

CLI Reference

FortiExtender 7.6.0



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



Aug 27, 2025

FortiExtender 7.6.0 CLI Reference

TABLE OF CONTENTS

Change Log	6
Introduction	7
Connect to the CLI	7
Console connection	7
SSH access	8
Enable SSH access to the CLI using a local console connection:	8
Access the FortiExtender CLI using SSH	9
CLI commands	11
Header	12
config version	12
Firewall	13
config policy	13
config traffic-shaper	17
config shaping-policy	18
config vip	19
LTE	22
config lte setting	22
config carrier	28
config simmap	29
config plan	30
Router	34
config router policy	34
config static	36
config target	37
config multicast	38
config pim-sm-global	39
config rp-address	39
config interface	39
config OSPF	40
config area	41
config network	41
config ospf-interface	41
config redistribute	42
config prefix-list	44
config rule	45
config route-map	46
config rule	46
System	48
config system global	48
config accprofile	49
config admin	52
config management	55

config fortigate	55
config cloud	56
config local	57
config local-access	58
config fortigate-backup	58
config interface	60
config VRRP	64
config vxlan	65
config aggregate-interface	66
config pppoe-interface	68
config dhcpserver	69
config reserved-addresses	69
config dhcprelay	72
config dns	74
config dns-server	75
config dns-database	76
config dns-entry	77
config vwan-member	79
config sms-notification	82
config receiver	82
config alert	83
config sms-remote-diag	85
config allowed-user	85
config syslog	86
config remote-servers	87
config statistic-report	87
config virtual-wire-pair	90
config api-user	90
config ntp	91
config ntpserver	92
config settings	93
config lan-switch	93
config ports	93
config system switch-interface	94
SNMP	97
config sysinfo	97
config community	97
config user	100
config hosts	101
HMON	104
config interface-monitoring	104
config hchk	104
VPN	108
config ipsec	108
config phase1-interface	108

config phase2-interface	112
config certificate	115
config ca	115
config local	116
Network	118
config address	118
config service	119
config service-custom	119
Execute	121
execute SSH username serverip	121
WiFi	122
config vap	122
config ap-security	124
config wifi-networks	125
config radio-profile	126
config wifi-general	127
User	129
config user radius	129
config user group	130

Change Log

Date	Change Description
08-27-2025	Updated config system switch-interface on page 94.
05-20-2025	Added config pppoe-interface on page 68. Updated config interface on page 60.
03-12-2025	Updated config plan on page 30.
02-06-2025	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 12](#)
- [Firewall on page 13](#)
- [LTE on page 22](#)
- [Router on page 34](#)
- [System on page 48](#)
- [SNMP on page 97](#)
- [HMON on page 104](#)
- [VPN on page 108](#)
- [Network on page 118](#)
- [Execute on page 121](#)



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 12](#)

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 policy on page 13](#)
- [config traffic-shaper on page 17](#)
- [config shaping-policy on page 18](#)
- [config vip on page 19](#)

config policy

Description: Configure firewall policies.

```
config 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]
  next
  delete <name>
  move <name1> [after | before] <name2>
end
purge
show
```

Sample command:

```
FX201E5919000057 (policy) # 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 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
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
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> </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.							
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.																	

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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	port4	Port 4 as the outgoing interface.	any	Any port as the outgoing interface.							
Option	Description													
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										
	<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										

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 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.											

```

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 17.		

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 22](#)
- [config carrier on page 28](#)
- [config simmap on page 29](#)
- [config plan on page 30](#)

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 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										
session-down-detection	Period to confirm a session has been disconnected.	integer	1 - 60	3										
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										

Parameter	Description	Type	Size	Default						
	<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						
	<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.									

Parameter	Description	Type	Size	Default
by-health-monitor	Sim switching occurs based on health checks like Ping/RTT.	option		disable
	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
	Option	Description		
	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
	Option	Description		
	enable	Enable SIM switching based on jitter.		
	disable	Disable SIM switching based on jitter.		
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

Parameter	Description	Type	Size	Default						
switch-back	Direct modem to switch back to a preferred SIM when the secondary SIM is active.	option		none						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>by-time</td> <td>Switch back at a specified time using the HH:MM format.</td> </tr> <tr> <td>by-timer</td> <td>Switch back after the specified duration is over.</td> </tr> </tbody> </table>	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.			
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						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable advanced settings.</td> </tr> <tr> <td>disable</td> <td>Disable advanced settings.</td> </tr> </tbody> </table>	Option	Description	enable	Enable advanced settings.	disable	Disable advanced settings.			
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						
	<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]

```



```

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
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]
  end
end

```

```

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
	Option	Description		
	all	All modems in the device.		

Parameter	Description	Type	Size	Default										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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	modem1	Only modem 1 will be used.	modem2	Only modem 2 will be used. (This option applies to devices with two modems.)							
Option	Description													
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										
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										

Parameter	Description	Type	Size	Default								
	<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								
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 34](#)
- [config static on page 36](#)
- [config target on page 37](#)
- [config multicast on page 38](#)
- [config OSPF on page 40](#)
- [config prefix-list on page 44](#)
- [config route-map on page 46](#)

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 static

Description: Configure static routes.

```

config 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 target

Description: Configure router targets.

```
config 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														
	<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 multicast

Description: Configure multicast router.

```

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

```

- [config pim-sm-global on page 39](#)
- [config rp-address on page 39](#)
- [config interface on page 39](#)

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
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

```

- [config area on page 41](#)
- [config network on page 41](#)
- [config ospf-interface on page 41](#)

- [config redistribute on page 42](#)

config area

Description: Configure OSPF area settings.

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

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
```

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
```

config redistribute

Description: Configure redistribute settings.

- [config connected on page 42](#)
- [config static on page 42](#)

config connected

Description: Configure redistribute connected routes.

```
config connected
  set status [enable | disable]
  set metric-type [1 | 2]
  set metric [0 - 16777214]
  set routemap <name1>
  unset
  show
end
```

config static

Description: Configure redistribute static routes.

```
config redistribute
  config static
    set status [enable | disable]
    set metric-type [1 | 2]
    set metric [0 - 16777214]
    set routemap <name1>
    unset
    show
  end
  show
end
show
end
```

Sample command:

```
FX201E5919000057 (ospf) # show
config router ospf
  set status disable
  set router-id 0.0.0.0
```

```

config area
  edit 192.168.200.24
  next
end
config network
  edit 1
    set prefix 192.168.200.0/24
    set area 192.168.200.24
  next
end
config ospf-interface
  edit 1
    set status enable
    set interface lan
    set mtu-ignore enable
    set cost 3400
  next
end
config redistribute
  config connected
    set status disable
    set metric-type 2
    set metric 10
    set routemap
  end
  config static
    set status disable
    set metric-type 2
    set metric 10
    set routemap
  end
end
end
end

```

Parameter	Description	Type	Size	Default						
status	Status of the OSPF configuration.	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.									
router-id	Router ID.	IPv4 address	-	0.0.0.0						
config area	OSPF area configuration.	IPv4 address	-	none						
config network	OSPF network configuration.	option	-	none						

Parameter	Description	Type	Size	Default																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>prefix</td> <td>Prefix.</td> </tr> <tr> <td>area</td> <td>Attach the network to area.</td> </tr> </tbody> </table>	Option	Description	prefix	Prefix.	area	Attach the network to area.																							
Option	Description																													
prefix	Prefix.																													
area	Attach the network to area.																													
config ospf-interface	OSPF interface configuration.	option	-	none																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>status</td> <td>Enable/disable status.</td> </tr> <tr> <td>interface</td> <td>Interface name.</td> </tr> <tr> <td>cost</td> <td>Cost of the interface: 0 - 65535; 0 means auto-cost.</td> </tr> <tr> <td>mtu-ignore</td> <td>Enable/disable ignore MTU.</td> </tr> </tbody> </table>	Option	Description	status	Enable/disable status.	interface	Interface name.	cost	Cost of the interface: 0 - 65535; 0 means auto-cost.	mtu-ignore	Enable/disable ignore MTU.																			
Option	Description																													
status	Enable/disable status.																													
interface	Interface name.																													
cost	Cost of the interface: 0 - 65535; 0 means auto-cost.																													
mtu-ignore	Enable/disable ignore MTU.																													
config redistribute	Redistribute configuration.	option	-	none																										
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>config connected</td> <td> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>status</td> <td>Enable/disable redistribute connected.</td> </tr> <tr> <td>metric-type</td> <td>Metric type integer.</td> </tr> <tr> <td>metric</td> <td>Redistribute metric setting.</td> </tr> <tr> <td>routemap</td> <td>Route map name.</td> </tr> </tbody> </table> </td> </tr> <tr> <td>config static</td> <td> <table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>status</td> <td>Enable/disable redistribute static.</td> </tr> <tr> <td>metric-type</td> <td>Metric type integer.</td> </tr> <tr> <td>metric</td> <td>Redistribute metric setting.</td> </tr> <tr> <td>routemap</td> <td>Route map name.</td> </tr> </tbody> </table> </td> </tr> </tbody> </table>	Option	Description	config connected	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>status</td> <td>Enable/disable redistribute connected.</td> </tr> <tr> <td>metric-type</td> <td>Metric type integer.</td> </tr> <tr> <td>metric</td> <td>Redistribute metric setting.</td> </tr> <tr> <td>routemap</td> <td>Route map name.</td> </tr> </tbody> </table>	Option	Description	status	Enable/disable redistribute connected.	metric-type	Metric type integer.	metric	Redistribute metric setting.	routemap	Route map name.	config static	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>status</td> <td>Enable/disable redistribute static.</td> </tr> <tr> <td>metric-type</td> <td>Metric type integer.</td> </tr> <tr> <td>metric</td> <td>Redistribute metric setting.</td> </tr> <tr> <td>routemap</td> <td>Route map name.</td> </tr> </tbody> </table>	Option	Description	status	Enable/disable redistribute static.	metric-type	Metric type integer.	metric	Redistribute metric setting.	routemap	Route map name.			
Option	Description																													
config connected	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>status</td> <td>Enable/disable redistribute connected.</td> </tr> <tr> <td>metric-type</td> <td>Metric type integer.</td> </tr> <tr> <td>metric</td> <td>Redistribute metric setting.</td> </tr> <tr> <td>routemap</td> <td>Route map name.</td> </tr> </tbody> </table>	Option	Description	status	Enable/disable redistribute connected.	metric-type	Metric type integer.	metric	Redistribute metric setting.	routemap	Route map name.																			
Option	Description																													
status	Enable/disable redistribute connected.																													
metric-type	Metric type integer.																													
metric	Redistribute metric setting.																													
routemap	Route map name.																													
config static	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>status</td> <td>Enable/disable redistribute static.</td> </tr> <tr> <td>metric-type</td> <td>Metric type integer.</td> </tr> <tr> <td>metric</td> <td>Redistribute metric setting.</td> </tr> <tr> <td>routemap</td> <td>Route map name.</td> </tr> </tbody> </table>	Option	Description	status	Enable/disable redistribute static.	metric-type	Metric type integer.	metric	Redistribute metric setting.	routemap	Route map name.																			
Option	Description																													
status	Enable/disable redistribute static.																													
metric-type	Metric type integer.																													
metric	Redistribute metric setting.																													
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 45](#)

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						
	<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 46](#)

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
	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 48
- [config accprofile](#) on page 49
- [config admin](#) on page 52
- [config management](#) on page 55
- [config interface](#) on page 60
- [config dhcpserver](#) on page 69
- [config dhcprelay](#) on page 72
- [config dns](#) on page 74
- [config dns-server](#) on page 75
- [config dns-database](#) on page 76
- [config dns-entry](#) on page 77
- [config vwan-member](#) on page 79
- [config sms-notification](#) on page 82
- [config sms-remote-diag](#) on page 85
- [config syslog](#) on page 86
- [config virtual-wire-pair](#) on page 90
- [config api-user](#) on page 90
- [config ntp](#) on page 91
- [config settings](#) on page 93
- [config lan-switch](#) on page 93
- [config system switch-interface](#) on page 94

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}
  unset
  show
end
```



```

    set vpn [read-write | read | no-access]
    set network [read-write | read | no-access]
    unset
    next
    show
    abort
    end
delete <name>
purge
show
end

```

Sample command:

```

FX201E5919000057 (accprofile) # show
config system accprofile
  edit some_access
    set header read-write
    set firewall read
    set lte read
    set router no-access
    set system read-write
    set snmp read
    set hmon read
    set vpn no-access
    set network read
  next

```

Parameter	Description	Type	Size	Default								
header	Header settings.	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.											
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								

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.											
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.											
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.											
snmp	SNMP 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.											
hmon	Health monitor 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.											
vpn	VPN 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> </tbody> </table>	Option	Description	read-write	Read-write access.							
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.											
network	Network 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.											

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	Type	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 wildcard is enabled, the remote user can share the account and log in without needing to create multiple user accounts. That means, you can use the user and password pair stored in the remote server without needing to match the table name.</p> <p>Only one wildcard remote account is allowed to exist under system admin.</p>	option	-	disable
password	<p>Admin user password</p> <p>Note: If wildcard 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 remote-auth is enabled, remote-group becomes mandatory. Otherwise remote-group is hidden.</p>	option	-	none

Parameter	Description	Typy	Size	Default
	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.			
trusthost1	Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none
Trusthost2	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	IPv4 address	-	none

Parameter	Description	Typy	Size	Default
Trusthost10	administrator can connect to the device. Address or subnet address and netmask from which the administrator can connect to the device.	IPv4 address	-	none

config management

Description: Configure Extender management settings.

```
config 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
	Option	Description		
	auto	Automatic.		
	fortigate	FortiGate.		
	cloud	FortiExtender Cloud.		
	local	Local.		

- [config fortigate on page 55](#)
- [config cloud on page 56](#)
- [config local on page 57](#)
- [config local-access on page 58](#)
- [config fortigate-backup on page 58](#)

config fortigate

Description: Configure FortiGate settings.


```

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
	Option	Description		
	nat	NAT.		
ip-passthrough	IP-passthrough.			
proxy	Status of proxy connection.	option	-	disable
	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 local

Description: Configure local settings.

```

config local
  set mode [ip-passthrough | nat]
  unset
  show
end

```

Parameter	Description	Type	Size	Default
mode	Networking mode.	option	-	nat

Parameter	Description	Type	Size	Default
	Option	Description		
	nat	NAT.		
	ip-passthrough	IP-passthrough.		

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.		
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 interface

Description: Configure interface settings.

```

config interface
edit <name>
set *type [loopback | virtual-wan | vlan | capwap | dummy]
set status [enable | disable]
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 <name1>, <name2>, ...
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

Parameter	Description	Type	Size	Default
	Option	Description		
	loopback	Loopback interface.		
	virtual-wan	Virtual-WAN interface.		
	vlan	VLAN interface.		
	capwap	CAPWAP interface.		
	dummy	Dummy interface.		
status	Interface status.	option	-	up
	Option	Description		
	up	Bring the interface up.		
	down	Bring the interface down.		
mode	Addressing mode.	option	-	static
	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
	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

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable VRRP virtual MAC.		
	disable	Disable VRRP virtual MAC.		
allowaccess	Types of management access allowed to this interface.	string	-	none
defaultgw	Ability to get the gateway IP from the DHCP server.	option	-	enable
	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
	Option	Description		
	enable	Enable DNS server override.		
	disable	Disable DNS server override.		
redundant-by	Use of the benchmark for redundant algorithm.	option	-	priority
	Option	Description		
	priority	Redundant by priority.		
	cost	Redundant by cost.		
algorithm	LLB algorithm.	option	-	redundant
	Option	Description		
	redundant	Redundant as algorithm.		
	WRR	WRR as algorithm.		
FEC	Forward equivalence class.	option	-	source_ip
	Option	Description		
	source_ip	Forward equivalence class by source IP.		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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	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															
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 64](#)
- [config vxlan on page 65](#)
- [config aggregate-interface on page 66](#)
- [config pppoe-interface on page 68](#)

config VRRP

Description: Configure the VRRP settings.

```

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 vxlan

Description: Configure VXLAN devices

```

config 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	Descripton	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 aggregate-interface

Description: Configure the aggregate interface.

```

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

```

config members

Description: Configure interfaces to be aggregated.

```

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:

```

FX201E5919000057 (aggregate-interface) # show
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

Parameter	Description	Type	Size	Default						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>activebackup</td> <td>Active backup.</td> </tr> <tr> <td>loadbalance</td> <td>Load balance.</td> </tr> </tbody> </table>	Option	Description	activebackup	Active backup.	loadbalance	Load balance.			
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 dhcpserver

Description: Configure DHCP servers.

```

config dhcpserver
  edit <name>
    set status [enable | disable]
    set lease-time [300 - 8640000]
    set dns-service [default | specify | wan-dns]
    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 [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

```

config reserved-addresses

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

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

```

Sample command:

```

FX201E5919000057 (dhcpserver) # show
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
	Option	Description		
	enable	Enable the DHCP server.		
	disable	Disable the DHCP server.		
lease-time	Lease time in seconds. 0 means	integer	300 - 8640000	86400

Parameter	Description	Type	Size	Default		
reserved-address	Status of reserved address and MAC mapping.	Option	-	disable		
	Option	Description				
	enable	Enable reserved-address.				
	disable	Disable reserved-address.				
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 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												
	<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 dns
    set primary {ipv4-address}
    set secondary {ipv4-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:

```

FX201E5919000057 (dns) # show
config system dns
    set primary 208.91.112.53
    set secondary 208.91.112.52
    set timeout 5
    set retry 3
    set dns-cache-limit 5000
    set dns-cache-ttl 1800
    set cache-notfound-responses disable
    set source-ip 0.0.0.0
    set server-select-method least-rtt
end

```

Parameter	Description	Type	Size	Default
primary	Primary DNS server IP address. The default is the FortiGuard primary DNS server IP.	IPv4 address	-	208.91.112.53
secondary	Secondary DNS server IP address. The default is the FortiGuard secondary DNS server.	IPv4 address	-	208.91.112.52
timeout	DNS query timeout interval in seconds.	integer	1 - 10	5
retry	Number of times to retry.	integer	0 - 5	3
dns-cache-limit	Maximum number of records in DNS cache.	integer	0 - 4294967295	5000

Parameter	Description	Type	Size	Default
dns-cache-ttl	Duration in seconds that DNS cache retains information.	integer	60 - 86400	1800
cache-notfound-responses	Status of response from the DNS server when a record is not in cache.	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	The way in which configured servers are prioritized.	option	-	least-rtt
	Option	Description		
	least-rtt	least-rtt as server-select-method.		
	failover	failover as server-select-method.		

config dns-server

Description: Configure DNS servers.

```

config dns-server
  edit <name>
    set *interface <name1>
    set *mode [recursive | non-recursive | forward-only]
    unset
    next
    show
    abort
    end
  delete <name>
  purge
  show
  end

```

Sample command:

```

FX201E5919000057 (dns-server) # show
config system dns-server
  edit 1

```

```

set interface lan
set mode recursive
next
end

```

Parameter	Description	Type	Size	Default
Name	Name of the DNS server.	string	1 - 35 characters in length	none
interface	A system interface enabled for DNS service.	option	-	none
mode	DNS server mode.	option	-	none
	Option	Description		
	recursive	Shadow the DNS database and forward.		
	non-recursive	Public DNS database only.		
	forward-only	Forward only.		

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

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 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						
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
	Option	Description		
	enable	Enable resource record.		

Parameter	Description	Type	Size	Default												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>disable</td> <td>Disable resource record.</td> </tr> </tbody> </table>				Option	Description	disable	Disable resource record.								
Option	Description															
disable	Disable resource record.															
type	Resource record type.	option	-	A												
	<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

Parameter	Description	Type	Size	Default
out-bandwidth-threshold	Bandwidth threshold in MB for output traffic. 0 indicates infinity.	integer	0 - 2147483647	0
health-check	Link health check of the virtual-wan member.	string	-	none
health-check-fail-threshold	The number of consecutive failed probes before the member is considered dead.	integer	1 - 10	5
health-check-success-threshold	The number of consecutive successful probes before the member is considered alive.	integer	1 - 10	5
link-cost-factor	Criteria by which link selection is made.	option	-	none
		Option	Description	
		latency	link-cost-factor based on latency.	
		jitter	link-cost-factor based on jitter.	
		packetloss	link-cost-factor based on packet-loss.	
latency-threshold	Latency in milliseconds for SLA to make decisions.	integer	0 - 10000000	5

Parameter	Description	Type	Size	Default
jitter-threshold	Jitter in milliseconds for SLA to make decisions.	integer	0 - 10000000	5
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 82](#)
- [config alert on page 83](#)

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

Parameter	Description	Type	Size	Default
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

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	string	Up to 127	data plan is

Parameter	Description	Type	Size	Default
	exhausted alert message.		characters in length.	exhausted
session-disconnect	LTE data session disconnect alert message.	string	Up to 127 characters in length.	LTE data session is disconnected
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 85](#)

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																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the sender.</td> </tr> <tr> <td>disable</td> <td>Disable the sender.</td> </tr> </tbody> </table>	Option	Description	enable	Enable the sender.	disable	Disable the sender.															
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																		
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>reboot</td> <td>Root the device.</td> </tr> <tr> <td>factory-reset</td> <td>Reset the device to its factory settings.</td> </tr> <tr> <td>set-apn</td> <td>Set the APN.</td> </tr> <tr> <td>modem-reset</td> <td>Reset the modem.</td> </tr> <tr> <td>get-modem-status</td> <td>Get the modem status.</td> </tr> <tr> <td>get-extender-status</td> <td>Get the FortiExtender status.</td> </tr> <tr> <td>get-system-version</td> <td>Get the system version.</td> </tr> <tr> <td>get-system-status</td> <td>Get the system status.</td> </tr> </tbody> </table>	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.			
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]
  end
end

```

```

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
	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
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
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
	Option	Description		
	fortiguard	The FortiGuard NTP server.		
	custom	A custom NTP server.		

- [config ntpserver on page 92](#)

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 lan-switch

Description: Configure LAN switch settings.

config ports

Description: Configure LAN switch ports.

```
config system lan-switch
  config ports
    edit <name>
      set
      unset
      next
      show
      abort
    end
    delete <name>
    purge
    show
  end
show
end
show
end
```

Sample command:

```
FX201E5919000057 # config system lan-switch
FX201E5919000057 (lan-switch) # show
config system lan-switch
  config ports
    edit port1
    next
    edit port2
    next
    edit port3
    next
  end
end
```

Parameter	Description	Type	Size	Default
name	The LAN port ID.	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.

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}
  next
end
set stp [enable | disable]
next
end

```

Sample syntax:

```

config system switch-interface
edit le-switch
set vlan-support enable
config member
edit port1 # access port
set type physical
set port port1
set vids
set pvid 101
next
edit port4 # access port
set type physical
set port port4
set vids
set pvid 102
next
edit le-agg-link # trunk port
set type aggregate
set port le-agg-link
set vids 101 102
set pvid 0
next
end
set stp disable
next
end

```

Parameter	Description	Type	Size	Default
name	The LAN port ID.	string	-	none
vlan-support	Enable/disable VLAN support.	option	-	
config member	Interfaces within the virtual switch.	option	-	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	-	

Parameter	Description	Type	Size	Default						
vids	VLAN ID list.	integer	1 to 4089							
pvid	Port VLAN ID.	integer	1 to 4089							
stp	Spanning Tree Protocol.	option	-	disable						
	<table><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.									

SNMP

This section shows the syntax of the following commands:

- [config sysinfo on page 97](#)
- [config community on page 97](#)
- [config user on page 100](#)
- [config hosts on page 101](#)

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						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable the SNMP community configuration.</td> </tr> <tr> <td>disable</td> <td>Disable the SNMP community configuration.</td> </tr> </tbody> </table>				Option	Description	enable	Enable the SNMP community configuration.	disable	Disable the SNMP community configuration.
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						
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>enable</td> <td>Enable SNMP v1 queries.</td> </tr> <tr> <td>disable</td> <td>Disable SNMP v1 queries.</td> </tr> </tbody> </table>				Option	Description	enable	Enable SNMP v1 queries.	disable	Disable SNMP v1 queries.
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-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 address of the SNMP manager (host) in x.x.x.x/24 format.	IPv4 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.

Sample command:

```

FX201E5919000057 (snmp) # show
config snmp
  config sysinfo
    set status enable
    set description this is a test comment
    set contact-info +15082558567
    set location
  end
  config community
    edit comm1
      set name 1
      set status enable
      set hosts host1
      set query-v1-status enable
      set query-v1-port 161
      set query-v2c-status disable
      set query-v2c-port 161
      set trap-v1-status disable
      set trap-v1-lport 162
      set trap-v1-rport 162
      set trap-v2c-status disable
      set trap-v2c-lport 162
      set trap-v2c-rport 162
      set events data-exhausted fgt-backup-mode-switch
    next
  end
config user
  edit user1

```

```
    set name user1
    set status enable
    set notify-hosts host1
    set trap-status enable
    set trap-lport 162
    set trap-rport 162
    set queries disable
    set query-port 161
    set events data-exhausted fgt-backup-mode-switch low-signal-strength
    set security-level auth-priv
    set auth-proto sha1
    set auth-pwd *****
    set priv-proto aes
    set priv-pwd *****
  next
end
config hosts
  edit host1
    set host-ip 192.168.1.100/24
    set host-type any
  next
end
end
```

HMON

This section shows the syntax of the following commands:

- [config interface-monitoring on page 104](#)
- [config hchk on page 104](#)

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 108](#)
- [config certificate on page 115](#)

config ipsec

Description: Configure IPsec settings.

- [config phase1-interface on page 108](#)
- [config phase2-interface on page 112](#)

config phase1-interface

Description: Configure the VPN remote gateway.

```
config vpn ipsec phase1-interface
  edit <name>
    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 *remotegw-ddns {string} *available when type is set to ddns
    set authmethod [psk | signature]
    set *psksecret {string}
    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												
ike-version	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	Phase1 proposal.	option	-	aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-sha1												
	<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> </tbody> </table>	Option	Description	des-md5		des-sha1		des-sha256		3des-md5		3des-sha1				
Option	Description															
des-md5																
des-sha1																
des-sha256																
3des-md5																
3des-sha1																

Parameter	Description	Type	Size	Default																																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <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	3des-sha256		aes128-md5		aes128-sha1		aes128-sha256		aes256-md5		aes256-sha1		aes256-sha256																								
Option	Description																																							
3des-sha256																																								
aes128-md5																																								
aes128-sha1																																								
aes128-sha256																																								
aes256-md5																																								
aes256-sha1																																								
aes256-sha256																																								
dhgrp	DH group.	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> <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	1		2		5		14		15		16		17		18		19		20		21		27		28		29		30		31		32				
Option	Description																																							
1																																								
2																																								
5																																								
14																																								
15																																								
16																																								
17																																								
18																																								
19																																								
20																																								
21																																								
27																																								
28																																								
29																																								
30																																								
31																																								
32																																								
interface	The outgoing 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 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.															
remote-gw	The IPv4 address of the remote gateway's external interface.	IPv4 address	-	none												
authmethod	Authentication method.	option	-	psk												
	<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.															
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	string	-	none												
localid	Local ID.	string	-	none												
peerid	Peer identity.	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												
	<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.	string	-	none												

Parameter	Description	Type	Size	Default
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 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 encapsulation [tunnel-mode | transport-mode]
set protocol [0 - 255]
set src-addr-type [subnet | range | ip | name]
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-port [0 - 65535]
set dst-addr-type [subnet | range | ip | name]
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-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
pfs	Status of the PFS feature.	option	-	enable
	Option	Description		
	enable	Enable PFS.		
	disable	Disable PFS.		
dhgrp	Phase 2 DH group.	option	-	14, 5
	Option	Description		
	1			
	2			
	5			
	14			
	15			
	16			

Parameter	Description	Type	Size	Default
	Option	Description		
	17			
	18			
	19			
	20			
	21			
	27			
	28			
	29			
	30			
	31			
	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.		

Parameter	Description	Type	Size	Default
	Option	Description		
	ip	IPv4 IP.		
	name	IPv4 network address 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
dst-addr-type	Remote proxy ID type.	option	-	subnet
	Option	Description		
	subnet	IPv4 subnet.		
	range	IPv4 range.		
	ip	IPv4 IP.		
	name	IPv4 network address name.		
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
src-start-ip	Local proxy ID start.	IPv4 address	-	none
src-end-ip	Local proxy ID end.	IPv4 address	-	none
dst-start-ip	Remote proxy ID start.	IPv4 address	-	none
dst-end-ip	Remote proxy ID end	IPv4 address	-	none
src-name	Local proxy ID name.	string	-	none
dst-name	Remote proxy ID name.	string	-	none

config certificate

Description: Configure VPN certificates.

- [config ca on page 115](#)
- [config local on page 116](#)

config 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
```

config local

Description: Configure Local keys and certificates.

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

Sample command:

```
FX201E5919000057 (certificate) # show
config vpn certificate
  config ca
    edit Fortinet_CA
      set comment
      set source factory
    next
    edit Fortinet_CA_Backup
      set comment
      set source factory
    next
    edit Fortinet_Sub_CA
      set comment
      set source factory
    next
  end
  config local
    edit Fortinet_Factory
```

```
    set comment
    set source factory
next
edit Fortinet_Factory_Backup
    set comment
    set source factory
next
end
end
```

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

Network

This section shows the syntax of the following commands:

- [config address on page 118](#)
- [config service-custom on page 119](#)

config address

Description: Configure IPv4 addresses.

```
config 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
	Option	Description		
	ipmask	IP address and subnet mask.		
	iprange	IP range.		

Parameter	Description	Type	Size	Default
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 ommand:

```

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										
	<table><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><tr><td>ip</td><td>IP protocol.</td></tr></tbody></table>	Option	Description	tcp	TCP protocol.	udp	UDP protocol.	icmp	ICMP protocol.	ip	IP protocol.			
Option	Description													
tcp	TCP protocol.													
udp	UDP protocol.													
icmp	ICMP protocol.													
ip	IP protocol.													
protocol-number	IP protocol number.	integer	0 - 254	0										

Execute

This section shows the syntax of the following command:

- [execute SSH username serverip on page 121](#)

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
```

WiFi

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



WiFi is for the FEV-211F platform only.

- [config vap on page 122](#)
- [config ap-security on page 124](#)
- [config wifi-networks on page 125](#)
- [config radio-profile on page 126](#)
- [config wifi-general on page 127](#)

config vap

Description: Configure WiFi virtual access point.

```
Edit <WiFi Access Point Name>
  set ssid <name>
  set broadcast-ssid [enable | disable]
  set dtim {1-255}
  set rts-threshold {256-2347}
  set max-clients {0-512}
  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>
```



FortiExtender supports the following security modes:

- OPEN
- WPA2-Personal
- WPA-WPA2-Personal
- WPA3-SAE
- WPA3-SAE-Transition
- WPA2-Enterprise
- WPA3-Enterprise-Only
- WPA3-Enterprise-Transition
- WPA3-Enterprise-192-bit



If security-mode is set to WPA2-Personal, WPA-WPA2-Personal, WPA3-SAE, or WPA3-SAE-Transition, you must also configure the following settings:

```
set pmf <option>
set passphrase <password>
```



If security-mode is set to WPA2-Enterprise, WPA3-Enterprise-Only, WPA3-Enterprise-Transition, or WPA3-Enterprise-192-bit, you must configure the following settings:

```
set auth-server-addr <url>
set auth-server-port <port number> # default as 1812
set auth-server-secret <password>
```

Sample command:

```
config wifi 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
```

config ap-security

Description: Configure security mode for WiFi access point.

```
config ap-security
    set security-mode <encryption mode>
    # Security encryption modes including:
        OPEN
        WPA2-Personal
        WPA-WPA2-Personal
        WPA3-SAE
        WPA3-SAE-Transition
        WPA2-Enterprise
        WPA3-Enterprise-Only
        WPA3-Enterprise-Transition
        WPA3-Enterprise-192-bit
    if security-mode chooses OPEN:
        set pmf <option>
        # pmf option includes the options:
            disabled
            optional
            required
    if security-mode chooses these options: WPA2-Personal, WPA-WPA2-Personal, WPA3-SAE,WPA3-SAE-
        Transition, configure the following commands:
            set pmf <option>
            set passphrase <password>
    if security-mode chooses these options: WPA2-Enterprise, WPA3-Enterprise-Only, WPA3-Enterprise-
        Transition, WPA3-Enterprise-192-bit, configure the following commands:
            set auth-server-addr <url>
            set auth-server-port <port number> # default as 1812
            set auth-server-secret <password>
```

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 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 wlan-members
  config ap-security
    set security-mode WPA2-Personal
    set pmf disabled
    set passphrase *****
  end
next
end
```

config wifi-networks

Description: Configure WiFi networks for Station Mode.

```
edit <name>
  set ssid <id>
  set security-mode <encryption mode>
  # the security mode has the following options:
  OPEN
  WPA-Personal
  WPA2-Personal
  WPA-WPA2-Personal
  WPA3-SAE
  WPA3-SAE-Transition
  WPA-Enterprise
  WPA2-Enterprise
  WPA-WPA2-Enterprise
  WPA3-Enterprise-Only
  WPA3-Enterprise-Transition
  set pmf <option>
  # pmf option includes the options:
  disabled
  optional
  required
```

Sample command:

```
config wifi wifi-networks
  edit 2g-ArloNetwork
    set ssid ArloNetwork
    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
```

config radio-profile

Description: Configure WiFi Radio profile.

```
config wifi radio-profile
edit <radio profile name>
set band <2GHz/5GHz>
set status <enable/disable>
set role <lan/wan> # two options for role, as lan and wan
If role is set as lan, configure the following parameters for the WiFi lan interface:
set operating-standards auto
set beacon-interval {100-3500}
set 80211d [ enable | disable]
set max-clients {0-512}
set power-mode auto
  set channel
set bandwidth auto
set extension-channel auto
set guard-interval auto
set vap <ap names> #maximum 4 APs for the vap configure
```

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
```

config wifi-general

Description: Configure general WiFi settings.

```
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 county codes varies with the region code of the devices in use. The list of country codes shown above applies to devices with the region code "A" only.

User

This section shows the syntax of the following commands:

- [config user radius on page 129](#)
- [config user group on page 130](#)

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}
  next
end
```

Sample command:

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

Parameter	Description	Type	Size	Default
name	Name of the RADIUS server table.	string	-	none
server	Primary RADIUS server IP address in IPv4.	string	-	none
secret	Pre-shared secret key used to access the primary RADIUS server.	password	1-128	none

Parameter	Description	Type	Size	Default
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

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.



www.fortinet.com

Copyright© 2025 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.