ip6-rdnss-list	Specify the RA DNS service info. You can create multiple DNS entries.	table	-	null												

config system vxlan

Description: Configure VXLAN devices

```

config system vxlan
  edit <name>
    set *vni [1 - 16777215]
    set *remote-ip {ipv4-address}
    set *local-ip {ipv4-address}
    set dstport [1 - 65535]
  unset
  next
  show
  abort
  end
  delete <name>
  purge
  show
  end

```

Sample command:

```

FX201E5919000057 (vxlan) # show
config system vxlan
  edit 1
    set vni 500
    set remote-ip 192.168.201.1
    set local-ip 192.168.200.1

```

```

    set dstport 4789
  next
end

```

Parameter	Description	Type	Size	Default
vni	VXLAN network ID.	integer	1 - 1677721	0
remote-ip	IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN.	IPv4 address	-	none
local-ip	IPv4 address of the VXLAN interface on the device at the local end of the VXLAN.	IPv4 address	-	none
dstport	VXLAN destination port.	integer	1 - 65535	4789

config system aggregate-interface

Description: Configure the aggregate interface. Each table entry indicates an aggregate interface to be created and one or more interfaces can be aggregated under this aggregate interface.

```

config system aggregate-interface
  edit <name>
    set mode [activebackup | loadbalance]
    config members
    next
    set mapping-timeout [0 - 86400] *available when mode is set to load balance
  unset

```

Sample command:

```

config system aggregate-interface
  edit agg1
    set mode loadbalance
    set mapping-timeout 60
    config members
  end
next

```

- [config members on page 80](#)

config members

Description: Configure interfaces to be aggregated.

```
config system aggregate-interface
  edit <name>
    config members
      edit <name>
        set *interface <name1>
        set weight [1 - 256]
        set health-check-event
        set health-check-fail-cnt [1 - 10]
        set health-check-recovery-cnt [1 - 10]
      unset
    next
  show
  abort
end
delete <name>
purge
show
end
next
show
abort
end
delete <name>
purge
show
end
```

Sample command:

```
config system aggregate-interface
  edit agg1
    set mode loadbalance
    set mapping-timeout 244
    config members
      edit 23
        set interface port4
        set weight 1
        set health-check-event
        set health-check-fail-cnt 5
        set health-check-recovery-cnt 5
      next
    end
  next
end
```

Parameter	Description	Type	Size	Default
mode	Aggregate interface mode.	option	-	activebackup
	Option	Description		
	activebackup	Active backup.		
	loadbalance	Load balance.		
mapping-timeout	source-mac-to-member mapping timeout in seconds.	integer	0 - 86400	60
interface	Member interface.	option	-	none
weight	Member weight in load balancing.	integer	1 - 256	1
health-check-event	Member monitor.	option	-	none
health-check-fail-cnt	Number of failures before the member is considered dead.	integer	1 - 10	5
health-check-recovery-cnt	Number of successes before the member is considered alive.	integer	1 - 10	5

config pppoe-interface

Description: Configure the aggregate interface.

```
config pppoe-interface
edit <name>
set status [up | down]
set device <name1>
set username {string}
set password {string}
unset
```

Sample command:

```
config system pppoe-interface
edit pppoe1
set status up
set device port1
set username test
```

```

set password *****
next
end

```

Parameter	Description	Type	Size	Default
status	Bring the PPPoE up or down	option	-	up
	Option	Description		
	up	Set interface status up.		
	down	Set interface status down.		
device	Name of the physical interface	option	-	none
username	The ISP provided username of the PPPoE account.	string	-	none
password	The PPPoE account's password.	string	-	none

config system dhcpserver

Description: Configure DHCP servers.

```

config system dhcpserver
  edit <name>
    set status [enable | disable | backup]
    set lease-time [300 - 8640000]
    set dns-service [default | specify | wan-dns | local]
    set dns-server1 {ipv4-address} *available when dns-service is set to specify
    set dns-server2 {ipv4-address} *available when dns-service is set to specify
    set dns-server3 {ipv4-address} *available when dns-service is set to specify
    set ntp-service [local | default| specify]
    set ntp-server1 {ipv4-address}
    set ntp-server2 {ipv4-address}
    set ntp-server3 {ipv4-address}
    set *default-gateway {ipv4-address}
    set *netmask {netmask}
    set *interface <name1>
    set *start-ip {ipv4-address}
    set *end-ip {ipv4-address}
    set mtu [512 - 9000]
    set reserved-address [enable | disable]
  unset

```

Sample command:

```

config system dhcpserver
  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 port4
    set start-ip 192.168.200.110
    set end-ip 192.168.200.210
    set mtu 1500
    set reserved-address disable
  next
end

```

Parameter	Description	Type	Size	Default										
status	Status of the DHCP configuration.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the DHCP server.</td> </tr> <tr> <td>disable</td> <td>Disable the DHCP server.</td> </tr> <tr> <td>backup</td> <td>Enable in VRRP backup mode. (Note: The DHCP server is launched only when the VRRP primary goes down.)</td> </tr> </tbody> </table>	Option	Description	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.)					
Option	Description													
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.)													
lease-time	Lease time in seconds. 0 means unlimited.	integer	300 - 8640000	86400										
dns-service	Options for assigning DNS servers to DHCP clients.	Option	-	default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>local</td> <td>The IP address of the interface of the DHCP server that is added becomes the clients' DNS server IP address.</td> </tr> <tr> <td>default</td> <td>Clients are assigned the FortiExtender configured DNS server.</td> </tr> <tr> <td>specify</td> <td>Specify up to three DNS servers in the DHCP server configuration.</td> </tr> <tr> <td>wan-dns</td> <td>Use the WAN port DNS server. The DNS of the WAN interface that is added becomes clients' DNS server IP address.</td> </tr> </tbody> </table>	Option	Description	local	The IP address of the interface of the DHCP server that is added becomes the 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	Use the WAN port DNS server. The DNS of the WAN interface that is added becomes clients' DNS server IP address.			
Option	Description													
local	The IP address of the interface of the DHCP server that is added becomes the 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	Use the WAN port DNS server. The DNS of the WAN interface that is added becomes clients' DNS server IP address.													

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lo</td> <td>Loopback as the DHCP server interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the DHCP server interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the DHCP server interface.</td> </tr> </tbody> </table>	Option	Description	lo	Loopback as the DHCP server interface.	wan	WAN as the DHCP server interface.	port4	Port 4 as the DHCP server interface.			
Option	Description											
lo	Loopback as the DHCP server interface.											
wan	WAN as the DHCP server interface.											
port4	Port 4 as the DHCP server interface.											
start-ip	Specify the start IP address of the DHCP IP address range. For example, 192.168.1.100.	IPv4 address	-	none								
end-ip	Specify the end IP address of the DHCP IP address range. For example, 192.168.1.120.	IPv4 address	-	none								
mtu	Specify the client's MTU size.	integer	512 - 9000	1500								
reserved-address	Status of reserved address and MAC mapping.	Option	-	disable								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the reserved address option by configuring the IP, MAC, and action as reserved or block.</td> </tr> <tr> <td>disable</td> <td>Disable the reserved address option.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the reserved address option by configuring the IP, MAC, and action as reserved or block.	disable	Disable the reserved address option.					
Option	Description											
enable	Enable the reserved address option by configuring the IP, MAC, and action as reserved or block.											
disable	Disable the reserved address option.											

- [config reserved-address on page 85](#)

config reserved-address

Description: Configure options for the DHCP server to assign IP settings to specific MAC addresses.

```

config system dhcpserver
  edit <name>
    set reserved-address enable
    config reserved-addresses
      edit <name>
        set *ip {ipv4-address}
        set *mac {mac-address}
        set *action [block | reserved]
      unset
      next
      show
      abort
    end
  delete <name>
  purge
  show

```

```

end
next
show
end
delete <name>
purge
show
end

```

Parameter	Description	Type	Size	Default
ip	IP address to be reserved for the MAC address.	IPv4 address	-	none
mac	MAC address of the client that will get the reserved IP address.	string	-	none
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-	reserved

Option	Description
block	Block the address.
reserved	Reserve the address.

config system dhcp6server

Description: Configure DHCP6 servers.

```

config system dhcp6server
edit <name>
set status [enable | disable]
set lease-time [300 - 8640000]
set dns-service [default | specify]
set subnet {ipv6-address}
set interface [option1 | ...]
set ip-mode [range]
config ip-range
edit <name>
set start-ip {ipv6-address}
set end-ip {ipv6-address}
next
end
config prefix-range
edit <name>
set start-ip {ipv6-address}
set end-ip {ipv6-address}

```

```

        set prefix-length <integer>
    next
end
next
end

```

Sample command:

```

config system dhcp6server
edit 1
    set status enable
    set lease-time 604800
    set dns-service specify
    set dns-server1
    set dns-server2
    set dns-server3
    set dns-server4
    set subnet 2001:1:3::/64
    set interface lan
    set ip-mode range
    config ip-range
        edit 1
            set start-ip 2001:1:3::2
            set end-ip 2001:1:3::5
        next
    end
    config prefix-range
        edit 1
            set start-ip 2001:1:3:0000:1000::
            set end-ip 2001:1:3:0000:1001::
            set prefix-length 80
        next
    end
next
end

```

Parameter	Description	Type	Size	Default						
status	Status of the DHCP6 configuration.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the DHCP6 server.</td> </tr> <tr> <td>disable</td> <td>Disable the DHCP6 server.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the DHCP6 server.	disable	Disable the DHCP6 server.			
Option	Description									
enable	Enable the DHCP6 server.									
disable	Disable the DHCP6 server.									
lease-time	Lease time in seconds. 0 means unlimited.	integer	300 - 8640000	604800						
dns-service	Options for assigning IPv6 DNS servers to DHCP6 clients	Option	-	specify						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>default</td> <td>Clients are assigned the FortiExtender configured DNS server.</td> </tr> <tr> <td>specify</td> <td>Specify DNS servers in the DHCP server configuration.</td> </tr> </tbody> </table>	Option	Description	default	Clients are assigned the FortiExtender configured DNS server.	specify	Specify DNS servers in the DHCP server configuration.			
Option	Description									
default	Clients are assigned the FortiExtender configured DNS server.									
specify	Specify DNS servers in the DHCP server configuration.									
dns-server1	Specify the IP address of DNS Server 1. Available when dns-service is set to specify.	IPv6 address	-	none						
dns-server2	Specify the IP address of DNS Server 2. Available when dns-service is set to specify.	IPv6 address	-	none						
dns-server3	Specify the IP address of DNS Server 3. Available when dns-service is set to specify.	IPv6 address	-	none						
dns-server4	Specify the IP address of DNS Server 4. Available when dns-service is set to specify.	IPv6 address	-	none						
subnet	Defines a managed IPv6 prefix and its associated pools and options.	IPv6 subnet	-	none						
interface	DHCP6 server can assign IP configurations to clients connected to this interface. Options vary depending on the interface type.	option	-	none						
ip-mode	Method used to assign client IP	option	-	range						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>range</td> <td>Assign by IP range.</td> </tr> </tbody> </table>	Option	Description	range	Assign by IP range.					
Option	Description									
range	Assign by IP range.									
ip-range	Configure IPv6 address list. See config ip-range on page 88 .	array	-	none						
prefix-range	Configure IPv6 prefix list. See config prefix-range on page 89 .	array	-	none						

config ip-range

Parameter	Description	Type	Size	Default
start-ip	Start of IP range.	IPv6 address	-	none
end-ip	End of IP range.	IPv6 address	-	none

config prefix-range

Parameter	Description	Type	Size	Default
start-ip	Start of prefix range.	IPv6 address	-	none
end-ip	End of prefix range.	IPv6 address	-	none
prefix-length	Prefix length.	integer	-	

config dhcprelay

Description: Configure DHCP relay.

```

config dhcprelay
  edit <name>
    set status [enable | disable]
    set *client-interfaces <name1>, <name2>, ...
    set *server-interface <name1>
    set *server-ip {ipv4-address}
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end

```

Sample command:

```

FX201E5919000057 (dhcprelay) # show
config system dhcprelay
  edit 1
    set status enable
    set client-interfaces lan
    set server-interface port4
    set server-ip 192.168.200.124
  next
end

```

Parameter	Description	Type	Size	Default
status	Status of the DHCP relay configuration.	option	-	enable

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable DHCP relay.</td> </tr> <tr> <td>disable</td> <td>Disable DHCP relay</td> </tr> </tbody> </table>	Option	Description	enable	Enable DHCP relay.	disable	Disable DHCP relay									
Option	Description															
enable	Enable DHCP relay.															
disable	Disable DHCP relay															
client-interfaces	The interfaces connected to DHCP clients.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as client interfaces.</td> </tr> <tr> <td>lo</td> <td>Loopback as client interfaces.</td> </tr> <tr> <td>wan</td> <td>WAN as client interfaces.</td> </tr> <tr> <td>port4</td> <td>Port 4 as client interfaces.</td> </tr> <tr> <td>lte</td> <td>LTE as client interfaces.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as client interfaces.	lo	Loopback as client interfaces.	wan	WAN as client interfaces.	port4	Port 4 as client interfaces.	lte	LTE as client interfaces.			
Option	Description															
lan	LAN as client interfaces.															
lo	Loopback as client interfaces.															
wan	WAN as client interfaces.															
port4	Port 4 as client interfaces.															
lte	LTE as client interfaces.															
server-interface	The interface used to reach out to the DHCP server.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as client interfaces.</td> </tr> <tr> <td>lo</td> <td>Loopback as client interfaces.</td> </tr> <tr> <td>wan</td> <td>WAN as client interfaces.</td> </tr> <tr> <td>port4</td> <td>Port 4 as client interfaces.</td> </tr> <tr> <td>lte</td> <td>LTE as client interfaces.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as client interfaces.	lo	Loopback as client interfaces.	wan	WAN as client interfaces.	port4	Port 4 as client interfaces.	lte	LTE as client interfaces.			
Option	Description															
lan	LAN as client interfaces.															
lo	Loopback as client interfaces.															
wan	WAN as client interfaces.															
port4	Port 4 as client interfaces.															
lte	LTE as client interfaces.															
server-ip	IP address of the DHCP server.	IPv4 address	-	none												

config dns

Description: Configure DNS settings used to resolve domain names to IP addresses.

```

config system dns
  set primary {ipv4-address}
  set secondary {ipv4-address}
  set ip6-primary {ipv6-address}
  set ip6-secondary {ipv6-address}
  set timeout [1 - 10]
  set retry [0 - 5]
  set dns-cache-limit [0 - 4294967295]

```

```

set dns-cache-ttl [60 - 86400]
set cache-notfound-response [enable | disable]
set source-ip {ipv4-address}
set server-select-method [least-rtt | failover]
unset
show
end

```

Sample command:

```

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-notfound-responses disable
  set source-ip 0.0.0.0
  set server-select-method least-rtt
end

```

Parameter	Description	Type	Size	Default
primary	Primary static DNS server IPv4 address. The default is the FortiGuard primary DNS server IP.	IPv4 address	-	208.91.112.53
secondary	Secondary static DNS server IPv4 address. The default is the FortiGuard secondary DNS server.	IPv4 address	-	208.91.112.52
ip6-primary	Primary static DNS server IPv6 address. The default value is empty and will not add to the DNS server pool.	IPv6 address	-	::
ip6-secondary	Secondary static DNS server IPv6 address. The default value is empty and will not add to the DNS server pool.	IPv6 address	-	::
timeout	DNS query timeout interval in seconds.	integer	1 - 10	5
retry	Specify the number of retry attempts allowed for unsuccessful connections.	integer	0 - 5	3

Parameter	Description	Type	Size	Default
dns-cache-limit	Specify the maximum amount of records in the DNS cache that can be stored.	integer	0 - 4294967295	5000
dns-cache-ttl	Duration in seconds that DNS cache retains information.	integer	60 - 86400	1800
cache-notfound-responses	Specify whether or not to save the not-found response into cache. If enabled, no need to forward the not-found response to the DNS server in the future.	option	-	disable
	Option	Description		
	enable	Enable cache-notfound-responses.		
	disable	Disable cache-notfound-responses.		
source-ip	IP address used by the DNS server as its source IP.	IPv4 address	-	0.0.0.0
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt
	Option	Description		
	least-rtt	In the dns-server selection pool, the round-trip time of each dns-server ip is calculated and sorted from the shortest to the longest, picking from the shortest one.		
	failover	This algorithm is a relatively fixed order. The first pick doesn't change until it fails the first time. The order is primary DNS > secondary DNS > dynamic DNS (learned from DHCP).		

config dns-server

Description: Configure DNS servers.

```

config system dns-server
  edit <name>
    set interface <name1>
    set mode [recursive | non-recursive | forward-only]
    set dns-filter <name>
  next
end

```

Parameter	Description	Type	Size	Default								
Name	Name of the DNS server.	string	1 - 35 characters	none								
interface	A system interface enabled for DNS service.	option	-	none								
mode	DNS server mode.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>recursive</td> <td>Shadow the DNS database and forward.</td> </tr> <tr> <td>non-recursive</td> <td>Public DNS database only.</td> </tr> <tr> <td>forward-only</td> <td>Forward only.</td> </tr> </tbody> </table>	Option	Description	recursive	Shadow the DNS database and forward.	non-recursive	Public DNS database only.	forward-only	Forward only.			
Option	Description											
recursive	Shadow the DNS database and forward.											
non-recursive	Public DNS database only.											
forward-only	Forward only.											
dns-filter	Enter a previously created DNS filter profile.	string	-	none								

config dns-database

Description: Configure DNS databases.

```

config 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 [1 - 2147483647]
    set authoritative [enable | disable]
    set forwarder {ipv4-address}, {ipv4-address}, ...
    set source-ip {ipv4-address}
    config dns-entry {{{ see next for more info }}}
  unset

```

Parameter	Description	Type	Size	Default						
name	Name of the DNS database.	string	-	none						
status	Status of the DNS zone.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the DNS zone.</td> </tr> <tr> <td>disable</td> <td>Disable the DNS zone.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the DNS zone.	disable	Disable the DNS zone.			
Option	Description									
enable	Enable the DNS zone.									
disable	Disable the DNS zone.									
domain	Domain zone name.	string	-	none						

Parameter	Description	Type	Size	Default						
type	Zone type.	option	-	primary						
view	Zone view to serve internal or public DNS clients.	option	-	shadow						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>shadow</td> <td>Shadow the DNS zone to serve internal clients.</td> </tr> <tr> <td>public</td> <td>Public DNS zone to serve public clients.</td> </tr> </tbody> </table>	Option	Description	shadow	Shadow the DNS zone to serve internal clients.	public	Public DNS zone to serve public clients.			
Option	Description									
shadow	Shadow the DNS zone to serve internal clients.									
public	Public DNS zone to serve public clients.									
primary-name	Domain name of the default DNS server for the zone.	string	-	none						
contact	Email address of the administrator of the zone. It could be a simple username or full email address.	string	-	host						
ttl	Default time-to-live value (in seconds) for the entries of the DNS zone.	integer	1 - 2147483647	86400						
authoritative	Status of the authoritative zone.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable authoritative zone.</td> </tr> <tr> <td>disable</td> <td>Disable authoritative zone.</td> </tr> </tbody> </table>	Option	Description	enable	Enable authoritative zone.	disable	Disable authoritative zone.			
Option	Description									
enable	Enable authoritative zone.									
disable	Disable authoritative zone.									
forwarder	The list of DNS zone forwarder IP addresses, separate by white space.	IPv4 address	-	none						
source-ip	Source IP for forwarding to the DNS server.	IPv4 address	-	none						

config dns-entry

Description: Configure DNS entries.

```

config dns-entry
  edit <name>
    set status [enable | disable]
    set type [A | NS | CNAME | MX | PTR]
    set *hostname {string}
    set *ip {ipv4-address} *available when type is set to A or PTR
    set *canonical-name {string} *available when type is set to CNAME
    set preference [0 - 65535] *available when type is set to MX
  unset
  next

```

```

        show
        abort
        end
delete <name>
purge
show
end
next

```

Sample command:

```

FX201E5919000057 (dns-database) # show
config system dns-database
  edit 1
    set status enable
    set domain example.com
    set type primary
    set view public
    set primary-name dns
    set contact host
    set ttl 86400
    set authoritative enable
    set forwarder 1.2.4.8 8.8.4.4
    set source-ip
  config dns-entry
    edit 1
      set status enable
      set type A
      set ttl 0
      set hostname host1
      set ip 172.30.145.225
    next
  end
next
end

```

Parameter	Description	Type	Size	Default						
name	The DNS entry ID number.	integer	1 - 4294967295	none						
status	The resource record status.	option	-	enable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable resource record.</td> </tr> <tr> <td>disable</td> <td>Disable resource record.</td> </tr> </tbody> </table>	Option	Description	enable	Enable resource record.	disable	Disable resource record.			
Option	Description									
enable	Enable resource record.									
disable	Disable resource record.									
type	Resource record type.	option	-	A						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>Address record.</td> </tr> <tr> <td>NS</td> <td>Name server record.</td> </tr> <tr> <td>CNAME</td> <td>Canonical name record.</td> </tr> <tr> <td>MX</td> <td>Mail exchange record.</td> </tr> <tr> <td>PTR</td> <td>PTR resource record.</td> </tr> </tbody> </table>	Option	Description	A	Address record.	NS	Name server record.	CNAME	Canonical name record.	MX	Mail exchange record.	PTR	PTR resource record.			
Option	Description															
A	Address record.															
NS	Name server record.															
CNAME	Canonical name record.															
MX	Mail exchange record.															
PTR	PTR resource record.															
ttl	The time-to-live value (in seconds) for the entry.	integer	0 - 2147483647	0												
hostname	Name of the host.	string	-	none												
ip	IP address of the host.	IPv4 address	-	none												

config vwan-member

Description: Configure virtual VWAN interface members.

```

config vwan-member
  edit <name>
    set target <name1>
    set priority [1 - 7]
    set weight [1 - 256]
    set in-bandwidth-threshold [0 - 2147483647]
    set out-bandwidth-threshold [0 - 2147483647]
    set total-bandwidth-threshold [0 - 2147483647]
    set health-check <name1>
    set health-check-fail-threshold [1 - 10]
    set health-check-success-threshold [1 - 10]
    set link-cost-factor [latency | jitter | packet-loss]
    set latency-threshold [0 - 10000000, default = 5]
    set jitter-threshold [0 - 10000000, default = 5]
    set packetloss--threshold [0 - 100, default = 100]
    unset
    next
    show
    abort
  end
delete <name>
purge
show
end

```

Sample command:

```

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 5
set jitter-threshold 5
set packetloss-threshold 100

```

Parameter	Description	Type	Size	Default
target	Forwarding target.	string	-	none
priority	Priority of the member. The lower the value, the higher the priority.	integer	1 - 7	1
weight	Weight of the member.	integer	1 - 256	1
in-bandwidth-threshold	Bandwidth threshold in MB for input traffic. 0 indicates infinity.	integer	0 - 2147483647	0
out-bandwidth-threshold	Bandwidth threshold in MB for output traffic. 0 indicates infinity.	integer	0 - 2147483647	0

Parameter	Description	Type	Size	Default
packetloss-threshold	Packet loss in percentage for SLA to make decisions.	integer	0 - 100	100

config sms-notification

Description: Configure Extender SMS notification settings.

```
config sms-notification
    set notification [enable | disable]
    unset
```

- [config receiver on page 99](#)
- [config alert on page 100](#)

config receiver

Description: Configure SMS receiver.

```
config receiver
    edit <name>
        set receiver [enable | disable]
        set *phone-number +{country code}{phone number}
        set alert <name1>, <name2>, ...
        unset
        next
        show
        abort
        end
    delete <name>
    purge
    move <name1> [before | after] <name2>
    show
    end
```

Parameter	Description	Type	Size	Default
phone-number	The phone number consists of an optional "+" and up to 20 digits. No alphabetical letters is allowed.	string	Up to 20 digits	none
alert	Predefined alert to send to the receivers. (System reboot and OS image fallback alerts will be sent to the first user only!)	option	-	none

Parameter	Description	Type	Size	Default
	Option	Description		
	system-reboot	System reboot alert. Only the first user can receive this alert.		
	data-exhausted	Data plan exhausted alert.		
	session-disconnect	LTE data session disconnect alert.		
	low-signal-strength	Low LTE signal strength alert.		
	os-image-fallback	OS image fallback alert. Only the first user can receive this alert.		
	mode-switch	System networking mode switch alert.		
	fgt-backup-mode-switch	The number of consecutive successful probes before the member is considered alive.		

config alert

Description: Configure alert type message setting.

```

config alert
  set system-reboot {string}
  set data-exhausted {string}
  set session-disconnect {string}
  set low-signal-strength {string}
  set os-image-fallback {string}
  set mode-switch {string}
  set fgt-backup-mode-switch {string}
  unset
  show
end
show
end

```

Parameter	Description	Type	Size	Default
system-reboot	System reboot alert. Only the first user can receive this alert message.	string	Up to 127 characters in length.	system will reboot
data-exhausted	Data plan exhausted alert message.	string	Up to 127 characters in length.	data plan is exhausted
session-disconnect	LTE data session disconnect alert message.	string	Up to 127 characters in length.	LTE data session is disconnected

Parameter	Description	Type	Size	Default
low-signal-strength	Low LTE signal strength alert message.	string	Up to 127 characters in length.	LTE signal strength is too low
os-image-fallback	OS image fallback alert. Only the first user can receive this alert message.	string	Up to 127 characters in length.	system start to fallback OS image
mode-switch	System networking mode switch alert message.	string	Up to 127 characters in length.	system networking mode switched
fgt-backup-mode-switch	FortiGate backup work mode switching alert message.	string	Up to 127 characters in length.	FortiGate backup work mode switched

Sample command:

```

FX201E5919000057 (sms-notification) # show
config system sms-notification
  set notification disable
  config receiver
    edit rec1
      set receiver enable
      set phone-number +15082558657
      set alert data-exhausted fgt-backup-mode-switch low-signal-strength mode-switch os-
image-fallback session-disconnect
    next
  end
config 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
end

```

config sms-remote-diag

Description: Configure Extender SMS remote diagnosis settings.

```

config sms-remote-diag
  set remote-diag [enable | disable]
  unset

```

Parameter	Description	Type	Size	Default
remote-diag	Status of the SMS remote diagnose function.	option	-	disable
	Option	Description		
	enable	Enable SMS remote diagnose.		
	disable	Disable SMS remote diagnose.		

- [config allowed-user on page 102](#)

config allowed-user

Description: Configure SMS remote diagnosis-allowed SMS sender.

```

config allowed-user
  edit <name>
    set sender [enable | disable]
    set *phone-number +{country code}{phone number}
    set allowed-command-type <name1>, <name2>, ...
    unset
    next
    show
    abort
  end
  delete <name>
  purge
  show
end
show
end

```

Sample command:

```

FX201E5919000057 (sms-remote-diag) # show
config system sms-remote-diag
  set remote-diag disable
  config allowed-user
    edit user1
      set sender enable
      set phone-number +15082558567
      set allowed-command-type factory-reset get-extender-status get-modem-status get-
system-status
    next
  end
end

```

Parameter	Description	Type	Size	Default
sender	Status of the sender.	option	-	disable
	Option	Description		
	enable	Enable the sender.		
	disable	Disable the sender.		
phone-number	The sender's phone number. Format: + (country code)(phone number)	phone number	-	none
allowed-command-type	Permitted command types from the sender.	options	-	none
	Option	Description		
	reboot	Root the device.		
	factory-reset	Reset the device to its factory settings.		
	set-apn	Set the APN.		
	modem-reset	Reset the modem.		
	get-modem-status	Get the modem status.		
	get-extender-status	Get the FortiExtender status.		
	get-system-version	Get the system version.		
	get-system-status	Get the system status.		

config syslog

Description: Configure syslog server settings.

```

config system syslog
  config remote-servers {string}
  edit <name>
    set ip* {ipv4-address}
    set port [1 - 65535]
  unset
  delete <name>
  purge
  show
  end
  config statistic-report
    set status [disable | enable]

```

```

    set interval [1 - 3600]
    config cpu-usage
        set threshold [0 - 100]
        thrset variance [0 - 100]
    end
    config memory-usage
        set threshold [0 - 100]
        set variance [0 - 100]
    end
    config cpu-temperature
        set threshold [0 - 120]
        set variance [0 - 120]
    end
end
show
end

```

config remote-servers

Description: Configure syslog remote servers settings.

```

config remote-servers
    edit <name>
        set ip* {ipv4-address}
        set port [1 - 65535]
        unset
        end
        next
        show
        abort
    delete
    purge
    end
    show

```

Parameter	Description	Type	Size	Default
ip	The IP address of the remote server.	IPv4 address	-	none
port	The remote syslog server port.	integer	1 - 65535	514

config statistic-report

Description: Configure syslog statistic report settings.

```

config statistic-report
    set status [enable | disable]
    set interval [1 - 3600]
    unset

```

Parameter	Description	Type	Size	Default						
status	Status syslog statistic report.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable syslog statistic report.</td> </tr> <tr> <td>disable</td> <td>Disable Enable syslog statistic report.</td> </tr> </tbody> </table>	Option	Description	enable	Enable syslog statistic report.	disable	Disable Enable syslog statistic report.			
Option	Description									
enable	Enable syslog statistic report.									
disable	Disable Enable syslog statistic report.									
interval	The time interval (in seconds) of system status reports.	integer	1 - 3600	30						

config cpu-usage

Description: Configures CPU usage rate statistic report settings.

```
config cpu-usage
    set threshold [0 - 100]
    set variance [0 - 100]
unset
show
end
```

Parameter	Description	Type	Size	Default
threshold	The percentage of CPU usage threshold for system abnormal event report. 0 means disabled.	integer	0 - 100	70
variance	The variance of the CPU usage report when it exceeds the threshold. 0 means report all the time.	integer	0 - 100	5

config memory-usage

Description: Configures memory usage statistic report settings.

```
config memory-usage
    set threshold [0 - 100]
    set variance [0 - 100]
unset
show
end
```

Parameter	Size	Type	Size	Default
threshold	The percentage of memory usage threshold for system abnormal event report. 0 means disabled.	integer	0 - 100	50

Parameter	Size	Type	Size	Default
variance	The variance of the memory usage report when it exceeds the threshold. 0 means report all the time.	integer	0 - 100	5

config cpu-temperature

Description: Configures CPU temperature statistic report settings.

```
config cpu-temperature
  set threshold [0 - 120]
  set variance [0 - 120]
unset
show
end
```

Parameter	Description	Type	Size	Default
threshold	The CPU temperature threshold for system abnormal event report. 0 means disabled.	integer	0 - 120	80
variance	The variance of the CPU temperature report when it exceeds the threshold. 0 means report all the time.	integer	0 - 120	5

Sample command:

```
FX201E5919000057 (syslog) # show
config system syslog
  config remote-servers
    edit serv1
      set ip 192.148.200.193
      set port 514
    next
  end
  config statistic-report
    set status enable
    set interval 30
    config cpu-usage
      set threshold 70
      set variance 5
    end
    config memory-usage
      set threshold 50
      set variance 5
    end
  end
```

```

    config cpu-temperature
      set threshold 80
      set variance 5
    end
  end
end

```

config virtual-wire-pair

Description: Configure LAN-to-LTE interface mapping.

```

config virtual-wire-pair
  set lte-mapping <name1>
  unset
  show
end

```

Sample command:

```

FX201E5919000057 (virtual-wire-pair) # show
config system virtual-wire-pair
  set lte1-mapping lan
end

```

Parameter	Description	Type	Size	Default
lte1-mapping	LTE1 interface's LAN interface mapping.	option. (One of the physical or virtual system LAN side interfaces. Use the tab key to get the full list.)	-	none

config api-user

Description: Configure API user settings.

```

config api-user
  edit <name>
    set comment {string}
    unset
    next
  show
  abort

```

```

    end
  delete <name>
  purge
  show
end

```

Sample command:

```

FX201E5919000057 (api-user) # show
config system api-user
  edit 1
    set comment this is a test api user
  next
end

```

Parameter	Description	Type	Size	Default
name	The name of the API user.	string	-	none
comment	A brief comment of the API user.	string	-	none

config ntp

Description: Configure NTP synchronization in local management mode.

```

config ntp
  set type [fortiguard | custom]
  unset
  config ntpserver
    edit <name>
      set *server {ipv4-address} OR {string}
      unset
      next
      show
      abort
    end
  delete <name>
  purge
  show
end
show
end

```

Parameter	Description	Type	Size	Default
type	Type of NTP server.	option	-	fortiguard

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>fortiguard</td> <td>The FortiGuard NTP server.</td> </tr> <tr> <td>custom</td> <td>A custom NTP server.</td> </tr> </tbody> </table>	Option	Description	fortiguard	The FortiGuard NTP server.	custom	A custom NTP server.			
Option	Description									
fortiguard	The FortiGuard NTP server.									
custom	A custom NTP server.									

- [config ntpserver on page 109](#)

config ntpserver

Description: Configure available third-party NTP servers (up to 4 servers).

```

config ntpserver
  edit <name>
    set *server {ipv4-address} OR {string}
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end
show
end

```

Parameter	Description	Type	Size	Default
server	IP address or hostname of the NTP server.	string	-	none

Sample command:

```

FX201E5919000057 (ntp) # show
config system ntp
  set type custom
  config ntpserver
    edit 1
      set server 10.139.20.54
    next
  end
end

```

config settings

Description: Configure system settings.

```
config settings
  set ike-port [1024 - 65535]
  unset
  show
  end
```

Sample command:

```
FX201E5919000057 (settings) # show
config system settings
  set ike-port 500
end
```

Parameter	Description	Type	Size	Default
ike-port	IKE phase 1 port number.	integer	1024 - 65535	500

config system lan-switch

Description: Configure LAN switch settings.

```
config system lan-switch
  set stp {enable | disable}
  config ports
    edit <name>
      set security-8021x-member-mode {enable | disable}
    next
  end
  set wired-security-mode [802.1X]
  set wired-security-group <security group ID>
end
```

Sample command:

```
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

```

Parameter	Description	Type	Size	Default
stp	Enable/disable spanning tree protocol.	option	-	
wired-security-mode	Turn on 802.1x authentication for this interface. Only available on FortiExtender IPQ4019 platforms.	option	-	
wired-security-group	Names of user groups that can authenticate with the 802.1X	option	-	

config ports

Description: Configure LAN switch ports.

Parameter	Description	Type	Size	Default
config ports	Interfaces within the virtual switch.	option (Any of the physical LAN port IDs)	-	none

Option	Description
port1	LAN port 1.
port2	LAN port 2.
port3	LAN port 3.
port4	LAN port 4.
security-8021x-member-mode	Enable/disable 802.1x authentication on a port. Only available on FortiExtender IPQ4019 platforms.

config system switch-interface

Description: When the FortiExtender is in standalone mode, you can configure your switch interface settings.

When the FortiExtender is being managed from the FortiGate, you can view LAN extension settings synced from the FortiGate. You cannot configure these settings directly on the FortiExtender; you must make them through the FortiGate LAN extension profile first.

```
config system switch-interface
  edit <name>
    set vlan-support [enable | disable]
    config member
      edit <name1>
        set type [ aggregate | physical | vap]
        set port
        set vids {1-4089}
        set pvid {1-4089}
        set security-8021x-member-mode [enable | disable]
      next
    end
    set stp [enable | disable]
    set td-mode [disable | include]
    set wired-security-mode [802.1X]
    set wired-security-group <security group ID>
  next
end
```

Sample syntax:

```
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
    end
    set stp disable
    set ts-mode disable
    set wired-security-mode 802.1X
    set wired-security-group test
  next
end
```

Parameter	Description	Type	Size	Default						
vlan-support	Enable/disable VLAN support.	option	-							
stp	Spanning Tree Protocol.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable Spanning Tree Protocol.</td> </tr> <tr> <td>disable</td> <td>Disable Spanning Tree Protocol.</td> </tr> </tbody> </table>	Option	Description	enable	Enable Spanning Tree Protocol.	disable	Disable Spanning Tree Protocol.			
Option	Description									
enable	Enable Spanning Tree Protocol.									
disable	Disable Spanning Tree Protocol.									
ts-mode	Read-only: Split tunnel mode.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>include</td> <td>Enable Split tunnel mode</td> </tr> <tr> <td>disable</td> <td>Disable Split tunnel mode.</td> </tr> </tbody> </table>	Option	Description	include	Enable Split tunnel mode	disable	Disable Split tunnel mode.			
Option	Description									
include	Enable Split tunnel mode									
disable	Disable Split tunnel mode.									
wired-security-mode	Turn on 802.1x authentication for this interface. Only available on FortiExtender Branch platforms.	option	-							
wired-security-group	Names of user groups that can authenticate with the 802.1X.	option	-							
dst-mac	Read-only: MAC address of the remote gateway pushed from FortiOS.	string	-	none						
dst-addr	Read-only: Destination IP addresses	string	-	none						
services	Read-only: Internet services.	options	-	none						

config members

Parameter	Description	Type	Size	Default
config member	Interfaces within the virtual switch.	option	-	none
name	The LAN port ID.	string	-	none
type	Interface type.	option	-	
port	Interface within the virtual switch.	option	-	
vap	Virtual Access Point, which must NOT be configured as a WLAN bridge, will be added as a member of the switch-interface.	option	-	
vids	VLAN ID list.	integer	1 to 4089	
pvid	Port VLAN ID.	integer	1 to 4089	

Parameter	Description	Type	Size	Default
security-8021x-member-mode	Enable/disable 802.1x authentication on a port. Only available on FortiExtender Branch platforms.	option	-	

config system ipsec

Description: Configure IPsec VPN settings.

config ssh-crypto

Description: Configure system SSH crypto.

```
config system ssh-crypto
  set strong-crypto [enable | disable]
end
```

Sample command:

```
config system ssh-crypto
  set strong-crypto enable
  set ssh-enc-algo aes256-ctr aes256-gcm@openssh.com
  set ssh-hsk-algo ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 rsa-sha2-256 rsa-sha2-512 ssh-ed25519
  set ssh-kex-algo curve25519-sha256@libssh.org diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512
  set ssh-mac-algo hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-512-etm@openssh.com
end
```

Parameter	Description	Type	Size	Default
strong-crypto	Enable/disable strong encryption for SSH	option	-	disable
	Option	Description		
	<i>enable</i>	Enable strong encryption for SSH		
	<i>disable</i>	Disable strong encryption for SSH		

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>diffie-hellman-group-exchange-sha256</i></td> <td>diffie-hellman-group-exchange-sha256</td> </tr> <tr> <td><i>diffie-hellman-group14-sha256</i></td> <td>diffie-hellman-group14-sha256</td> </tr> <tr> <td><i>diffie-hellman-group16-sha512</i></td> <td>diffie-hellman-group16-sha512</td> </tr> <tr> <td><i>diffie-hellman-group18-sha512</i></td> <td>diffie-hellman-group18-sha512</td> </tr> </tbody> </table>	Option	Description	<i>diffie-hellman-group-exchange-sha256</i>	diffie-hellman-group-exchange-sha256	<i>diffie-hellman-group14-sha256</i>	diffie-hellman-group14-sha256	<i>diffie-hellman-group16-sha512</i>	diffie-hellman-group16-sha512	<i>diffie-hellman-group18-sha512</i>	diffie-hellman-group18-sha512			
Option	Description													
<i>diffie-hellman-group-exchange-sha256</i>	diffie-hellman-group-exchange-sha256													
<i>diffie-hellman-group14-sha256</i>	diffie-hellman-group14-sha256													
<i>diffie-hellman-group16-sha512</i>	diffie-hellman-group16-sha512													
<i>diffie-hellman-group18-sha512</i>	diffie-hellman-group18-sha512													
set ssh-mac-algo	Set supported ciphers for ssh-mac-algo.	option	-	hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-512-etm@openssh.com										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>hmac-sha2-256</i></td> <td>hmac-sha2-256</td> </tr> <tr> <td><i>hmac-sha2-256-etm@openssh.com</i></td> <td>hmac-sha2-256-etm@openssh.com</td> </tr> <tr> <td><i>hmac-sha2-512</i></td> <td>hmac-sha2-512</td> </tr> <tr> <td><i>hmac-sha2-512-etm@openssh.com</i></td> <td>hmac-sha2-512-etm@openssh.com</td> </tr> </tbody> </table>	Option	Description	<i>hmac-sha2-256</i>	hmac-sha2-256	<i>hmac-sha2-256-etm@openssh.com</i>	hmac-sha2-256-etm@openssh.com	<i>hmac-sha2-512</i>	hmac-sha2-512	<i>hmac-sha2-512-etm@openssh.com</i>	hmac-sha2-512-etm@openssh.com			
Option	Description													
<i>hmac-sha2-256</i>	hmac-sha2-256													
<i>hmac-sha2-256-etm@openssh.com</i>	hmac-sha2-256-etm@openssh.com													
<i>hmac-sha2-512</i>	hmac-sha2-512													
<i>hmac-sha2-512-etm@openssh.com</i>	hmac-sha2-512-etm@openssh.com													

config system automation trigger

Description: Configure a trigger for automation stitches.

```

config system automation trigger
  edit <Automation Trigger Name>
    set description <string>
    set trigger-type <event-based>
    set event-type <digital-io-alert>
    set digital-io-alert-id <digital I/O alert ID>
  next
end

```

Sample command:

```
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
```

Parameter	Description	Type	Size	Default				
description	Describe the automation trigger.	string	-	none				
trigger-type	Set a trigger type.	option	-	event-based				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>event-based</td> <td>Set to trigger at specific system events or conditions, for example a digital I/O alert.</td> </tr> </tbody> </table>		Option	Description	event-based	Set to trigger at specific system events or conditions, for example a digital I/O alert.		
Option	Description							
event-based	Set to trigger at specific system events or conditions, for example a digital I/O alert.							
event-type	If <code>trigger-type</code> is set to event-based, you must configure an event type.	option	-	none				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>digital-io-alert</td> <td>A digital I/O alert is detected.</td> </tr> </tbody> </table>		Option	Description	digital-io-alert	A digital I/O alert is detected.		
Option	Description							
digital-io-alert	A digital I/O alert is detected.							
digital-io-alert-id	If <code>event-type</code> is set to <code>digital-io-alert</code> , you must configure a digital I/O alert ID.	option	-	none				

config system automation action

Description: Configure an action for automation stitches.

```
config system automation action
edit <Automation Action Name>
set description <string>
set action-type {digital-output | sim-switch | modem-reset}
set digital-io-action-id <digital IO action ID>
set minimum-interval {integer}
set modem-id <modem ID>
next
end
```

Sample command:

```
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
```

Parameter	Description	Type	Size	Default								
description	Describe the automation action.	string	-	none								
action-type	Set an action type.	option	-	none								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>digital-output</td> <td>Output a digital signal via the digital out pin.</td> </tr> <tr> <td>sim-switch</td> <td>Change the currently active SIM card to an alternate one, enabling the device to connect through a different network or carrier as needed.</td> </tr> <tr> <td>modem-reset</td> <td>Perform a reboot or reset operation on the modem to reinitialize its settings and restore connectivity in case of issues.</td> </tr> </tbody> </table>	Option	Description	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.			
Option	Description											
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	option	-	none								
modem-id	If action-type is set to sim-switch or modem-reset, you must configure a modem ID.	option	-	none								
minimum-interval	Limit performing this action to no more than once in this interval (in seconds).	integer	[0 - 2592000], max value 30 days	0								

config system automation stitch

Description: Configure automation stitches.

```
config system automation stitch
edit <Automation Stitch Name>
set description <string>
```

```

set status {enable | disable}
set trigger <trigger ID>
config actions
  edit <name>
    set action <string>
    set delay <integer>
    set required {enable | disable}
  next
end
next
end

```

Sample command:

```

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
end

```

Parameter	Description	Type	Size	Default						
description	Describe the automation stitch.	string	-	none						
status	Enable or disable the automation stitch.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the automation stitch.</td> </tr> <tr> <td>disable</td> <td>Disable the automation stitch.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the automation stitch.	disable	Disable the automation stitch.			
Option	Description									
enable	Enable the automation stitch.									
disable	Disable the automation stitch.									
trigger	Enter the automation trigger ID.	option	-	none						

config actions

Parameter	Description	Type	Size	Default
action	Enter the automation action name.	string	-	none

Parameter	Description	Type	Size	Default
delay	Set the delay before execution (in seconds).	integer	[0-3600]	0
required	Set if this is required or not in the action chain.	option	-	disable

Option	Description
enable	Required in the action chain.
disable	Not required in the action chain.

config system digital-io digital

Description: List the supported digitals on FEV models.

Sample command:

```
config system digital-io digital
edit in
set direction in
next
edit out
set direction out
next
end
```

config system digital-io alert

Description: Configure digital I/O alerts on FEV models.

```
config system digital-io alert
edit <name>
set poll-period <integer>
set input-digital <digital name>
set alert-trigger-state {no-alert | high | low | both}
set report [enable | disable]
set report-type [snmp syslog]
set gpio-name <string>
set low-state-name <string>
set high-state-name <string>
```

```

next
end

```

Sample command:

```

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
end

```

Parameter	Description	Type	Size	Default										
poll-period	The interval between general purpose input output (GPIO) status checks, in milliseconds.	integer	[10-3600000]	100										
input-digital	Enter the digital name.	option	-	none										
alert-trigger-state	The changing state that will trigger the GPIO alert report and action.	option	-	no-alert										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>no-alert</td> <td>No alert.</td> </tr> <tr> <td>high</td> <td>The state is changed from low to high.</td> </tr> <tr> <td>low</td> <td>The state is changed from high to low.</td> </tr> <tr> <td>both</td> <td>The state is changed.</td> </tr> </tbody> </table>	Option	Description	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.			
Option	Description													
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.	option	-	enable										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable reports.</td> </tr> <tr> <td>disable</td> <td>Disable reports.</td> </tr> </tbody> </table>	Option	Description	enable	Enable reports.	disable	Disable reports.							
Option	Description													
enable	Enable reports.													
disable	Disable reports.													
report-type	Select a report type.	option	-	none										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>snmp</td> <td>The event will be reported by the SNMP trap.</td> </tr> </tbody> </table>	Option	Description	snmp	The event will be reported by the SNMP trap.									
Option	Description													
snmp	The event will be reported by the SNMP trap.													

Parameter	Description	Type	Size	Default				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>syslog</td> <td>The event will be recorded by the syslog.</td> </tr> </tbody> </table>	Option	Description	syslog	The event will be recorded by the syslog.			
Option	Description							
syslog	The event will be recorded by the syslog.							
gpio-name	The input digital name that will be generated in the report log.	string	-	none				
low-state-name	The low state name that will be generated in the report log.	string	-	none				
high-state-name	The high state name that will be generated in the report log.	string	-	none				

config system digital-io action

Description: Configure digital I/O actions on FEV models.

```
config system digital-io action
  edit <name>
    set output-digital <digital name>
    set output-digital-state {high | low}
  next
end
```

Sample command:

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

Parameter	Description	Type	Size	Default						
output-digital	The digital that will run the alert action on.	option	-	none						
output-digital-state	The digital state that will be set when the alert is detected.	option	-	none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>high</td> <td>Change the state to high.</td> </tr> <tr> <td>low</td> <td>Change the state to low.</td> </tr> </tbody> </table>	Option	Description	high	Change the state to high.	low	Change the state to low.			
Option	Description									
high	Change the state to high.									
low	Change the state to low.									

config system 802-1X-settings

Description: Configure global 802.1X settings.



Any change to the 802.1X setting may cause the supplicant to reauthenticate if wired security with 802.1x is enabled.

```
config system 802-1X-settings
  set reauth-period {integer}
  set retry-primary-interval {integer}
  set radius-client-failover-wait {integer}
end
```

Parameter	Description	Type	Size	Default
reauth-period	Period of time to allow for reauthentication in seconds (0 = disable reauthentication).	integer	1 - 1440	60
retry-primary-interval	Retry interval for attempting to switch back to the primary RADIUS server, specified in seconds. The default value is 0, which disables switching back to the primary server.	integer	-	0
radius-client-failover-wait	RADIUS force failover timeout (seconds). Time to wait for a response before triggering failover (15, 30, and 45 seconds, default 45 seconds).	integer	-	45

config system ignition-sensing

Description: Configure ignition sensing on FEV 211/212F models.

```
config system ignition-sensing
  set status {enable | disable}
  set poweroff-delay <integer>
end
```

Sample command:

```
config system ignition-sensing
  set status enable
  set poweroff-delay 60
end
```

Parameter	Description	Type	Size	Default					
status	The digital state that will be set when the alert is detected.	option	-	enable					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>The device will automatically shut down under the following conditions: <ul style="list-style-type: none"> The power supply voltage is 12V and the ignition sense pin on the power supply is not connected to 12V. The power supply voltage is 24V and the ignition sense pin on the power supply is not connected to 24V. </td> </tr> <tr> <td>disable</td> <td>The device will not automatically shut down, and will automatically turn on if already shut down under the following conditions: <ul style="list-style-type: none"> If connected to a 12V power supply: <ul style="list-style-type: none"> When the power voltage is over 13.5V, or If the ignition sense pin on the power supply is connected to a positive terminal. If connected to a 24V power supply: <ul style="list-style-type: none"> When the power voltage is over 26.5V, or If the ignition sense pin on the power supply is connected to a positive terminal. </td> </tr> </tbody> </table>	Option	Description	enable	The device will automatically shut down under the following conditions: <ul style="list-style-type: none"> The power supply voltage is 12V and the ignition sense pin on the power supply is not connected to 12V. The power supply voltage is 24V and the ignition sense pin on the power supply is not connected to 24V. 	disable	The device will not automatically shut down, and will automatically turn on if already shut down under the following conditions: <ul style="list-style-type: none"> If connected to a 12V power supply: <ul style="list-style-type: none"> When the power voltage is over 13.5V, or If the ignition sense pin on the power supply is connected to a positive terminal. If connected to a 24V power supply: <ul style="list-style-type: none"> When the power voltage is over 26.5V, or If the ignition sense pin on the power supply is connected to a positive terminal. 		
Option	Description								
enable	The device will automatically shut down under the following conditions: <ul style="list-style-type: none"> The power supply voltage is 12V and the ignition sense pin on the power supply is not connected to 12V. The power supply voltage is 24V and the ignition sense pin on the power supply is not connected to 24V. 								
disable	The device will not automatically shut down, and will automatically turn on if already shut down under the following conditions: <ul style="list-style-type: none"> If connected to a 12V power supply: <ul style="list-style-type: none"> When the power voltage is over 13.5V, or If the ignition sense pin on the power supply is connected to a positive terminal. If connected to a 24V power supply: <ul style="list-style-type: none"> When the power voltage is over 26.5V, or If the ignition sense pin on the power supply is connected to a positive terminal. 								
 <p>If you are using a cigarette lighter socket to power the device and encounter an unexpected shutdown, set the status to <code>disable</code>.</p>									
poweroff-delay	Delay powering off the device after this interval (in seconds).	integer	0 - 86400	600					

config system obm-console

Description: Redirect the out-of-band management (OBM) console output to a local USB, FTP, SFTP, SMB, or NFS server.

```

config system obm-console
  config log-storage
    edit <name>
      set protocol [local_usb | ftp | sftp | smb | nfs]
      set folder <string>
      set server <IP address>
      set port <integer>
      set username <string>
      set password <string>
      set share video

```

```

    set export <string>
  next
end
end

```

Parameter	Description	Type	Size	Default												
protocol	Select which protocol to use to transfer the OOB console output.	option	-													
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>local_usb</td> <td>Local USB</td> </tr> <tr> <td>ftp</td> <td>FTP</td> </tr> <tr> <td>sftp</td> <td>SFTP</td> </tr> <tr> <td>smb</td> <td>SMB</td> </tr> <tr> <td>nfs</td> <td>NFS</td> </tr> </tbody> </table>	Option	Description	local_usb	Local USB	ftp	FTP	sftp	SFTP	smb	SMB	nfs	NFS			
Option	Description															
local_usb	Local USB															
ftp	FTP															
sftp	SFTP															
smb	SMB															
nfs	NFS															
folder	Enter the folder where the log file should be saved on the server.	string	-													
server	Enter the IP address of the server.	string	-													
share	If protocol is set to smb, enter which folder to share the output to.	string	-													
port	Enter the remote server listening port. When the port is set to 0, FortiExtender uses the default port for each protocol.	option	-													
username	Enter the username of the server.	string	-													
password	Enter the password of the server.	string	-													
export	If protocol is set to nfs, enter which folder to export the output to.	string	-													

SNMP

This section shows the syntax of the following commands:

- [config sysinfo on page 126](#)
- [config community on page 126](#)
- [config user on page 129](#)
- [config hosts on page 130](#)

config sysinfo

Description: Configure SNMP system info settings.

```
config sysinfo
  set status [enable | disable]
  set description {string}
  set contact-info {string}
  set location {string}
  unset
  show
  end
```

Parameter	Description	Type	Size	Default						
status	The status of sysinfo configuration.	option	-	disable						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Enable the sysinfo configuration.</td></tr><tr><td>disable</td><td>Disable the sysinfo configuration.</td></tr></tbody></table>	Option	Description	enable	Enable the sysinfo configuration.	disable	Disable the sysinfo configuration.			
Option	Description									
enable	Enable the sysinfo configuration.									
disable	Disable the sysinfo configuration.									
description	A brief description of the system.	string	1 - 127 characters in length	none						
contact-info	Contact information.	string	1 - 127 characters in length	none						
location	System location.	string	1 - 127 characters in length	none						

config community

Description: Configure SNMP v1/v2 community settings.

```

config community
  edit <name>
    set *name {string}
    set status [enable | disable]
    set hosts <name1>, <name2>, ...
    set query-v1-status [enable | disable]
    set query-v1-port [1 - 65535]
    set query-v2-status [enable | disable]
    set query-v2-port [1 - 65535]
    set trap-v1-status [enable | disable]
    set trap-v1-lport [1 - 65535]
    set trap-v1-rport [1 - 65535]
    set trap-v2c-status [enable | disable]
    set trap-v2c-lport [1 - 65535]
    set trap-v2c-rport [1 - 65535]
    set events <name1>, <name2>, ...
    unset
    next
    show
  end
delete <name>
purge
show
end

```

Parameter	Description	Type	Size	Default
name	Name of the SNMP community.	string	-	none
status	The status of the SNMP community configuration.	option	-	disable
	Option	Description		
	enable	Enable the SNMP community configuration.		
	disable	Disable the SNMP community configuration.		
hosts	SNMP community host names.	option	-	none
query-v1-status	Status of SNMP v1 queries.	option	-	disable
	Option	Description		
	enable	Enable SNMP v1 queries.		
	disable	Disable SNMP v1 queries.		
query-v1-port	SNMP v1 query port number.	integer	1 - 65535	161
query-v2-status	Status of SNMP v2 queries.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable SNMP v2 queries.		
	disable	Disable SNMP v2 queries.		
query-v2-port	SNMP v2 query port number.	integer	1 - 65535	161
trap-v1-status	Status of SNMP v1 traps.	option	-	disable
	Option	Description		
	enable	Enable SNMP v1 traps.		
	disable	Disable SNMP v1 traps.		
trap-v1-lport	SNMP v1 trap local port.	integer	1 - 65535	162
trap-v1-rport	SNMP v1 trap remote port.	integer	1 - 65535	162
trap-v2-status	Status of SNMP v2 traps.	option	-	disable
	Option	Description		
	enable	Enable SNMP v2 traps.		
	disable	Disable SNMP v2 traps.		
trap-v2-lport	SNMP v2 trap local port.	integer	1 - 65535	162
trap-v2-rport	SNMP v2 trap remote port.	integer	1 - 65535	162
events	SNMP trap events.	option	-	none
	Option	Description		
	system-reboot	System reboot events.		
	data-exhausted	Data usage exhaustion events.		
	session-disconnect	Modem data session disconnect events.		
	low-signal-strength	Modem low signal strength events.		
	os-image-fallback	System OS image fallback events.		
	mode-switch	System mode switch events.		
	fgt-backup-mode-switch	System FGT VRRP backup mode switch events.		

config user

Description: Configure SNMP v3 user settings.

```

config user
  edit <name>
    set *name {string}
    set status [enable | disable]
    set notify-hosts <name1>, <name2>, ...
    set trap-status [enable | disable]
    set trap-lport [1 - 65535]
    set trap-rport [1 - 65535]
    set queries [enable | disable]
    set query-port [1 - 65535]
    set events <name1>, <name2>, ...
    set security-level [no-auth-no-priv | auth-no-priv | auth-priv]
    set auth-proto [md5 | sha1] *available when security level includes auth
    set *auth-pwd {string} *available when security level includes auth
    set priv-proto [aes | des] *available when security level includes priv
    set *priv-pwd {string}*available when security level includes priv
  unset
  next
  show
  abort
  end
delete <name>
purge
show
end

```

Parameter	Description	Type	Size	Default						
name	Username of the SNMP user.	string	-	none						
status	Status of the SNMP user configuration.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the SNMP user.</td> </tr> <tr> <td>disable</td> <td>Disable the SNMP user.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the SNMP user.	disable	Disable the SNMP user.			
Option	Description									
enable	Enable the SNMP user.									
disable	Disable the SNMP user.									
notify-hosts	SNMP managers to which notifications (traps) are sent.	option	-	none						
trap-status	Status of the traps for the SNMP user.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the traps for the SNMP user.</td> </tr> <tr> <td>disable</td> <td>Disable the traps for the SNMP user.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the traps for the SNMP user.	disable	Disable the traps for the SNMP user.			
Option	Description									
enable	Enable the traps for the SNMP user.									
disable	Disable the traps for the SNMP user.									

Parameter	Description	Type	Size	Default
trap-lport	SNMPv3 trap local port.	integer	1 - 65535	162
trap-rport	SNMPv3 trap remote port.	integer	1 - 65535	162
queries	Status of SNMP queries for the user.	option	-	disable
query-port	SNMPv3 query port.	integer	1 - 65535	161
events	SNMP trap events.	option	-	none
	Option	Description		
	system-reboot	System reboot events.		
	data-exhausted	Data usage is exhaustion events.		
	session-disconnect	Modem data session disconnect events.		
	low-signal-strength	Modem low signal strength events.		
	os-image-fallback	System OS image fall back events.		
	mode-switch	System mode switch events.		
	fgt-backup-mode-switch	System FGT VRRP backup mode switch events.		
Security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv
	Option	Description		
	no-auth-no-priv	No authentication and no encryption.		
	auth-no-priv	Authentication and no encryption.		
	auth-priv	Authentication and encryption.		

config hosts

Description: Configure SNMP hosts settings.

```
config hosts
  edit <name>
    set *host-ip {ipv4 or ipv6 address}
    set host-type [any | query | trap]
    unset
    next
    show
    abort
  end
  delete <name>
  purge
```

```

show
end
show
end

```

Parameter	Description	Type	Size	Default
host-ip	IPv4 or IPv6 address of the SNMP manager (host), syntax: X.X.X.X/prefix or h:h:h:h:h:h:h/prefix.	IPv4 or IPv6 address	-	none
host-type	Whether the SNMP manager sends SNMP queries, or receives SNMP traps, or both.	option	-	none

Option	Description
any	Any type.
query	SNMP queries only.
trap	SNMP traps only.

HMON

This section shows the syntax of the following commands:

- [config interface-monitoring on page 132](#)
- [config hchk on page 132](#)

config interface-monitoring

Description: Configure monitoring interfaces.

```
config interface-monitoring
  edit <name>
    set interval [1 - 3600]
    set *interface <name1>, <name2>, ...
    set filter <name1>, <name2>, ...
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end
```

config hchk

Description: Configure measuring latency/loss/jitter.

```
config hchk
```

```
edit <name>
  set protocol [ping | http | dns]
  set interval [1 - 3600]
  set probe-cnt [1 - 10]
  set probe-tm [1 - 10]
  set *probe-target {ipv4-address}
  set port [1 - 65535] *available when protocol is set to http
  set http-get {string} *available when protocol is set to http
  set interface <name1>
  set src-type [none | interface | ip]
  set *stc-iface <name1> *available when src-type is set to interval
```

```

        set *src-ip {ipv4-address} *available when src-type is set to ip
        set filter <name1>, <name2>, ...
        unset
        next
        show
        abort
        end
delete <name>
purge
show
end
show
end

```

Sample command:

```

FX201E5919000057 (hmon) # show
config hmon
  config interface-monitoring
    edit 1
      set interval 30
      set interface wan
      set filter rx-bps rx-bytes rx-dropped rx-packets
    next
  end
  config hchk
    edit 1
      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 interface
      set src-iface wan
      set filter rtt loss
    next
  end
end

```

Parameter	Description	Type	Size	Default
interval	Monitoring interval in seconds.	integer	1 - 3600	30
interface	Interface to be monitored.	option	-	none
	Option	Description		
	lan	LAN as the outgoing interface.		

Parameter	Description	Type	Size	Default																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lo</td> <td>Loopback as the outgoing interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the outgoing interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the outgoing interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the outgoing interface.</td> </tr> </tbody> </table>	Option	Description	lo	Loopback as the outgoing interface.	lte1	LTE 1 as the outgoing interface.	wan	WAN as the outgoing interface.	port4	Port 4 as the outgoing interface.															
Option	Description																									
lo	Loopback as the outgoing interface.																									
lte1	LTE 1 as the outgoing interface.																									
wan	WAN as the outgoing interface.																									
port4	Port 4 as the outgoing interface.																									
filter	Filter types.	option	-	none																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>tx-bytes</td> <td>Transmitter bytes.</td> </tr> <tr> <td>rx-bytes</td> <td>Receiver bytes.</td> </tr> <tr> <td>tx-packets</td> <td>Transmitter packets.</td> </tr> <tr> <td>rx-packets</td> <td>Receiver packets.</td> </tr> <tr> <td>tx-dropped</td> <td>Transmitter dropped bytes.</td> </tr> <tr> <td>rx-dropped</td> <td>Receiver dropped bytes.</td> </tr> <tr> <td>tx-bps</td> <td>Transmitter bytes per second.</td> </tr> <tr> <td>rx-bps</td> <td>Receiver bytes per second.</td> </tr> <tr> <td>tx-pps</td> <td>Transmitter packets per second.</td> </tr> <tr> <td>rx-pps</td> <td>Receiver packets per second.</td> </tr> </tbody> </table>	Option	Description	tx-bytes	Transmitter bytes.	rx-bytes	Receiver bytes.	tx-packets	Transmitter packets.	rx-packets	Receiver packets.	tx-dropped	Transmitter dropped bytes.	rx-dropped	Receiver dropped bytes.	tx-bps	Transmitter bytes per second.	rx-bps	Receiver bytes per second.	tx-pps	Transmitter packets per second.	rx-pps	Receiver packets per second.			
Option	Description																									
tx-bytes	Transmitter bytes.																									
rx-bytes	Receiver bytes.																									
tx-packets	Transmitter packets.																									
rx-packets	Receiver packets.																									
tx-dropped	Transmitter dropped bytes.																									
rx-dropped	Receiver dropped bytes.																									
tx-bps	Transmitter bytes per second.																									
rx-bps	Receiver bytes per second.																									
tx-pps	Transmitter packets per second.																									
rx-pps	Receiver packets per second.																									
protocol	The protocol to use for status checks.	option	-	ping																						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ping</td> <td>Use PING to test the link with the probe-target.</td> </tr> <tr> <td>http</td> <td>Use HTTP-GET to test the link with the probe-target.</td> </tr> <tr> <td>dns</td> <td>Use DNS-Query to test the link with the probe-target.</td> </tr> </tbody> </table>	Option	Description	ping	Use PING to test the link with the probe-target.	http	Use HTTP-GET to test the link with the probe-target.	dns	Use DNS-Query to test the link with the probe-target.																	
Option	Description																									
ping	Use PING to test the link with the probe-target.																									
http	Use HTTP-GET to test the link with the probe-target.																									
dns	Use DNS-Query to test the link with the probe-target.																									
interval	Monitoring Interval in seconds.	integer	1 - 3600	5																						
probe-cnt	Number of probes sent within an interval.	integer	1 - 10	1																						
probe-tm	Timeout for a probe in seconds.	integer	1 - 10	2																						
interface	The outbound interface of probe packets.	option	-	none																						

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the outgoing interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the outgoing interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the outgoing interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the outgoing interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the outgoing interface.</td> </tr> </tbody> </table>				Option	Description	lan	LAN as the outgoing interface.	lo	Loopback as the outgoing interface.	lte1	LTE 1 as the outgoing interface.	wan	WAN as the outgoing interface.	port4	Port 4 as the outgoing interface.
Option	Description															
lan	LAN as the outgoing interface.															
lo	Loopback as the outgoing interface.															
lte1	LTE 1 as the outgoing interface.															
wan	WAN as the outgoing interface.															
port4	Port 4 as the outgoing interface.															
src-type	The way to set the source address for probes.	option	-	none												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>none</td> <td>Do not set the source address.</td> </tr> <tr> <td>interface</td> <td>Set the source address as the address derived from a specific interface.</td> </tr> <tr> <td>ip</td> <td>Set the source address as a specific IP.</td> </tr> </tbody> </table>				Option	Description	none	Do not set the source address.	interface	Set the source address as the address derived from a specific interface.	ip	Set the source address as a specific IP.				
Option	Description															
none	Do not set the source address.															
interface	Set the source address as the address derived from a specific interface.															
ip	Set the source address as a specific IP.															
filter	Filter type.	option	-	rtt loss												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>rtt</td> <td>Round trip time.</td> </tr> <tr> <td>loss</td> <td>Packet loss.</td> </tr> </tbody> </table>				Option	Description	rtt	Round trip time.	loss	Packet loss.						
Option	Description															
rtt	Round trip time.															
loss	Packet loss.															

VPN

This section shows the syntax of the following commands:

- [config ipsec on page 136](#)
- [config vpn certificate on page 146](#)

config ipsec

Description: Configure IPsec settings.

- [config phase1-interface on page 136](#)
- [config phase2-interface on page 141](#)

config phase1-interface

Description: Configure the VPN remote gateway.

```
config vpn ipsec phase1-interface
edit <name>
    set ip-version [4 | 6]
    set ike-version [1 | 2]
    set keylife [120 - 172800]
    set proposal [des-md5 | des-sha1 | des-sha256 | 3des-md5 | 3des-sha1 | 3dessha256 | aes128-md5
| aes128-sha1 | aes128-sha256 | aes256-md5 | aes256-sha1 | aes256-sha256]
    set dhgrp [1 | 2 | 5 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 27 | 28 | 29 | 30 | 31 | 32 ]
    set *interface <name1>
    set type [static | ddns]
    set *remote-gw {ipv4-address}
    set *remote-gw6 {ipv6-address}
    set *remotegw-ddns {string} *available when type is set to ddns
    set authmethod [psk | signature]
    set *psksecret {string}
    set *certificate <local-cert-name>
    set *peer <ca-cert-name>
    set localid {string}
    set peerid {string}
    set add-gw-route [enable | disable]
    set dev-id-notification [enable | disable]
    set dev-id <name1> *available when dev-id-notification is enabled
    set monitor <name>
next
end
```

Sample command:

```

config vpn ipsec phase1-interface
edit phase1_1
  set ike-version 2
  set keylife 86400
  set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3dessha1
  set dhgrp 14 5 31 20
  set interface wan
  set type static
  set remote-gw 207.102.148.196
  set authmethod psk
  set psksecret *****
  set localid 92
  set peerid 22
  set add-gw-route disable
  set dev-id-notification disable
  set monitor pri
next
end

```

Parameter	Description	Type	Size	Default						
ip-version	Specify the IP version for the VPN interface.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>4</td> <td>IPv4</td> </tr> <tr> <td>6</td> <td>IPv6</td> </tr> </tbody> </table>	Option	Description	4	IPv4	6	IPv6			
Option	Description									
4	IPv4									
6	IPv6									
ike-version	Specify the IKE protocol version.	option	-	2						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Version 1</td> </tr> <tr> <td>2</td> <td>Version 2</td> </tr> </tbody> </table>	Option	Description	1	Version 1	2	Version 2			
Option	Description									
1	Version 1									
2	Version 2									
keylife	Time to wait in seconds before the phase 1 encryption key expires.	integer	120 - 172800	86400						
proposal	Specify Phase-1 proposal.	option	-	aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-sha1						

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>des-md5</td><td></td></tr> <tr><td>des-sha1</td><td></td></tr> <tr><td>des-sha256</td><td></td></tr> <tr><td>3des-md5</td><td></td></tr> <tr><td>3des-sha1</td><td></td></tr> <tr><td>3des-sha256</td><td></td></tr> <tr><td>aes128-md5</td><td></td></tr> <tr><td>aes128-sha1</td><td></td></tr> <tr><td>aes128-sha256</td><td></td></tr> <tr><td>aes256-md5</td><td></td></tr> <tr><td>aes256-sha1</td><td></td></tr> <tr><td>aes256-sha256</td><td></td></tr> </tbody> </table>	Option	Description	des-md5		des-sha1		des-sha256		3des-md5		3des-sha1		3des-sha256		aes128-md5		aes128-sha1		aes128-sha256		aes256-md5		aes256-sha1		aes256-sha256				
Option	Description																													
des-md5																														
des-sha1																														
des-sha256																														
3des-md5																														
3des-sha1																														
3des-sha256																														
aes128-md5																														
aes128-sha1																														
aes128-sha256																														
aes256-md5																														
aes256-sha1																														
aes256-sha256																														
dhgrp	<p>Diffie-Hellman (DH) key exchange in phase1 is used to negotiate and exchange private keys for phase2.</p> <p>Note: Any DH groups less than 15 are not recommended due to their low security levels. 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).</p>	option	-	14, 5																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>1</td><td></td></tr> <tr><td>2</td><td></td></tr> <tr><td>5</td><td></td></tr> <tr><td>14</td><td></td></tr> <tr><td>15</td><td></td></tr> <tr><td>16</td><td></td></tr> <tr><td>17</td><td></td></tr> <tr><td>18</td><td></td></tr> <tr><td>19</td><td></td></tr> </tbody> </table>	Option	Description	1		2		5		14		15		16		17		18		19										
Option	Description																													
1																														
2																														
5																														
14																														
15																														
16																														
17																														
18																														
19																														

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>20</td> <td></td> </tr> <tr> <td>21</td> <td></td> </tr> <tr> <td>27</td> <td></td> </tr> <tr> <td>28</td> <td></td> </tr> <tr> <td>29</td> <td></td> </tr> <tr> <td>30</td> <td></td> </tr> <tr> <td>31</td> <td></td> </tr> <tr> <td>32</td> <td></td> </tr> </tbody> </table>	Option	Description	20		21		27		28		29		30		31		32				
Option	Description																					
20																						
21																						
27																						
28																						
29																						
30																						
31																						
32																						
interface	The outgoing interface.	option	-	none																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>LAN as the outgoing interface.</td> </tr> <tr> <td>lo</td> <td>Loopback as the outgoing interface.</td> </tr> <tr> <td>lte1</td> <td>LTE 1 as the outgoing interface.</td> </tr> <tr> <td>wan</td> <td>WAN as the outgoing interface.</td> </tr> <tr> <td>port4</td> <td>Port 4 as the outgoing interface.</td> </tr> </tbody> </table>	Option	Description	lan	LAN as the outgoing interface.	lo	Loopback as the outgoing interface.	lte1	LTE 1 as the outgoing interface.	wan	WAN as the outgoing interface.	port4	Port 4 as the outgoing interface.									
Option	Description																					
lan	LAN as the outgoing interface.																					
lo	Loopback as the outgoing interface.																					
lte1	LTE 1 as the outgoing interface.																					
wan	WAN as the outgoing interface.																					
port4	Port 4 as the outgoing interface.																					
type	Select a remote gateway type.			none																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>static</td> <td>Static gateway.</td> </tr> <tr> <td>ddns</td> <td>Dynamic DNS gateway.</td> </tr> </tbody> </table>	Option	Description	static	Static gateway.	ddns	Dynamic DNS gateway.															
Option	Description																					
static	Static gateway.																					
ddns	Dynamic DNS gateway.																					
remote-gw	The IPv4 address of the remote gateway's external interface.	IPv4 address	-	none																		
remote-gw6	The IPv6 address of the remote gateway's external interface.	IPv6 address	-	none																		
remotegw-ddns	Specify the domain name of the remote gateway, for example, name.DDNS.com. Available when type is set to ddns.	string	-	none																		
authmethod	Authentication method.	option	-	psk																		

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>psk</td> <td>Preshared key.</td> </tr> <tr> <td>signature</td> <td>Signature certificate.</td> </tr> </tbody> </table>	Option	Description	psk	Preshared key.	signature	Signature certificate.			
Option	Description									
psk	Preshared key.									
signature	Signature certificate.									
certificate	<p>Specify the name of up to four local signed personal certificates.</p> <p>Note: This entry is only available when authmethod is set to signature. The certificates must have already been installed on the FortiExtender before you are trying to enter them here.</p>			none						
peer	<p>The name of the CA certificate used to authenticate that the peer certificate is issued by it or its sub-CA.</p> <p>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.</p> <p>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.</p>			none						
psksecret	Specify the pre-shared secret created when configuring the VPN client for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	string	-	none						
localid	Local ID.	string	-	none						
peerid	Peer identity to accept.	string	-	none						
add-gw-route	Whether to automatically add a route to the remote gateway.	option	-	disable						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable automatically adding a route to the remote gateway.</td> </tr> <tr> <td>disable</td> <td>Disable automatically adding a route to the remote gateway.</td> </tr> </tbody> </table>	Option	Description	enable	Enable automatically adding a route to the remote gateway.	disable	Disable automatically adding a route to the remote gateway.			
Option	Description									
enable	Enable automatically adding a route to the remote gateway.									
disable	Disable automatically adding a route to the remote gateway.									
dev-id-notification	Whether to enable device ID notification for the first IKE message.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable device ID notification.</td> </tr> <tr> <td>disable</td> <td>Disable device ID notification.</td> </tr> </tbody> </table>	Option	Description	enable	Enable device ID notification.	disable	Disable device ID notification.			
Option	Description									
enable	Enable device ID notification.									
disable	Disable device ID notification.									
dev-id	The Device ID carried by the device ID notification. Available when dev-id-notification is enabled.	string	-	none						
monitor	Specify the IPsec phase1 interface as primary.	string	-	none						

config phase2-interface

Description: Configure VPN autokey tunnel.

```

config phase2-interface
  edit <name>
    set *phase1name
    set proposal {option1}, {option2}, ...
    set pfs [enable | disable]
    set dhgrp [1 | 2 | 5 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 27 | 28 | 29 | 30 | 31 | 32 ]
    set keylife-type [seconds | kbs]
    set keylifeseconds [120 - 172800]
    set keylifekbs [5120 - 4294967295]
    set encapsulation [tunnel-mode | transport-mode]
    set protocol [0 - 255]
    set src-addr-type [subnet | range | ip | name | subnet6 | range6 | ip6 | name6]
    set src-subnet {ipv4-subnet}
    set *src-start-ip {ipv4-address} *available when src-addr-type is range and ip
    set *src-end-ip {ipv4-address} *available when src-addr-type is range
    set *src-name {string} *available when src-addr-type is name
    set src-subnet6 {ipv6-subnet}
    set *src-start-ip6 {ipv6-address} *available when src-addr-type is range6 and ip6
    set *src-end-ip6 {ipv6-address} *available when src-addr-type is range6
    set *src-name6 {string} *available when src-addr-type is name6
    set src-port [0 - 65535]
    set dst-addr-type [subnet | range | ip | name | subnet6 | range6 | ip6 | name6]
    set dst-subnet {ipv4-subnet}
    set *dst-start-ip {ipv4-address} *available when dst-addr-type is range and ip
    set *dst-end-ip {ipv4-address} *available when dst-addr-type is range
    set *dst-name {string} *available when dst-addr-type is name
    set dst-subnet6 {ipv6-subnet}
    set *dst-start-ip6 {ipv6-address} *available when dst-addr-type is range6 and ip6
    set *dst-end-ip6 {ipv6-address} *available when dst-addr-type is range6
    set *dst-name6 {string} *available when dst-addr-type is name6

```

```

    set dst-port [0 - 65535]
unset
next
show
abort
end
delete <name>
purge
show
end
show
end

```

Sample command:

```

FX201E5919000057 (phase2-interface) # show
config vpn ipsec phase2-interface
edit phase2_1
set phase1name phase1_1
set proposal aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256 3dessha256
set pfs enable
set dhgrp 14 5 31 20
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 107.204.148.0/24
set dst-port 234
next
end

```

Parameter	Description	Type	Size	Default
phase1name	Phase 1 name (which determines the options required for phase 2).	string	-	none
proposal	Phase 2 proposal.	option	-	aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256 3des-sha256

Parameter	Description	Type	Size	Default																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>des-md5</td> <td>des-md5</td> </tr> <tr> <td>des-sha1</td> <td>des-sha1</td> </tr> <tr> <td>des-sha256</td> <td>des-sha256</td> </tr> <tr> <td>3des-md5</td> <td>3des-md5</td> </tr> <tr> <td>3des-sha1</td> <td>3des-sha1</td> </tr> <tr> <td>3des-sha256</td> <td>3des-sha256</td> </tr> <tr> <td>aes128-md5</td> <td>aes128-md5</td> </tr> <tr> <td>aes128-sha1</td> <td>aes128-sha1</td> </tr> <tr> <td>aes128-sha256</td> <td>aes128-sha256</td> </tr> <tr> <td>aes256-md5</td> <td>aes256-md5</td> </tr> <tr> <td>aes256-sha1</td> <td>aes256-sha1</td> </tr> <tr> <td>aes256-sha256</td> <td>aes256-sha256</td> </tr> <tr> <td>null-sha1</td> <td>null-sha1</td> </tr> <tr> <td>null-sha256</td> <td>null-sha256</td> </tr> </tbody> </table>	Option	Description	des-md5	des-md5	des-sha1	des-sha1	des-sha256	des-sha256	3des-md5	3des-md5	3des-sha1	3des-sha1	3des-sha256	3des-sha256	aes128-md5	aes128-md5	aes128-sha1	aes128-sha1	aes128-sha256	aes128-sha256	aes256-md5	aes256-md5	aes256-sha1	aes256-sha1	aes256-sha256	aes256-sha256	null-sha1	null-sha1	null-sha256	null-sha256			
Option	Description																																	
des-md5	des-md5																																	
des-sha1	des-sha1																																	
des-sha256	des-sha256																																	
3des-md5	3des-md5																																	
3des-sha1	3des-sha1																																	
3des-sha256	3des-sha256																																	
aes128-md5	aes128-md5																																	
aes128-sha1	aes128-sha1																																	
aes128-sha256	aes128-sha256																																	
aes256-md5	aes256-md5																																	
aes256-sha1	aes256-sha1																																	
aes256-sha256	aes256-sha256																																	
null-sha1	null-sha1																																	
null-sha256	null-sha256																																	
pfs	Status of the PFS feature.	option	-	enable																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable PFS.</td> </tr> <tr> <td>disable</td> <td>Disable PFS.</td> </tr> </tbody> </table>	Option	Description	enable	Enable PFS.	disable	Disable PFS.																											
Option	Description																																	
enable	Enable PFS.																																	
disable	Disable PFS.																																	
dhgrp	Phase 2 DH group.	option	-	14, 5																														
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>DH Group 1.</td> </tr> <tr> <td>2</td> <td>DH Group 2.</td> </tr> <tr> <td>5</td> <td>DH Group 5.</td> </tr> <tr> <td>14</td> <td>DH Group 14.</td> </tr> <tr> <td>15</td> <td>DH Group 15.</td> </tr> <tr> <td>16</td> <td>DH Group 16.</td> </tr> <tr> <td>17</td> <td>DH Group 17.</td> </tr> <tr> <td>18</td> <td>DH Group 18.</td> </tr> </tbody> </table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.															
Option	Description																																	
1	DH Group 1.																																	
2	DH Group 2.																																	
5	DH Group 5.																																	
14	DH Group 14.																																	
15	DH Group 15.																																	
16	DH Group 16.																																	
17	DH Group 17.																																	
18	DH Group 18.																																	

Parameter	Description	Type	Size	Default
	Option	Description		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
	27	DH Group 27.		
	28	DH Group 28.		
	29	DH Group 29.		
	30	DH Group 30.		
	31	DH Group 31.		
	32	DH Group 32.		
keylife-type	Keylife type	option	-	seconds
	Option	Description		
	seconds	Seconds.		
	kbs	Kbs.		
keylifeseconds	Phase 2 key life in seconds.	integer	120 – 172800	43200
keylifekbs	Phase 2 key life in the number of bytes of traffic.	integer	5120 - 4294967295	5120
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode
	Option	Description		
	tunnel-mode	Tunnel mode.		
	transport-mode	Transport mode.		
protocol	Quick mode protocol selector.	integer	1 - 255	0
src-addr-type	Local proxy ID type.	option	-	subnet
	Option	Description		
	subnet	IPv4 subnet.		
	range	IPv4 range.		
	ip	IPv4 address.		
	name	IPv4 address object name.		

Parameter	Description	Type	Size	Default																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>subnet6</td> <td>IPv6 subnet.</td> </tr> <tr> <td>range6</td> <td>IPv6 range.</td> </tr> <tr> <td>ip6</td> <td>IPv6 address.</td> </tr> <tr> <td>name6</td> <td>IPv6 address object name.</td> </tr> </tbody> </table>		Option	Description	subnet6	IPv6 subnet.	range6	IPv6 range.	ip6	IPv6 address.	name6	IPv6 address object name.										
Option	Description																					
subnet6	IPv6 subnet.																					
range6	IPv6 range.																					
ip6	IPv6 address.																					
name6	IPv6 address object name.																					
src-subnet	Local proxy ID subnet.	IPv4 address	-	0.0.0.0/0																		
src-port	Quick mode source port.	integer	1 - 65535, or 0 for all	0																		
src-start-ip	Local proxy ID start when src-addr-type is range and ip.	IPv4 address	-	none																		
src-end-ip	Local proxy ID end when src-addr-type is range.	IPv4 address	-	none																		
src-name	Local proxy ID name when src-addr-type is name.	string	-	none																		
src-subnet6	Local proxy ID IPv6 subnet when src-addr-type is subnet6.	IPv6 address	-	0::0/0																		
src-start-ip6	Local proxy ID IPv6 start when src-addr-type is range6 and ip6.	IPv6 address	-	none																		
src-end-ip6	Local proxy ID IPv6 end when src-addr-type is range6.	IPv6 address	-	none																		
src-name6	Local proxy ID IPv6 name when src-addr-type is name6.	string	-	none																		
dst-addr-type	Remote proxy ID type.	option	-	subnet																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>subnet</td> <td>IPv4 subnet.</td> </tr> <tr> <td>range</td> <td>IPv4 range.</td> </tr> <tr> <td>ip</td> <td>IPv4 address.</td> </tr> <tr> <td>name</td> <td>IPv4 address object name.</td> </tr> <tr> <td>subnet6</td> <td>IPv6 subnet.</td> </tr> <tr> <td>range6</td> <td>IPv6 range.</td> </tr> <tr> <td>ip6</td> <td>IPv6 address.</td> </tr> <tr> <td>name6</td> <td>IPv6 address object name.</td> </tr> </tbody> </table>		Option	Description	subnet	IPv4 subnet.	range	IPv4 range.	ip	IPv4 address.	name	IPv4 address object name.	subnet6	IPv6 subnet.	range6	IPv6 range.	ip6	IPv6 address.	name6	IPv6 address object name.		
Option	Description																					
subnet	IPv4 subnet.																					
range	IPv4 range.																					
ip	IPv4 address.																					
name	IPv4 address object name.																					
subnet6	IPv6 subnet.																					
range6	IPv6 range.																					
ip6	IPv6 address.																					
name6	IPv6 address object name.																					

Parameter	Description	Type	Size	Default
dst-subnet	Remote proxy ID subnet.	IPv4 address	-	0.0.0.0/0
dst-port	Quick mode source port.	integer	1 - 65535, or 0 for all	0
dst-start-ip	Remote proxy ID start when dst-addr-type is range and ip.	IPv4 address	-	none
dst-end-ip	Remote proxy ID end when dst-addr-type is range.	IPv4 address	-	none
dst-name	Remote proxy ID name when dst-addr-type is name.	string	-	none
dst-subnet6	Remote proxy ID IPv6 subnet when dst-addr-type is subnet6.	IPv6 address	-	0::0/0
dst-start-ip6	Remote proxy ID IPv6 start when dst-addr-type is range6 and ip6.	IPv6 address	-	none
dst-end-ip6	Remote proxy ID IPv6 end when dst-addr-type is range6.	IPv6 address	-	none
dst-name6	Remote proxy ID IPv6 name when dst-addr-type is name6.	string	-	none

config vpn certificate

Description: Configure VPN certificates.

- [config vpn certificate ca on page 146](#)
- [config vpn certificate local on page 147](#)

config vpn certificate ca

Description: Configure CA certificates.

```

config ca
  edit <name>
    set comment {string}
    set *source [factory | user]
    unset
    next
    abort
    show
    end
  delete <name>
  purge
  show

```

```
end
```

Sample command:

```
config vpn certificate ca
  edit Fortinet_CA
    set comment
    set source factory
  next
end
```

config vpn certificate local

Description: Configure local keys and certificates.

```
config vpn certificate local
  edit <name>
    set comment {string}
    set source [factory | user]
    set enroll-protocol [none | scep]
    unset
    next
    show
    abort
  end
  delete <name>
  purge
  show
end
```

Sample command:

```
config vpn certificate local
  edit Fortinet_Factory
    set comment
    set source factory
    set enroll-protocol scep
  next
end
```

Parameter	Description	Type	Size	Default
comment	Optional comments.	string	Up to 255 characters in length.	none
source	Source of CA certificate.	option	-	factory

Parameter	Description	Type	Size	Default						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>factory</td><td>From the manufacturer.</td></tr><tr><td>user</td><td>From the user.</td></tr></tbody></table>	Option	Description	factory	From the manufacturer.	user	From the user.			
Option	Description									
factory	From the manufacturer.									
user	From the user.									
enroll-protocol	Certificate enrollment protocol.	option	-							
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>None</td><td>None.</td></tr><tr><td>scep</td><td>Use SCEP.</td></tr></tbody></table>	Option	Description	None	None.	scep	Use SCEP.			
Option	Description									
None	None.									
scep	Use SCEP.									

Network

This section shows the syntax of the following commands:

- [config network address on page 149](#)
- [config service-custom on page 150](#)
- [config network address6 on page 151](#)

config network address

Description: Configure IPv4 addresses.

```
config network address
  edit <name>
    set type [ipmask | iprange]
    set subnet {ipv4-address}
    set start-ip {ipv4-address} *available when type is set to iprange
    set end-ip {ipv4-address} *available when type is set to iprange
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end
```

Sample command:

```
FX201E5919000057 (address) # show
config network address
  edit lan
    set type ipmask
    set subnet 192.168.200.0/24
  next
```

Parameter	Description	Type	Size	Default
type	Type of address.	option	-	ipmask

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>ipmask</td> <td>IP address and subnet mask.</td> </tr> <tr> <td>iprange</td> <td>IP range.</td> </tr> </tbody> </table>	Option	Description	ipmask	IP address and subnet mask.	iprange	IP range.			
Option	Description									
ipmask	IP address and subnet mask.									
iprange	IP range.									
subnet	IP address and subnet mask.	IPv4 address	-	none						
start-ip	The first IP address (inclusive) in the range of IP addresses.	IPv4 address	-	none						
end-ip	The last IP address (inclusive) in the range of IP addresses.	IPv4 address	-	none						

config service

Description: Configure firewall service.

config service-custom

Description: Configure custom services.

```

config service-custom
  edit <name>
    set protocol [TCP | UDP | ICMP | IP]
    set protocol number (0 - 254)
    set tcp-portrange <dstport_low>[-<dstport_high>:<srcport_low>-<srcport_high>] *available
      when protocol is set to TCP
    set udp-portrange <dstport_low>[-<dstport_high>:<srcport_low>-<srcport_high>] *available
      when protocol is set to UDP
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end
show
end

```

Sample command:

```

FX201E5919000057 (service) # show
config network service

```

```

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

```

Parameter	Size	Type	Size	Default
protocol	Protocol type based on IANA numbers.	option	-	ip
	Option	Description		
	tcp	TCP protocol.		
	udp	UDP protocol.		
	icmp	ICMP protocol.		
	ip	IP protocol.		
protocol-number	IP protocol number.	integer	0 - 254	0

config network address6

Description: Configure IPv6 addresses.

```

config network address6
  edit <name>
    set type [ipmask | iprange]
    set subnet {ipv6-address}
    unset
    next
    show
    abort
  end
  delete <name>
  purge
  show
end

```

Sample command:

```

config network address6
  edit all
    set type ipmask
    set subnet 0::0/0
  next
  edit none

```

```
set type ipmask
set subnet 0::0/128
next
end
```

Parameter	Description	Type	Size	Default						
type	Type of address.	option	-	ipmask						
	<table border="1"><thead><tr><th>Option</th><th>Description</th></tr></thead><tbody><tr><td>ipmask</td><td>IP address and subnet mask.</td></tr><tr><td>iprange</td><td>IP range.</td></tr></tbody></table>	Option	Description	ipmask	IP address and subnet mask.	iprange	IP range.			
Option	Description									
ipmask	IP address and subnet mask.									
iprange	IP range.									
subnet	IP address and subnet mask.	IPv6 address	-	none						

Execute

This section shows the syntax of the following command:

- [execute interface dhcpclient-renew on page 153](#)
- [execute SSH username serverip on page 154](#)
- [execute vpn certificate local generate rsa on page 154](#)
- [execute sim-switch on page 155](#)
- [execute modem on page 155](#)

execute interface dhcpclient-renew

Description: Manually renew DHCP lease on specified interface

```
#execute interface dhcpclient-renew <interface name>
```

Sample command:

```
execute interface dhcpclient-renew wan
```

execute obm-console

Description: Access the out-of-band management (OBM) console interface via the USB port. Enter the baudrate to access the console login.

```
#execute obm-console
```

Sample 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

execute SSH username serverip

Description: Configure SSH client log into other devices from FortiExtender.

```
#execute ssh username serverip
```

Sample command:

```
execute ssh admin 192.168.1.115
```

execute vpn certificate local generate rsa

Description: Generate a Certificate Signing Request.

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

Sample command:

```
# 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
```

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	

Field	Description	Mandatory	Type	Value Range
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	

execute sim-switch

Description: Immediately switches the inactive SIM to the active SIM; two SIMs need to be inserted 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.

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

Sample command:

```
execute sim-switch modem1
```

execute modem

Description: Configure the modem to manage eSIM.

```
#execute modem <modem> <field>
```

Sample command:

```
execute modem modem1 esim-enable-access
```

Field	Description
sim1	SIM1 specific operations.
sim2	SIM2 specific operations.
esim-enable-access	Enable access to the eSIM chip.
esim-disable-access	Disable access to eeSIM chip.
esim-details	eSIM details. This is solely for the device's EID.
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.

WiFi

This section presents the CLI commands for configuring Wi-Fi network settings.

```
config wifi
  config vap
    edit <WiFi Access Point Name>
      config ap-security
        ...
      end
    next
  end
  config wifi-networks
    ...
  end
  config radio-profile
    ...
  end
  config wifi-general
    ...
  end
end
```



WiFi settings are only available on Wi-Fi capable platforms.

- [config vap on page 157](#)
 - [config ap-security on page 160](#)
- [config wifi-networks on page 162](#)
- [config radio-profile on page 164](#)
- [config wifi-general on page 167](#)

config vap

Description: Configure WiFi virtual access point.

```
config wifi
  config vap
    edit <WiFi Access Point Name>
      set ssid <string>
      set broadcast-ssid [enable | disable]
      set dtim {integer}
```

```
set rts-threshold {integer}
set max-clients {integer}
set target-wake-time [enable | disable]
set bss-color-partial [enable | disable]
set mu-mimo [enable | disable]
set wlan-bridge [yes |no ]
set wlan-members
config ap-security
    set security-mode <encryption mode>
end
next
end
end
```

Sample command:

```
config wifi
config vap
edit fev-home-2g-1
    set ssid fev-home-2g-1
    set broadcast-ssid enable
    set dtim 1
    set rts-threshold 2347
    set max-clients 9
    set target-wake-time enable
    set bss-color-partial enable
    set mu-mimo enable
    set wlan-bridge no
    set wlan-members
    config ap-security
        set security-mode WPA2-Enterprise
        set auth-server-addr 192.168.11.99
        set auth-server-port 1812
        set auth-server-secret *****
        set pmf optional
    end
next
edit fev-home-5g-1
    set ssid fev-home-5g-1
    set broadcast-ssid enable
    set dtim 1
    set rts-threshold 2347
    set max-clients 9
    set target-wake-time enable
    set bss-color-partial enable
    set mu-mimo enable
    set wlan-bridge yes
    set wlan-members
    config ap-security
        set security-mode WPA2-Personal
        set pmf required
```

```

    set passphrase *****
  end
next
end
end

```

Parameter	Description	Type	Size	Default						
ssid	IEEE 802.11 service set identifier (SSID) for the wireless interface. Users who wish to use the wireless network must configure their computers to access this SSID name.	string	-							
broadcast-ssid	Enable/disable broadcasting the SSID	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable broadcasting the SSID.</td> </tr> <tr> <td>disable</td> <td>Disable broadcasting the SSID.</td> </tr> </tbody> </table>	Option	Description	enable	Enable broadcasting the SSID.	disable	Disable broadcasting the SSID.			
Option	Description									
enable	Enable broadcasting the SSID.									
disable	Disable broadcasting the SSID.									
dtim	Wi-Fi Delivery Traffic Indication Map (DTIM)	integer	1-255							
rts-threshold	Maximum packet size for RTS transmissions.	integer	256-2347							
max-clients	Maximum number of clients that can connect simultaneously to the VAP.	integer	0-512							
target-wake-time	Enable/disable 802.11ax target wake time.	option								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable 802.11ax target wake time.</td> </tr> <tr> <td>disable</td> <td>Disable 802.11ax target wake time.</td> </tr> </tbody> </table>	Option	Description	enable	Enable 802.11ax target wake time.	disable	Disable 802.11ax target wake time.			
Option	Description									
enable	Enable 802.11ax target wake time.									
disable	Disable 802.11ax target wake time.									
bss-color-partial	Enable/disable 802.11ax partial BSS color.	option								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable 802.11ax partial BSS color.</td> </tr> <tr> <td>disable</td> <td>Disable 802.11ax partial BSS color.</td> </tr> </tbody> </table>	Option	Description	enable	Enable 802.11ax partial BSS color.	disable	Disable 802.11ax partial BSS color.			
Option	Description									
enable	Enable 802.11ax partial BSS color.									
disable	Disable 802.11ax partial BSS color.									
mu-mimo	Enable/disable Multi-user MIMO.	option								

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable Multi-user MIMO.</td> </tr> <tr> <td>disable</td> <td>Disable Multi-user MIMO.</td> </tr> </tbody> </table>	Option	Description	enable	Enable Multi-user MIMO.	disable	Disable Multi-user MIMO.			
Option	Description									
enable	Enable Multi-user MIMO.									
disable	Disable Multi-user MIMO.									
wlan-bridge	Select if you want the SSID to act as a bridge between wireless and wired networks, integrating wireless devices into the same network.	option								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>Allow the SSID to act as a WLAN bridge.</td> </tr> <tr> <td>no</td> <td>Do not allow the SSID to act as a WLAN bridge.</td> </tr> </tbody> </table>	Option	Description	yes	Allow the SSID to act as a WLAN bridge.	no	Do not allow the SSID to act as a WLAN bridge.			
Option	Description									
yes	Allow the SSID to act as a WLAN bridge.									
no	Do not allow the SSID to act as a WLAN bridge.									
wlan-members	When WLAN Bridge is enabled, you can add WLAN members to the SSID configuration.									

- [config ap-security on page 160](#)

config ap-security

Description: Configure security mode for WiFi access point.

```

config wifi
  config vap
    edit <WiFi Access Point Name>
      config ap-security
        set security-mode <encryption mode>
        set pmf <option>
        set source-ip <ipv4 or ipv6 address>
        set passphrase <password>
        set auth-server-addr <ipv4 or ipv6 address>
        set auth-server-port <port number>
        set auth-server-secret <password>
      end
    next
  end
end
end

```

Sample command

```

config wifi vap
  edit fev-home-2g-1

```

```

set ssid fev-home-2g-1
set broadcast-ssid enable
set wlan-members
config ap-security
    set security-mode WPA2-Enterprise
    set source-ip ::
    set auth-server-addr 2001:10:10:10:39b9:4295:b105:a255
    set auth-server-port 1812
    set auth-server-secret *****
    set pmf optional
end
next
edit fev-home-5g-1
    set ssid fev-home-5g-1
    set broadcast-ssid enable
    set wlan-members
    config ap-security
        set security-mode WPA2-Personal
        set pmf disabled
        set passphrase *****
    end
next
end

```

Parameter	Description	Type	Size	Default																				
security-mode	Select which security mode to use.	option	-																					
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>OPEN</td> <td>Wi-Fi security OPEN</td> </tr> <tr> <td>WPA2-Personal</td> <td>Wi-Fi security WPA2 Personal</td> </tr> <tr> <td>WPA-WPA2-Personal</td> <td>Wi-Fi security WPA-WPA2 Personal</td> </tr> <tr> <td>WPA3-SAE</td> <td>Wi-Fi security WPA3 SAE</td> </tr> <tr> <td>WPA3-SAE-Transition</td> <td>Wi-Fi security WPA3 SAE Transition</td> </tr> <tr> <td>WPA2-Enterprise</td> <td>Wi-Fi security WPA2 Enterprise</td> </tr> <tr> <td>WPA3-Enterprise-Only</td> <td>Wi-Fi security WPA3 Enterprise only</td> </tr> <tr> <td>WPA3-Enterprise-Transition</td> <td>Wi-Fi security WPA3 Enterprise Transition</td> </tr> <tr> <td>WPA3-Enterprise-192-bit</td> <td>Wi-Fi security WPA3 Enterprise 192-bit</td> </tr> </tbody> </table>	Option	Description	OPEN	Wi-Fi security OPEN	WPA2-Personal	Wi-Fi security WPA2 Personal	WPA-WPA2-Personal	Wi-Fi security WPA-WPA2 Personal	WPA3-SAE	Wi-Fi security WPA3 SAE	WPA3-SAE-Transition	Wi-Fi security WPA3 SAE Transition	WPA2-Enterprise	Wi-Fi security WPA2 Enterprise	WPA3-Enterprise-Only	Wi-Fi security WPA3 Enterprise only	WPA3-Enterprise-Transition	Wi-Fi security WPA3 Enterprise Transition	WPA3-Enterprise-192-bit	Wi-Fi security WPA3 Enterprise 192-bit			
Option	Description																							
OPEN	Wi-Fi security OPEN																							
WPA2-Personal	Wi-Fi security WPA2 Personal																							
WPA-WPA2-Personal	Wi-Fi security WPA-WPA2 Personal																							
WPA3-SAE	Wi-Fi security WPA3 SAE																							
WPA3-SAE-Transition	Wi-Fi security WPA3 SAE Transition																							
WPA2-Enterprise	Wi-Fi security WPA2 Enterprise																							
WPA3-Enterprise-Only	Wi-Fi security WPA3 Enterprise only																							
WPA3-Enterprise-Transition	Wi-Fi security WPA3 Enterprise Transition																							
WPA3-Enterprise-192-bit	Wi-Fi security WPA3 Enterprise 192-bit																							
pmf	Protected Management Frames (PMF) support.	option	-																					

Parameter	Description	Type	Size	Default								
	This option is available if <code>security-mode</code> is set to OPEN, WPA2-Personal, WPA-WPA2-Personal, WPA3-SAE, or WPA3-SAE-Transition.											
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>disabled</td> <td>Disable PMF completely.</td> </tr> <tr> <td>required</td> <td>Enable PMF and deny clients without PMF.</td> </tr> <tr> <td>optional</td> <td>Enable PMF and allow clients without PMF.</td> </tr> </tbody> </table>	Option	Description	disabled	Disable PMF completely.	required	Enable PMF and deny clients without PMF.	optional	Enable PMF and allow clients without PMF.			
Option	Description											
disabled	Disable PMF completely.											
required	Enable PMF and deny clients without PMF.											
optional	Enable PMF and allow clients without PMF.											
passphrase	WPA pre-shared key (PSK) to be used to authenticate WiFi users. This option is available if <code>security-mode</code> is set to WPA2-Personal, WPA-WPA2-Personal, WPA3-SAE, or or WPA3-SAE-Transition.	password										
source-ip	Source IP address for communications to the RADIUS server (IPv4 and IPv6 format).	string										
auth-server-addr	RADIUS authentication server (IPv4 and IPv6 format). This option is available if <code>security-mode</code> is set to WPA2-Enterprise, WPA3-Enterprise-Only, WPA3-Enterprise-Transition, or WPA3-Enterprise-192-bit.	string										
auth-server-port	Wi-Fi Authentication Server Port. This option is available if <code>security-mode</code> is set to WPA2-Enterprise, WPA3-Enterprise-Only, WPA3-Enterprise-Transition, or WPA3-Enterprise-192-bit.	integer		1812								
auth-server-secret	Wi-Fi Authentication Server Secret. This option is available if <code>security-mode</code> is set to WPA2-Enterprise, WPA3-Enterprise-Only, WPA3-Enterprise-Transition, or WPA3-Enterprise-192-bit.	string										

config wifi-networks

Description: Configure WiFi networks for Station Mode.

```

config wifi
  config wifi-networks
    edit <name>
      set ssid <id>
      set security-mode <encryption mode>
      set pmf <option>
      set identity <string>
      set password <string>
      set sae-password <string>
    next
  end
end

```

Sample command:

```

config wifi wifi-networks
  edit 2g-Network
    set ssid Network
    set security-mode WPA3-Enterprise-Only
    set pmf required
    set identity *****
    set password *****
  next
  edit 5g-Dream
    set ssid Dream
    set security-mode WPA3-SAE
    set pmf
    set sae-password *****
  next
  edit 5g-Hope
    set ssid Hope
    set security-mode WPA2-Enterprise
    set pmf
    set identity *****
    set password *****
  next
end

```

Parameter	Description	Type	Size	Default
ssid	IEEE 802.11 service set identifier (SSID) for the wireless interface. Users who wish to use the wireless network must configure their computers to access this SSID name.	string		
security-mode	Select which security mode to use.	option	-	

Parameter	Description	Type	Size	Default																								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>OPEN</td> <td>Wi-Fi security OPEN</td> </tr> <tr> <td>WPA-Personal</td> <td>Wi-Fi security WPA Personal</td> </tr> <tr> <td>WPA2-Personal</td> <td>Wi-Fi security WPA2 Personal</td> </tr> <tr> <td>WPA-WPA2-Personal</td> <td>Wi-Fi security WPA-WPA2 Personal</td> </tr> <tr> <td>WPA3-SAE</td> <td>Wi-Fi security WPA3 SAE</td> </tr> <tr> <td>WPA3-SAE-Transition</td> <td>Wi-Fi security WPA3 SAE Transition</td> </tr> <tr> <td>WPA-Enterprise</td> <td>Wi-Fi security WPA Enterprise</td> </tr> <tr> <td>WPA2-Enterprise</td> <td>Wi-Fi security WPA2 Enterprise</td> </tr> <tr> <td>WPA-WPA2-Enterprise</td> <td>Wi-Fi security WPA-WPA2 Enterprise</td> </tr> <tr> <td>WPA3-Enterprise-Only</td> <td>Wi-Fi security WPA3 Enterprise only</td> </tr> <tr> <td>WPA3-Enterprise-Transition</td> <td>Wi-Fi security WPA3 Enterprise Transition</td> </tr> </tbody> </table>	Option	Description	OPEN	Wi-Fi security OPEN	WPA-Personal	Wi-Fi security WPA Personal	WPA2-Personal	Wi-Fi security WPA2 Personal	WPA-WPA2-Personal	Wi-Fi security WPA-WPA2 Personal	WPA3-SAE	Wi-Fi security WPA3 SAE	WPA3-SAE-Transition	Wi-Fi security WPA3 SAE Transition	WPA-Enterprise	Wi-Fi security WPA Enterprise	WPA2-Enterprise	Wi-Fi security WPA2 Enterprise	WPA-WPA2-Enterprise	Wi-Fi security WPA-WPA2 Enterprise	WPA3-Enterprise-Only	Wi-Fi security WPA3 Enterprise only	WPA3-Enterprise-Transition	Wi-Fi security WPA3 Enterprise Transition			
Option	Description																											
OPEN	Wi-Fi security OPEN																											
WPA-Personal	Wi-Fi security WPA Personal																											
WPA2-Personal	Wi-Fi security WPA2 Personal																											
WPA-WPA2-Personal	Wi-Fi security WPA-WPA2 Personal																											
WPA3-SAE	Wi-Fi security WPA3 SAE																											
WPA3-SAE-Transition	Wi-Fi security WPA3 SAE Transition																											
WPA-Enterprise	Wi-Fi security WPA Enterprise																											
WPA2-Enterprise	Wi-Fi security WPA2 Enterprise																											
WPA-WPA2-Enterprise	Wi-Fi security WPA-WPA2 Enterprise																											
WPA3-Enterprise-Only	Wi-Fi security WPA3 Enterprise only																											
WPA3-Enterprise-Transition	Wi-Fi security WPA3 Enterprise Transition																											
pmf	Protected Management Frames (PMF) support.	option	-																									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>disabled</td> <td>Disable PMF completely.</td> </tr> <tr> <td>required</td> <td>Enable PMF and deny clients without PMF.</td> </tr> <tr> <td>optional</td> <td>Enable PMF and allow clients without PMF.</td> </tr> </tbody> </table>	Option	Description	disabled	Disable PMF completely.	required	Enable PMF and deny clients without PMF.	optional	Enable PMF and allow clients without PMF.																			
Option	Description																											
disabled	Disable PMF completely.																											
required	Enable PMF and deny clients without PMF.																											
optional	Enable PMF and allow clients without PMF.																											
identity	Wi-Fi identity	string																										
password	Wi-Fi passphrase.	string																										
sae-password	WPA3 SAE password to be used to authenticate WiFi users.	string																										

config radio-profile

Description: Configure WiFi Radio profile.

```
config wifi
  config radio-profile
    edit <radio profile name>
      set band <2GHz/5GHz>
      set status <enable/disable>
```

```

set role <lan/wan>
set operating-standards [auto|11A-N-AC-AX|...]
set beacon-interval {100-3500}
set 80211d [ enable | disable]
set max-clients {0-512}
set power-mode auto
set channel {option1}, {option2}, ...
set bandwidth [auto|20MHz|...]
set extension-channel [auto|higher|...]
set guard-interval [auto|400ns|...]
set vap <ap names>
next
end
end

```

Sample command:

```

FVA21FTF22000003 (wifi) # config radio-profile
config wifi radio-profile
  edit 2g-profile
    set band 2GHz
    set enable enable
    set role lan
    set operating-standards auto
    set power-mode auto
    set channel
    set bandwidth auto
    set extension-channel auto
    set guard-interval auto
    set vap fev-home-2g-1 fev-home-2g-3 fev-home-2g-4
  next
edit 5g-profile
  set band 5GHz
  set enable enable
  set role wan
  set wifi-networks 5g-Dream
next
end

```

Parameter	Description	Type	Size	Default
band	Wi-Fi band selection 2.4GHz / 5GHz.	option		
	Option	Description		
	2GHz	Wi-Fi 2.4GHz		
	5GHz	Wi-Fi 5GHz		
status	Enable/disable Wi-Fi radio.	option	-	

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enabled</td> <td>Enable Wi-Fi radio.</td> </tr> <tr> <td>disabled</td> <td>Disable Wi-Fi radio.</td> </tr> </tbody> </table>	Option	Description	enabled	Enable Wi-Fi radio.	disabled	Disable Wi-Fi radio.					
Option	Description											
enabled	Enable Wi-Fi radio.											
disabled	Disable Wi-Fi radio.											
role	Set the radio role to LAN or WAN interface.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>lan</td> <td>Set the radio role to LAN. If the role is set as LAN, you can configure additional parameters for the WiF LAN interface,</td> </tr> <tr> <td>wan</td> <td>Set the radio role to WAN.</td> </tr> </tbody> </table>	Option	Description	lan	Set the radio role to LAN. If the role is set as LAN, you can configure additional parameters for the WiF LAN interface,	wan	Set the radio role to WAN.					
Option	Description											
lan	Set the radio role to LAN. If the role is set as LAN, you can configure additional parameters for the WiF LAN interface,											
wan	Set the radio role to WAN.											
operating-standards	Wi-Fi operating standard.	option										
beacon-interval	Wi-Fi beacon interval in milliseconds.	integer	100-3500									
80211d	Enable/disable Wi-Fi 802.11d.	option										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enabled</td> <td>Enable 802.11d.</td> </tr> <tr> <td>disabled</td> <td>Disable 802.11d.</td> </tr> </tbody> </table>	Option	Description	enabled	Enable 802.11d.	disabled	Disable 802.11d.					
Option	Description											
enabled	Enable 802.11d.											
disabled	Disable 802.11d.											
max-clients	Maximum number of Wi-Fi radio clients	integer	0-512									
power-mode	Set the power mode for your radio.	option										
channel	Wi-Fi channels.	option										
bandwidth	Wi-Fi channel bandwidth.	option										
extension-channel	Wi-Fi extension channel.	option										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>Wi-Fi extension channel auto.</td> </tr> <tr> <td>higher</td> <td>Wi-Fi extension channel higher.</td> </tr> <tr> <td>lower</td> <td>Wi-Fi extension channel lower.</td> </tr> </tbody> </table>	Option	Description	auto	Wi-Fi extension channel auto.	higher	Wi-Fi extension channel higher.	lower	Wi-Fi extension channel lower.			
Option	Description											
auto	Wi-Fi extension channel auto.											
higher	Wi-Fi extension channel higher.											
lower	Wi-Fi extension channel lower.											
guard-interval	Wi-Fi guard interval.	option										

Parameter	Description	Type	Size	Default								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>auto</td> <td>Wi-Fi guard interval auto</td> </tr> <tr> <td>400ns</td> <td>Wi-Fi guard interval 400ns</td> </tr> <tr> <td>800ns</td> <td>Wi-Fi guard interval 800ns</td> </tr> </tbody> </table>	Option	Description	auto	Wi-Fi guard interval auto	400ns	Wi-Fi guard interval 400ns	800ns	Wi-Fi guard interval 800ns			
Option	Description											
auto	Wi-Fi guard interval auto											
400ns	Wi-Fi guard interval 400ns											
800ns	Wi-Fi guard interval 800ns											
vap	Enter virtual APs you want to apply radio configurations to. Maximum of 4 APs.	string										

config wifi-general

Description: Configure general WiFi settings.

```
config wifi
  config wifi-general
    set country-code <option>
  end
end
```

Sample command:

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

```
set country-code
AS    AMERICAN SAMOA
AR    ARGENTINA
BS    BAHAMAS
BM    BERMUDA
KY    CAYMAN ISLANDS
DM    DOMINICA
GU    GUAM
HT    HAITI
MH    MARSHALL ISLANDS
AW    ARUBA
NI    NICARAGUA
MP    NORTHERN MARIANA ISLANDS
PW    PALAU
PR    PUERTO RICO
KN    SAINT KITTS AND NEVIS
```

LC	SAINT LUCIA
VC	SAINT VINCENT AND GRENADIENS
US	UNITED STATES
VI	VIRGIN ISLANDS
CA	CANADA



The list of country codes shown above applies to devices with the region code "A" only.

Parameter	Description	Type	Size	Default
country-code	Set the country code of the device. Note: The list of county codes varies with the region code of the devices in use.	option	-	-

User

This section shows the syntax of the following commands:

- [config user group on page 169](#)
- [config user radius on page 169](#)
- [config user security-exempt-list on page 171](#)
- [config user security-exempt-list6 on page 172](#)

config user group

Apply a RADIUS server table to a user group.

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

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

config user radius

Configure the FortiExtender to access a RADIUS server.

```
config user radius
  edit <name>
    set server {string}
    set secret {password}
    set auth-type [auto||ms_chap_v2|...]
    set timeout {integer}
    set transport-protocol [udp]
    set nas-ip {string}
    set nas-identifier {string}
    set port {integer}
    set source-ip {ipv4-address}
```

```

next
end

```

Sample command:

```

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

```

Parameter	Description	Type	Size	Default
name	Name of the RADIUS server table.	string	-	none
server	Primary RADIUS FQDN or IP address.	string	-	none
secret	Pre-shared secret key used to access the primary RADIUS server.	password	1-128	none
auth-type	<p>Authentication protocols permitted for this RADIUS server. You can select the following options:</p> <ul style="list-style-type: none"> auto ms_chap_v2 ms_chap chap pap <p>If the authentication type is set to auto, FortiExtender uses the following protocols in sequence: PAP → MSCHAP_v2 → CHAP FortiExtender will only try the next protocol once it receives a RADIUS-reject message</p>	option	-	auto
timeout	Time in seconds to retry connecting to the RADIUS server.	integer	-	5
transport-protocol	<p>Transport protocol to be used.</p> <ul style="list-style-type: none"> udp 	option	-	udp
nas-ip	IPv4 address used for the FortiExtender to communicate with the RADIUS server. It is also used as the NAS-IP-Address and Called-Station-ID attributes.	string	-	none

Parameter	Description	Type	Size	Default
nas-identifier	Optional NAS-Identifier string for RADIUS messages	string	-	none
port	Primary RADIUS server port number	integer	-	none
source-ip	Source IP address for communications to the RADIUS server.	IPv4 address	-	0.0.0.0

config user security-exempt-list

Configure security exemption list.

```

config user security-exempt-list
  edit <name>
    set description {string}
    config rule
      edit <id>
        set dstaddr <name1>, <name2>, ...
        set service <name1>, <name2>, ...
        set srcaddr <name1>, <name2>, ...
      next
    end
  next
end

```

Parameter	Description	Type	Size	Default
name	Name of the exempt list.	string	Maximum length: 30	none
description	Description.	string	Maximum length: 127	none

config rule

Parameter	Description	Type	Size	Default
id	Security exempt rule name.	string	Maximum length: 30	none
dstaddr	The network address IDs of the exempt destination.	string	-	none
service	The IDs of the exempt destination service.	string	-	none
srcaddr	The network address IDs of the exempt source.	string	-	none

config user security-exempt-list6

Configure IPv6 security exemption list.

```
config user security-exempt-list6
  edit <name>
    set description {string}
  config rule
    edit <id>
      set srcaddr6 <name1>, <name2>, ...
      set dstaddr6 <name1>, <name2>, ...
      set service <name1>, <name2>, ...
    next
  end
next
end
```

Parameter	Description	Type	Size	Default
name	Name of the exempt list.	string	Maximum length: 30	none
description	Description.	string	Maximum length: 127	none

config rule

Parameter	Description	Type	Size	Default
id	Security exempt rule name.	string	Maximum length: 30	none
srcaddr6	The IPv6 network address IDs of the exempt source.	string	-	none
dstaddr6	The IPv6 network address IDs of the exempt destination.	string	-	none
service	The IDs of the exempt destination service.	string	-	none

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>wildcard</td> <td>Matches using regex rules for advanced pattern matching. Note: If the domain string contains the character ?, it can only be configured through the GUI.</td> </tr> <tr> <td>regex</td> <td>Matches patterns using wildcards (e.g., *.example.com). Note: Only the * wildcard is supported.</td> </tr> </tbody> </table>	Option	Description	wildcard	Matches using regex rules for advanced pattern matching. Note: If the domain string contains the character ?, it can only be configured through the GUI.	regex	Matches patterns using wildcards (e.g., *.example.com). Note: Only the * wildcard is supported.			
Option	Description									
wildcard	Matches using regex rules for advanced pattern matching. Note: If the domain string contains the character ?, it can only be configured through the GUI.									
regex	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.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>block</td> <td>If the local domain filter action is set to block and an entry matches, then that DNS query is blocked or redirected.</td> </tr> <tr> <td>allow</td> <td>If the local domain filter action is set to allow and an entry matches, it will directly return to the client DNS resolver.</td> </tr> </tbody> </table>	Option	Description	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.			
Option	Description									
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.	option	-							
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable this domain filter to take effect.</td> </tr> <tr> <td>disable</td> <td>Disable this domain filter.</td> </tr> </tbody> </table>	Option	Description	enable	Enable this domain filter to take effect.	disable	Disable this domain filter.			
Option	Description									
enable	Enable this domain filter to take effect.									
disable	Disable this domain filter.									

config dnsfilter profile

Description: Configure the DNS filter profile.

```

config dnsfilter profile
  edit <name>
    config domain-filter
      set domain-filter-table <name>
    end
    set block-action [block| redirect | block-servfail]
    set block-botnet [enable | disable]
    set safe-search [enable | disable]
    set youtube-restrict [strict | moderate]
    set redirect-portal {ipv4-address}
    set redirect-portal6 {ipv6-address}
  
```

```

next
end

```

Parameter	Description	Type	Size	Default								
block-action	Action to take for blocked domains.	option	-									
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>block</td> <td>The DNS request is blocked and a DNS response with NXDOMAIN is returned.</td> </tr> <tr> <td>redirect</td> <td>A DNS response containing the portal IP address is returned, redirecting blocked domains to the SDNS portal.</td> </tr> <tr> <td>block-sevrfail</td> <td>The DNS request is blocked, and a DNS response with SERVFAIL is returned.</td> </tr> </tbody> </table>	Option	Description	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-sevrfail	The DNS request is blocked, and a DNS response with SERVFAIL is returned.			
Option	Description											
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-sevrfail	The DNS request is blocked, and a DNS response with SERVFAIL is returned.											
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option		disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>disable</td> <td>Disable blocking botnet C&C DNS lookups.</td> </tr> <tr> <td>enable</td> <td>Enable blocking botnet C&C DNS lookups.</td> </tr> </tbody> </table>	Option	Description	disable	Disable blocking botnet C&C DNS lookups.	enable	Enable blocking botnet C&C DNS lookups.					
Option	Description											
disable	Disable blocking botnet C&C DNS lookups.											
enable	Enable blocking botnet C&C DNS lookups.											
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option		disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>disable</td> <td>Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.</td> </tr> <tr> <td>enable</td> <td>Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines.</td> </tr> </tbody> </table>	Option	Description	disable	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	enable	Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines.					
Option	Description											
disable	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.											
enable	Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines.											
youtube-restrict	When safe-search is enabled, you can set safe search for YouTube restriction level.	option		disabled								
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>strict</td> <td>Enable strict safe search for YouTube. This restricts YouTube access by responding to DNS resolutions with CNAME restrict.youtube.com.</td> </tr> <tr> <td>moderate</td> <td>Enable moderate safe search for YouTube. This restricts YouTube access by responding to DNS resolutions with CNAME restrictmoderate.youtube.com.</td> </tr> </tbody> </table>	Option	Description	strict	Enable strict safe search for YouTube. This restricts YouTube access by responding to DNS resolutions with CNAME restrict.youtube.com.	moderate	Enable moderate safe search for YouTube. This restricts YouTube access by responding to DNS resolutions with CNAME restrictmoderate.youtube.com.					
Option	Description											
strict	Enable strict safe search for YouTube. This restricts YouTube access by responding to DNS resolutions with CNAME restrict.youtube.com.											
moderate	Enable moderate safe search for YouTube. This restricts YouTube access by responding to DNS resolutions with CNAME restrictmoderate.youtube.com.											
redirect-portal	Enter the IPv4 address of the SDNS redirect portal	IPv4 address		0.0.0.0								
redirect-portal6	Enter the IPv6 address of the SDNS redirect portal	IPv6 address		::								

config domain filter

Parameter	Description	Type	Size	Default
domain-filter	Configure the domain-filter-table parameter to apply a previously created domain filter to this profile.	table	-	
domain-filter-table	Enter the domain filter name.	string	-	



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.