CLI Reference

FortiBranchSASE 7.6.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

Sep 26, 2025
FortiBranchSASE 7.6.4 CLI Reference

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-09-26	Initial release.

Introduction

FortiBranchSASE is a member of the FortiExtender product family. While FortiExtender and FortiBranchSASE share many features, this guide provides information specific to FortiBranchSASE

This *Reference Guide* introduces the syntax of commonly used CLI commands to configure and manage a FortiBranchSASE unit.

CLI commands in this *Reference Guide* are based on FortiBranchSASE-20G-WiFi.

Connect to the CLI

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

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

To access the FortiBranchSASE CLI via the FortiBranchSASE 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 FortiBranchSASE CLI outside of the GUI using:

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

Console connection

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

Direct console access to a FortiBranchSASE 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 FortiBranchSASE console, you need a console cable to connect the console port on the FortiBranchSASE 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 FortiBranchSASE 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 FortiBranchSASE 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 FortiBranchSASE, you must also configure the FortiBranchSASE using a static route that can forward packets from the FortiBranchSASE to the computer. This can be done using a local console connection or in the GUI.

To connect to the FortiBranchSASE 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 FortiBranchSASE network port either directly to the network port on your computer or to a network through which your computer can reach the FortiBranchSASE.
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
   end
   ```

   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, for example:

   ```
   config system interface
   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 FortiBranchSASE CLI using SSH

Once the FortiBranchSASE 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 FortiBranchSASE 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 FortiBranchSASE.

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

6. Click *Yes* to accept the FortiBranchSASE'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 FortiBranchSASE hostname followed by #). You can now enter CLI commands.

Header

This section shows the syntax of the following command:

- config version on page 11

config version

Description: Configure header version settings.

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

Sample command:

```
config header
  config version
    set config 10517384
    set certificate 3876258
  end
end
```

Parameter	Description	Type	Size	Default
config	Device configuration version.	integer	-	none
certificate	VPN certificate version.	integer	-	none

Firewall

This section shows the syntax of the following commands:

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:

```
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
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>srcintf</td><td>Incoming (ingress) interface.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>port4</td><td>Port 4 as the incoming interface.</td></tr>
<tr><td>any</td><td>Any port as the incoming interface.</td></tr>
</table></td></tr>
<tr><td>dstintf</td><td>Outgoing (egress) interface.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>port4</td><td>Port 4 as the outgoing interface.</td></tr>
<tr><td>any</td><td>Any port as the outgoing interface.</td></tr>
</table></td></tr>
<tr><td>srcaddr</td><td>Source address.</td><td>option</td><td>-</td><td>none</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table></td></tr>
<tr><td>dnat</td><td>Destination NAT.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable destination NAT.</td></tr>
<tr><td>disable</td><td>Disable destination NAT.</td></tr>
</table></td></tr>
<tr><td>dstaddr</td><td>Destination address.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table></td></tr>
<tr><td>action</td><td>Policy action.</td><td>option</td><td>-</td><td>accept</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>accept</td><td>Accept policy.</td></tr>
<tr><td>deny</td><td>Deny policy.</td></tr>
</table></td></tr>
<tr><td>status</td><td>Status of the policy.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Decription</th></tr>
<tr><td>enable</td><td>Enable this policy.</td></tr>
<tr><td>disable</td><td>Disable this policy.</td></tr>
</table></td></tr>
<tr><td>service</td><td>Service/service group name.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table></td></tr>
</table>

Parameter	Description	Type	Size	Default
nat	Source NAT.	option	-	disable

Option	Description
enable	Enable source NAT.
disable	Disable source NAT.

```
(policy) # move test2 after all-pass
(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
```

config traffic-shaper

Description: Configure firewall shapers.

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

Sample command:

```
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:

```
config firewall shaping-policy
  edit 1_policy
    set status enable
    set dstintf port1
    set traffic-shaper 1
  next
end
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>status</td><td>Status of the traffic shaping policy.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable the policy.</td></tr><tr><td>disable</td><td>Disable the policy.</td></tr></table></td></tr>
<tr><td>dstintf</td><td>Outgoing (egress) interface.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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>port4</td><td>Port 4 as the outgoing interface.</td></tr><tr><td>any</td><td>Any port as the outgoing interface.</td></tr></table></td></tr>
<tr><td>traffic-shaper</td><td>Traffic shaper to apply to traffic forwarded by the firewall policy.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Decription</th></tr><tr><td>1</td><td>Refer toconfig traffic-shaper on page 16.</td></tr></table></td></tr>
</table>

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:

```
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
```

Parameer	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	IPv4 address	-	none

<table>
<tr><th>Parameer</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td>network to which the external IP address is mapped.</td><td></td><td></td><td></td></tr>
<tr><td>extintf</td><td>Interface connected to the source network that receives packets to be forwarded to the destination network.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>port4</td><td>Port 4 as the outgoing interface.</td></tr>
<tr><td>any</td><td>Any port as the outgoing interface.</td></tr>
</table></td></tr>
<tr><td>portforward</td><td>Port forwarding.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Decription</th></tr>
<tr><td>enable</td><td>Enable port forwarding.</td></tr>
<tr><td>disable</td><td>Disable port forwarding.</td></tr>
</table></td></tr>
<tr><td>protocol</td><td>Protocol to use when forwarding packets.</td><td>option</td><td>-</td><td>tcp</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table></td></tr>
<tr><td>extport</td><td>Incoming port number to be mapped to a port number on the destination network.</td><td>number</td><td>1 - 65535</td><td>0</td></tr>
<tr><td>mappedport</td><td>Port number on the destination network to which the external port number is mapped.</td><td>number</td><td>1 - 65535</td><td>0</td></tr>
</table>

Router

This section shows the syntax of the following commands:

config router policy

Description: Configure router policies.

```
config route 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:

```
config router policy
    edit 1
        set input-device lan
        set srcaddr all
        set dstaddr all
        set service ALL
        set target target.port1
        set status enable
        set comment this is a test policy
    next
end
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>input-device</td><td>Incoming interface name.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>lan</td><td>LAN as the input device.</td></tr>
<tr><td>lo</td><td>Loopback as the input device.</td></tr>
<tr><td>port4</td><td>Port 4 as the input device.</td></tr>
<tr><td>port1</td><td>Port 1 as the input device.</td></tr>
</table></td></tr>
<tr><td>srcaddr</td><td>Source address.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>lan</td><td>LAN network address.</td></tr>
<tr><td>all</td><td>All the network addresses.</td></tr>
<tr><td>none</td><td>None of the network addresses.</td></tr>
</table></td></tr>
<tr><td>dstaddr</td><td>destination address.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>lan</td><td>LAN network address.</td></tr>
<tr><td>all</td><td>All the network addresses.</td></tr>
<tr><td>none</td><td>None of the network addresses.</td></tr>
</table></td></tr>
<tr><td>service</td><td>Service/service group names.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>ALL_ICMP</td><td>ICMP.</td></tr>
<tr><td>ALL</td><td>All.</td></tr>
<tr><td>etc</td><td>Refer to the different services in this command.</td></tr>
</table></td></tr>
<tr><td>target</td><td>The PBR's out-going interface and next-hop.</td><td>option</td><td>-</td><td>none</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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.port4</td><td>Port 4 as the target.</td></tr>
<tr><td>target.Port1</td><td>Port 1 as the target.</td></tr>
</table></td></tr>
<tr><td>status</td><td>Status of the policy based the routing rule.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable the policy.</td></tr>
<tr><td>disable</td><td>Disable the policy.</td></tr>
</table></td></tr>
<tr><td>comment</td><td>Comment on the policy.</td><td>string</td><td>1 - 255 characters in length</td><td>none</td></tr>
</table>

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:

```
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 port1
        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:

```
config router target
    edit target.lo
        set interface lo
        set next-hop
next
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>interface</td><td>Target interface.</td><td>option</td><td></td><td>none</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<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>port4</td><td>Port 4 as the target interface.</td></tr>
<tr><td>port1</td><td>Port 1 as the target interface.</td></tr>
</table>
</td></tr>
<tr><td>next-hop</td><td>Next-hop IP address in x.x.x.x format.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
</table>

config multicast

Description: Configure multicast router.

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

- config pim-sm-global on page 24
- config rp-address on page 24
- config interface on page 25

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.

Although "set" is an available option, there's no entry for the "set" command.

```
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:

```
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
```

Sample command:

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>status</td><td>Set the status of the OSPF:</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable OSPF</td></tr>
<tr><td>disable</td><td>Disable OSPF</td></tr>
</table></td></tr>
</table>

Parameter	Description	Type	Size	Default
set router-id	The router-id is a unique identity to the OSPF router. If no router-id is specified, the system will automatically choose the highest IP address as the router-id.	IPv4 address	-	0.0.0.0

- config area on page 27
- config network on page 28
- config ospf-interface on page 29
- config redistribute on page 30

config area

Description: Configure OSPF area settings.

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

Sample command:

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

Parameter	Description	Type	Size	Default
config area	OSPF area configuration. An area is a logical grouping of contiguous networks and routers in the same area with the same link-state database and topology. **Note:** The current release only supports Area 0 called the backbone area, and does not support multiple areas. All routers inside an area must have the same area ID to become OSPF neighbors. You can add Area 0 by editing Area 0.0.0.0	IPv4 address	-	none

config network

Description: Configure OSPF network settings.

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

Sample command:

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

Parameter	Description	Type	Size	Default
config network	OSPF network configuration.	option	-	none

Option	Description
prefix	Prefix used to identify network/subnet address for advertising to the OSPF domain.
area	Attach the network to area.

CLI Command	Description

`config network`
`edit [id]`
`set prefix`
`[X.X.X.X/Y]`
`set area 0.0.0.`
`Prefix`
	• id—string
	• X.X.X.X—Network prefix
	• Y—Netmask

config ospf-interface

Description: Configure OSPF interface settings.

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

Sample command:

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>config ospf-interface</td><td>OSPF interface configuration.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td>status</td><td>Enable/Disable OSPF processing on the said interface.</td><td>option</td><td></td><td>-</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable OSPF processing on the said interface.</td></tr><tr><td>disable</td><td>Disable OSPF processing on the said interface.</td></tr></table></td></tr>
<tr><td>set interface</td><td>Must be the VPN tunnel interface as OSPF is built over IPSEC VPN.</td><td></td><td></td><td></td></tr>
<tr><td>set mtu-ignore</td><td>Prevents OSPF neighbor adjacency failure caused by mismatched MTUs.</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>OSPF will stop detecting mismatched MTUs before</td></tr></table></td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td></td><td>forming OSPF adjacency</td></tr><tr><td>disable</td><td>OSPF will detect mismatched MTUs, and OSPF adjacency is not established if MTU is mismatched.</td></tr></table></td></tr>
<tr><td>set cost</td><td>Interface cost used to calculate the best path to reach other routers in the same area. 0 means auto-cost.</td><td>integer</td><td>0—
65535</td><td></td></tr>
</table>

config redistribute

Description: Configure redistribute settings.

```
config router ospf
  config redistribute
    config [connected | static]
      set status [enable | disable]
      set metric-type [1 | 2]
      set metric <value>
      set route-map <route-map name>
```

Sample command:

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

Parameter	Description	Type	Size	Default
status	Enable/disable redistributing routes.			
set metric-type	Specify the external link type to be used for the redistributed routes. The options are E1 and E2 (default).			E2

Parameter	Description	Type	Size	Default
set metric	Used for the redistributed routes.	integer	1 - 16777214	10
set routemap	Route map name.			

config prefix-list

Description: Configure IPv4 prefix lists.

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

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

- config rule on page 31

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:

```
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
	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 32

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:

```
config router route-map
    edit 1
        config rule
            edit 1
                set action permit
                set match-ip-address 1
            next
        end
    next
end
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>action</td><td>Action of the rule.</td><td>option</td><td>-</td><td>permit</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>match-ip-address</td><td>Match IP address permitted by the prefix-list.</td><td>string</td><td>-</td><td>none</td></tr>
</table>

System

This section shows the syntax of the following commands:

config system global

Description: Configure FortiBranchSASE global settings.

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

Sample command:

```
config system global
  set hostname BS20GWS224000007
  set timezone 80
  set auto-install-image disable
  set mdm-fw-server Fortiextender-firmware.forticloud.com
  set os-fw-server Fortiextender-firmware.forticloud.com
  set admin-server-cert my_fex_cert
end
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>hostname</td><td>Device display name.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>timezone</td><td>System timezone setting. (Note: Use the 'get timezone list' command to check the timezone ID.)</td><td>integer</td><td>0 - 87</td><td>80</td></tr>
<tr><td>auto-install-image</td><td>Automatically install image from USB.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable auto-install-image.</td></tr>
<tr><td>disable</td><td>Disable auto-install-image.</td></tr>
</table></td></tr>
<tr><td>default-image-file</td><td>Image file from USB.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>mdm-fw-server</td><td>Cloud modem image upgrade URL.</td><td>string</td><td>-</td><td>Fortiextender-firmware.forticloud.com</td></tr>
<tr><td>os-fw-server</td><td>Cloud OS image upgrade URL.</td><td>string</td><td>-</td><td>Fortiextender-firmware.forticloud.com</td></tr>
<tr><td>admin-server-cert</td><td>Server certificate that the FortiBranchSASE uses for HTTPS administrative connections.</td><td>string</td><td>-</td><td>Fortinet_Factory_Backup</td></tr>
</table>

config system accprofile

Description: Configure administration access profiles.

```
config system accprofile
  edit <name>
```

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

Sample command:

```
config system accprofile
    edit some_access
        set header read-write
        set firewall read
        set router no-access
        set system read-write
        set snmp read
        set hmon read
        set vpn no-access
        set network read
        set wifi read
        set user read-write
    next
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>header</td><td>Header settings.</td><td>option</td><td>-</td><td>read</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table></td></tr>
<tr><td>firewall</td><td>Firewall configuration.</td><td>option</td><td>-</td><td>read</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>router</td><td>Router configuration.</td><td>option</td><td>-</td><td>read</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>system</td><td>System configuration.</td><td>option</td><td>-</td><td>read</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>snmp</td><td>SNMP configuration.</td><td>option</td><td>-</td><td>read</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>hmon</td><td>Health monitor configuration.</td><td>option</td><td>-</td><td>read</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>vpn</td><td>VPN configuration.</td><td>option</td><td>-</td><td>read</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>read-write</td><td>Read-write access.</td></tr></table></td></tr>
</table>

Parameter	Description	Type	Size	Default
	Option	**Description**		
	read	Read access.		
	no-access	No access.		
network	Network configuration.	option	-	read
	Option	**Description**		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		
wifi	Wi-Fi configuration	option	-	read
	Option	**Description**		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		
user	User configuration	option	-	read
	Option	**Description**		
	read-write	Read-write access.		
	read	Read access.		
	no-access	No access.		

config admin

Description: Configure user access.

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

Sample command:

```
config system admin
  edit remote1
    set accprofile super_admin
    set remote-auth enable
    set wildcard enable
    set password ENC *
    set remote-group group1
    set trusthost1 192.168.200.110/24
    set trusthost2
    set trusthost3
    set trusthost4
    set trusthost5
    set trusthost6
    set trusthost7
    set trusthost8
    set trusthost9
    set trusthost10
  next
end
```

Parameter	Description	Typy	Size	Default
accprofile	Access profile.	string	-	none
remote-auth	Enable/disable authentication using a remote RADIUS server	option	-	disable
wildcard	Enable/disable wildcard RADIUS authentication **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.	option	-	disable

Parameter	Description	Typy	Size	Default
	Only one wildcard remote account is allowed to exist under `system admin`.			
password	Admin user password **Note:** If `wildcard` is enabled, you cannot set a password.	string	-	none
remote-group	Enter the FortiBranchSASE user group name you want to use for remote authentication. **Note:** If `remote-auth` is enabled, `remote-group` becomes mandatory. Otherwise `remote-group` is hidden. If `remote-auth` is enabled but `wildcard` is disabled, you must set a local `password`. If the RADIUS server is unreachable, FortiBranchSASE uses the local password. For other situations, such as if FortiBranchSASE receives a RADIUS reject message, the local password is omitted.	option	-	none
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	IPv4 address	-	none

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

config system bluetooth

Description: Configure Bluetooth settings on BLE capable models.

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

Sample command:

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

Parameter	Description	Type	Size	Default
status	Enable or disable the Bluetooth button on applicable models.	option	-	enable

Parameter	Description	Type	Size	Default

Option	Description
enable	Enable the Bluetooth button. The Bluetooth button can be triggered to provide Bluetooth functionality.
disable	Disable the Bluetooth button. Pressing the Bluetooth button will not trigger anything.

config 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	FortiEdge Cloud.
local	Local.

- config fortigate on page 42
- config cloud on page 43
- config local on page 44
- config local-access on page 45
- config fortigate-backup on page 45

config fortigate

Description: Configure FortiGate settings.

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

Parameter	Description	Type	Size	Default
ac-discovery-type	The method that the device uses to discover the AC, i.e., FortiGate.	option	-	broadcast
	Option	**Description**		
	broadcast	Broadcast.		
	static	Static IP address.		
server	IP address or hostname of the AC server.	string	-	none
ac-ctl-port	CAPWAP control port of the AC server.	integer	1024 - 49150	5246
ac-data-port	CAPWAP data port of the AC server.	integer	1024 - 49150	5246
discovery-intf	The physical port from which FortiBranchSASE sends broadcast packets in search for FortiGate.	option	-	none
	Option	**Description**		
	lan	LAN as the discovery interface.		
	Port1	Port 1 as the discovery interface.		
	port2	Port 2 as the discovery interface.		

config cloud

Description: Configure Cloud settings.

```
config cloud
      set dispatcher {string}
      set dispatcher-port {integer}
      set mode [ip-passthrough | nat]
      set proxy [enable | disable]
```

```
        set proxy-server {ipv4-address} *available when proxy is enabled
        set proxy-port [1 – 65535] *available when proxy is enabled
        unset
        show
        end
```

Parameter	Description	Type	Size	Default
dispatcher	Cloud dispatch URL.	string	-	Fortiextender-dispatch.forticloud.com
dispatcher-port	Cloud dispatch port.	integer	0 - 9223372036854775807	443
mode	Networking mode.	option	-	nat
	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
	Option	**Decription**		
	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.

Parameter	Description	Type	Size	Default
	Option	**Description**		
	lo	Loopback as vrrp-interface.		
	Port1	Port 1 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:

```
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 port1
  set status enable
end
end
```

config system interface

Description: Configure interface settings.

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

Parameter	Description	Type	Size	Default
type	Interface type.	option	-	none

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable VRRP virtual MAC.</td></tr><tr><td>disable</td><td>Disable VRRP virtual MAC.</td></tr></table></td></tr>
<tr><td>allowaccess</td><td>Types of management access allowed to this interface.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>security-mode</td><td>Turn on captive portal authentication for this interface.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No security option.</td></tr><tr><td>captive-portal</td><td>Captive portal authentication.</td></tr></table></td></tr>
<tr><td>security-external-web</td><td>URL of external authentication web server.</td><td>string</td><td>Maximum length: 255</td><td>-</td></tr>
<tr><td>security-groups</td><td>Names of user groups that can authenticate with the captive portal.</td><td>options</td><td>-</td><td>-</td></tr>
<tr><td>security-exempt-list</td><td>Name of security-exempt-list.</td><td>options</td><td>-</td><td>-</td></tr>
<tr><td>security-redirect-url</td><td>URL redirection after disclaimer/authentication.</td><td>string</td><td>Maximum length: 255</td><td>-</td></tr>
<tr><td>defaultgw</td><td>Ability to get the gateway IP from the DHCP server.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable getting the gateway IP from the DHCP server.</td></tr><tr><td>disable</td><td>Disable getting the gateway IP from the DHCP server.</td></tr></table></td></tr>
<tr><td>dns-server-override</td><td>Use DNS acquired by DHCP.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DNS server override.</td></tr><tr><td>disable</td><td>Disable DNS server override.</td></tr></table></td></tr>
<tr><td>redundant-by</td><td>Use of the benchmark for redundant algorithm.</td><td>option</td><td>-</td><td>priority</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>priority</td><td>Redundant by priority.</td></tr><tr><td>cost</td><td>Redundant by cost.</td></tr></table></td></tr>
<tr><td>algorithm</td><td>LLB algorithm.</td><td>option</td><td>-</td><td>redundant</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>redundant</td><td>Redundant as algorithm.</td></tr><tr><td>WRR</td><td>WRR as algorithm.</td></tr></table></td></tr>
<tr><td>FEC</td><td>Forward equivalence class.</td><td>option</td><td>-</td><td>source_ip</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>source_ip</td><td>Forward equivalence class by source IP.</td></tr><tr><td>dest_ip</td><td>Forward equivalence class by destination IP.</td></tr><tr><td>source_dest_ip_pair</td><td>Forward equivalence class by source and destination IP pair.</td></tr><tr><td>connection</td><td>Forward equivalence class by connection.</td></tr></table></td></tr>
<tr><td>session-timeout</td><td>FEC session timeout in seconds.</td><td>integer</td><td>0 - 86400</td><td>60</td></tr>
<tr><td>grace-period</td><td>Grace period measured in seconds before failback.</td><td>integer</td><td>0 - 10000000</td><td>0</td></tr>
<tr><td>members</td><td>Link members of virtual WAN.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td>rid</td><td>CAPWAP virtual interface ID.</td><td>integer</td><td>1, 2</td><td>1</td></tr>
<tr><td>vid</td><td>VLAN ID.</td><td>integer</td><td>1 - 4089</td><td>0</td></tr>
<tr><td>ingress-intf</td><td>CAPWAP or VLAN interface's parent interface.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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>port4</td><td>Port 4 as the ingress interface.</td></tr></table></td></tr>
<tr><td>Sfp-dsl</td><td>sfp-dsl status</td><td>option</td><td>-</td><td>disable</td></tr>
</table>

Parameter	Description	Type	Size	Default
	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
	Option	Description		
	Vdsl			
	Adsl			

- config VRRP on page 51

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:

```
config system interface
    edit lan
        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 system vxlan

Description: Configure VXLAN devices

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

Sample command:

```
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 system aggregate-interface

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

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

Sample command:

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

- config members on page 54

config members

Description: Configure interfaces to be aggregated.

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

```
show
abort
end
delete <name>
purge
show
end
```

Sample command:

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>mode</td><td>Aggregate interface mode.</td><td>option</td><td>-</td><td>activebackup</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>activebackup</td><td>Active backup.</td></tr><tr><td>loadbalance</td><td>Load balance.</td></tr></table></td></tr>
<tr><td>mapping-timeout</td><td>source-mac-to-member mapping timeout in seconds.</td><td>integer</td><td>0 - 86400</td><td>60</td></tr>
<tr><td>interface</td><td>Member interface.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td>weight</td><td>Member weight in load balancing.</td><td>integer</td><td>1 - 256</td><td>1</td></tr>
<tr><td>health-check-event</td><td>Member monitor.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td>health-check-fail-cnt</td><td>Number of failures before the member is considered dead.</td><td>integer</td><td>1 - 10</td><td>5</td></tr>
</table>

Parameter	Description	Type	Size	Default
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
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>status</td><td>Bring the PPPoE up or down</td><td>option</td><td>-</td><td>up</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>up</td><td>Set interface status up.</td></tr><tr><td>down</td><td>Set interface status down.</td></tr></table></td></tr>
<tr><td>device</td><td>Name of the physical interface</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td>username</td><td>The ISP provided username of the PPPoE account.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>password</td><td>The PPPoE account's password.</td><td>string</td><td>-</td><td>none</td></tr>
</table>

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:

```
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
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>status</td><td>Status of the DHCP configuration.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Decripton</th></tr>
<tr><td>enable</td><td>Enable the DHCP server.</td></tr>
<tr><td>disable</td><td>Disable the DHCP server.</td></tr>
</table></td></tr>
<tr><td>lease-time</td><td>Lease time in seconds. 0 means unlimited.</td><td>integer</td><td>300 - 8640000</td><td>86400</td></tr>
<tr><td>dns-service</td><td>Options for assigning DNS servers to DHCP clients.</td><td>Option</td><td>-</td><td>default</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>default</td><td>Use the default DNS server.</td></tr>
<tr><td>specify</td><td>Specify the DNS server to be used.</td></tr>
<tr><td>wan-dns</td><td>Use the WAN port DNS server.</td></tr>
</table></td></tr>
<tr><td>dns-server1</td><td>DNS server 1.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>dns-server2</td><td>DNS server 2.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>dns-server3</td><td>DNS server 3.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>ntp-service</td><td>Options for assigning Network Time Protocol (NTP) servers to DHCP clients.</td><td>option</td><td>-</td><td>specify</td></tr>
</table>

Parameter	Description	Type	Size	Default
ntp-server1	NTP server 1.	string	-	none
ntp-server2	NTP server 2.	string	-	none
ntp-server3	NTP server 3.	string	-	none
default-gateway	Default gateway IP address assigned by the DHCP server.	IPv4 address	-	none
netmask	Network mask assigned by the DHCP server.	string	-	none
interface	DHCP server can assign IP configurations to clients connected to this interface.	option	-	none
	Option	**Description**		
	lan	LAN as the DHCP server interface.		
	lo	Loopback as the DHCP server interface.		
	port1	Port 1 as the DHCP server interface.		
	port4	Port 4 as the DHCP server interface.		
start-ip	The first IP address in the IP range.	IPv4 address	-	none
end-ip	The last IP address in the IP range.	IPv4 address	-	none
mtu	Client's MTU.	integer	512 - 9000	1500
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:

```
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
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>status</td><td>Status of the DHCP relay configuration.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable DHCP relay.</td></tr>
<tr><td>disable</td><td>Disable DHCP relay</td></tr>
</table></td></tr>
<tr><td>client-interfaces</td><td>The interfaces connected to DHCP clients.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>lan</td><td>LAN as client interfaces.</td></tr>
<tr><td>lo</td><td>Loopback as client interfaces.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>port1</td><td>Port 1 as client interfaces.</td></tr><tr><td>port4</td><td>Port 4 as client interfaces.</td></tr></table></td></tr>
<tr><td>server-interface</td><td>The interface used to reach out to the DHCP server.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>lan</td><td>LAN as client interfaces.</td></tr><tr><td>lo</td><td>Loopback as client interfaces.</td></tr><tr><td>port1</td><td>Port1 as client interfaces.</td></tr><tr><td>port4</td><td>Port 4 as client interfaces.</td></tr></table></td></tr>
<tr><td>server-ip</td><td>IP address of the DHCP server.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
</table>

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:

```
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
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	**Descrption**		
	least-rtt	least-rtt as server-select-method.		
	failover	failover as server-select-method.		

config system dns-server

Description: Configure DNS servers.

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>Name</td><td>Name of the DNS server.</td><td>string</td><td>1 - 35 characters in length</td><td>none</td></tr>
<tr><td>interface</td><td>A system interface enabled for DNS service.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td>mode</td><td>DNS server mode.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>recursive</td><td>Shadow the DNS database and forward.</td></tr>
<tr><td>non-recursive</td><td>Public DNS database only.</td></tr>
<tr><td>forward-only</td><td>Forward only.</td></tr>
</table></td></tr>
<tr><td>dns-filter</td><td>Enter a previously created DNS filter profile.</td><td>string</td><td>-</td><td>none</td></tr>
</table>

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
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>name</td><td>Name of the DNS database.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>status</td><td>Status of the DNS zone.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable the DNS zone.</td></tr>
<tr><td>disable</td><td>Disable the DNS zone.</td></tr>
</table></td></tr>
<tr><td>domain</td><td>Domain zone name.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>type</td><td>Zone type.</td><td>option</td><td>-</td><td>primary</td></tr>
<tr><td>view</td><td>Zone view to serve internal or public DNS clients.</td><td>option</td><td>-</td><td>shadow</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table></td></tr>
<tr><td>primary-name</td><td>Domain name of the default DNS server for the zone.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>contact</td><td>Email address of the administrator of the zone. It could be a simple username or full email address.</td><td>string</td><td>-</td><td>host</td></tr>
<tr><td>ttl</td><td>Default time-to-live value (in seconds) for the entries of the DNS zone.</td><td>integer</td><td>1 - 2147483647</td><td>86400</td></tr>
<tr><td>authoritative</td><td>Status of the authoritative zone.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable authoritative zone.</td></tr>
<tr><td>disable</td><td>Disable authoritative zone.</td></tr>
</table></td></tr>
<tr><td>forwarder</td><td>The list of DNS zone forwarder IP addresses, separate by white space.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>source-ip</td><td>Source IP for forwarding to the DNS server.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
</table>

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:

```
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

Parameter	Description	Type	Size	Default
	Option	**Description**		
	enable	Enable resource record.		
	disable	Disable resource record.		
type	Resource record type.	option	-	A
	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.port1
      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.port2
      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	Decsription	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	integer	0 - 2147483647	0

<table>
<tr><th>Parameter</th><th>Decsription</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td>indicates infinity.</td><td></td><td></td><td></td></tr>
<tr><td>out-bandwidth-threshold</td><td>Bandwidth threshold in MB for output traffic. 0 indicates infinity.</td><td>integer</td><td>0 - 2147483647</td><td>0</td></tr>
<tr><td>health-check</td><td>Link health check of the virtual-wan member.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>health-check-fail-threshold</td><td>The number of consecutive failed probes before the member is considered dead.</td><td>integer</td><td>1 – 10</td><td>5</td></tr>
<tr><td>health-check-success-threshold</td><td>The number of consecutive successful probes before the member is considered alive.</td><td>integer</td><td>1 – 10</td><td>5</td></tr>
<tr><td>link-cost-factor</td><td>Criteria by which link selection is made.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Descri[ption</th></tr>
<tr><td>latency</td><td>link-cost-factor based on latency.</td></tr>
<tr><td>jitter</td><td>link-cost-factor based on jitter.</td></tr>
<tr><td>packetloss</td><td>link-cost-factor based on packet-loss.</td></tr>
</table>
</td></tr>
<tr><td>latency-threshold</td><td>Latency in milliseconds for SLA to make decisions.</td><td>integer</td><td>0 - 10000000</td><td>5</td></tr>
</table>

Parameter	Decsription	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 syslog

Description: Configure syslog server settings.

```
config system syslog
      config remote-servers {string}
      edit <name>
         set ip* {ipv4-address}
         set port [1 - 65535]
      unset
      delete <name>
      purge
      show
      end
      config statistic-report
         set status [disable | enable]
         set interval [1 - 3600]
         config cpu-usage
            set threshold [0 - 100]
            thrset variance [0 - 100]
         end
         config memory-usage
            set threshold [0 - 100]
            set variance [0 - 100]
         end
         config cpu-temperature
            set threshold [0 - 120]
            set variance [0 - 120]
         end
      end
show
end
```

config remote-servers

Description: Configure syslog remote servers settings.

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

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

config statistic-report

Description: Configure syslog statistic report settings.

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>status</td><td>Status syslog statistic report.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable syslog statistic report.</td></tr><tr><td>disable</td><td>Disable Enable syslog statistic report.</td></tr></table></td></tr>
<tr><td>interval</td><td>The time interval (in seconds) of system status reports.</td><td>integer</td><td>1 - 3600</td><td>30</td></tr>
</table>

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 -1 00	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	integer	0 - 120	5

Parameter	Description	Type	Size	Default
	temperature report when it exceeds the threshold. 0 means report all the time.			

Sample command:

```
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 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:

```
config system api-user
    edit 1
        set comment this is a test api user
    next
end
```

Parameter	Descripton	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	Decription	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 74

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:

```
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:

```
config system settings
    set ike-port 500
end
```

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

config system switch-interface

Description: View LAN extension settings synced from the FortiGate. You cannot configure these settings directly on the FortiBranchSASE; you must make them through the FortiGate LAN extension profile first.

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

Sample syntax:

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

Parametrer	Description	Type	Size	Default
vlan-support	Enable/disable VLAN support.	option	-	
stp	Spanning Tree Protocol.	option	-	disable
	Option	**Description**		
	enable	Enable Spanning Tree Protocol.		
	disable	Disable Spanning Tree Protocol.		
ts-mode	Read-only: Split tunnel mode.	option	-	disable
	Option	**Description**		
	include	Enable Split tunnel mode		
	disable	Disable Split tunnel mode.		
wired-security-mode	Turn on 802.1x authentication for this interface.	option	-	
wired-security-group	Names of user groups that can authenticate with the 802.1X.	option	-	
dst-mac	Read-only: MAC address of the remote gateway pushed from FortiOS.	string	-	none
dst-addr	Read-only: Destination IP addresses	string	-	none
services	Read-only: Internet services.	options	-	none

config members

Parameter	Description	Type	Size	Default
config member	Interfaces within the virtual switch.	option	-	none
name	The LAN port ID.	string	-	none
type	Interface type.	option	-	
port	Interface within the virtual switch.	option	-	

Parameter	Description	Type	Size	Default
vap	Virtual Access Point, which must NOT be configured as a WLAN bridge, will be added as a member of the switch-interface.	option	-	
vids	VLAN ID list.	integer	1 to 4089	
pvid	Port VLAN ID.	integer	1 to 4089	
security-8021x-member-mode	Enable/disable 802.1x authentication on a port.	option	-	

config ssh-crypto

Description: Configure system SSH crpyto.

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

Sample command:

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

Parameter	Description	Type	Size	Default
strong-crypto	Enable/disable strong encryption for SSH	option	-	disable

Option	Description
enable	Enable strong encryption for SSH
disable	Disable strong encryption for SSH

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>set ssh-enc-algo</td><td>Set supported ciphers for ssh-enc-algo.</td><td>option</td><td>-</td><td>aes256-ctr aes256-gcm@openssh.com</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><i>aes256-ctr</i></td><td>aes256-ctr</td></tr>
<tr><td><i>aes256-gcm@openssh.com</i></td><td>aes256-gcm@openssh.com</td></tr>
</table>
</td></tr>
<tr><td>set ssh-hsk-algo</td><td>Set supported ciphers for ssh-hsk-algo.</td><td>option</td><td>-</td><td>ecdsa-sha2-nistp521 ecdsa-sha2-nistp384 ecdsa-sha2-nistp256 rsa-sha2-256 rsa-sha2-512 ssh-ed25519</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><i>ecdsa-sha2-nistp256</i></td><td>ecdsa-sha2-nistp256</td></tr>
<tr><td><i>ecdsa-sha2-nistp384</i></td><td>ecdsa-sha2-nistp384</td></tr>
<tr><td><i>ecdsa-sha2-nistp521</i></td><td>ecdsa-sha2-nistp521</td></tr>
<tr><td><i>rsa-sha2-256</i></td><td>rsa-sha2-256</td></tr>
<tr><td><i>rsa-sha2-512</i></td><td>rsa-sha2-512</td></tr>
<tr><td><i>ssh-ed25519</i></td><td>ssh-ed25519</td></tr>
</table>
</td></tr>
<tr><td>set ssh-kex-algo</td><td>Set supported ciphers for ssh-kex-algo.</td><td>option</td><td>-</td><td>diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><i>curve25519-sha256@libssh.org</i></td><td>curve25519-sha256@libssh.org</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><em>diffie-hellman-group-exchange-sha256</em></td><td>diffie-hellman-group-exchange-sha256</td></tr>
<tr><td><em>diffie-hellman-group14-sha256</em></td><td>diffie-hellman-group14-sha256</td></tr>
<tr><td><em>diffie-hellman-group16-sha512</em></td><td>diffie-hellman-group16-sha512</td></tr>
<tr><td><em>diffie-hellman-group18-sha512</em></td><td>diffie-hellman-group18-sha512</td></tr>
</table>
</td></tr>
<tr><td>set ssh-mac-algo</td><td>Set supported ciphers for ssh-mac-algo.</td><td>option</td><td>-</td><td>hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><em>hmac-sha2-256</em></td><td>hmac-sha2-256</td></tr>
<tr><td><em>hmac-sha2-256-etm@openssh.com</em></td><td>hmac-sha2-256-etm@openssh.com</td></tr>
<tr><td><em>hmac-sha2-512</em></td><td>hmac-sha2-512</td></tr>
<tr><td><em>hmac-sha2-512-etm@openssh.com</em></td><td>hmac-sha2-512-etm@openssh.com</td></tr>
</table>
</td></tr>
</table>

config system 802-1X-settings

Description: Configure global 802.1X settings.

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

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

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

SNMP

This section shows the syntax of the following commands:

- config sysinfo on page 81
- config community on page 81
- config user on page 84
- config hosts on page 85

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
	Option	**Description**		
	enable	Enable the sysinfo configuration.		
	disable	Disable the sysinfo configuration.		
description	A brief description of the system.	string	1 - 127 characters in length	none
contact-info	Contact information.	string	1 - 127 characters in length	none
location	System location.	string	1 - 127 characters in length	none

config community

Description: Configure SNMP v1/v2 community settings.

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

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SNMP v2 queries.</td></tr><tr><td>disable</td><td>Disable SNMP v2 queries.</td></tr></table></td></tr>
<tr><td>query-v2-port</td><td>SNMP v2 query port number.</td><td>integer</td><td>1 - 65535</td><td>161</td></tr>
<tr><td>trap-v1-status</td><td>Status of SNMP v1 traps.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SNMP v1 traps.</td></tr><tr><td>disable</td><td>Disable SNMP v1 traps.</td></tr></table></td></tr>
<tr><td>trap-v1-lport</td><td>SNMP v1 trap local port.</td><td>integer</td><td>1 - 65535</td><td>162</td></tr>
<tr><td>trap-v1-rport</td><td>SNMP v1 trap remote port.</td><td>integer</td><td>1 - 65535</td><td>162</td></tr>
<tr><td>trap-v2-status</td><td>Status of SNMP v2 traps.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SNMP v2 traps.</td></tr><tr><td>disable</td><td>Disable SNMP v2 traps.</td></tr></table></td></tr>
<tr><td>trap-v2-lport</td><td>SNMP v2 trap local port.</td><td>integer</td><td>1 - 65535</td><td>162</td></tr>
<tr><td>trap-v2-rport</td><td>SNMP v2 trap remote port.</td><td>integer</td><td>1 - 65535</td><td>162</td></tr>
<tr><td>events</td><td>SNMP trap events.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>system-reboot</td><td>System reboot events.</td></tr><tr><td>data-exhausted</td><td>Data usage exhaustion events.</td></tr><tr><td>session-disconnect</td><td>Modem data session disconnect events.</td></tr><tr><td>low-signal-strength</td><td>Modem low signal strength events.</td></tr><tr><td>os-image-fallback</td><td>System OS image fallback events.</td></tr><tr><td>mode-switch</td><td>System mode switch events.</td></tr><tr><td>fgt-backup-mode-switch</td><td>System FGT VRRP backup mode switch events.</td></tr></table></td></tr>
</table>

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

Option	Description
enable	Enable the SNMP user.
disable	Disable the SNMP user.

Parameter	Description	Type	Size	Default
notify-hosts	SNMP managers to which notifications (traps) are sent.	option	-	none
trap-status	Status of the traps for the SNMP user.	option	-	disable

Option	Description
enable	Enable the traps for the SNMP user.
disable	Disable the traps for the SNMP user.

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>trap-lport</td><td>SNMPv3 trap local port.</td><td>integer</td><td>1 - 65535</td><td>162</td></tr>
<tr><td>trap-rport</td><td>SNMPv3 trap remote port.</td><td>integer</td><td>1 - 65535</td><td>162</td></tr>
<tr><td>queries</td><td>Status of SNMP queries for the user.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td>query-port</td><td>SNMPv3 query port.</td><td>integer</td><td>1 - 65535</td><td>161</td></tr>
<tr><td>events</td><td>SNMP trap events.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>system-reboot</td><td>System reboot events.</td></tr>
<tr><td>data-exhausted</td><td>Data usage is exhaustion events.</td></tr>
<tr><td>session-disconnect</td><td>Modem data session disconnect events.</td></tr>
<tr><td>low-signal-strength</td><td>Modem low signal strength events.</td></tr>
<tr><td>os-image-fallback</td><td>System OS image fall back events.</td></tr>
<tr><td>mode-switch</td><td>System mode switch events.</td></tr>
<tr><td>fgt-backup-mode-switch</td><td>System FGT VRRP backup mode switch events.</td></tr>
</table>
</td></tr>
<tr><td>Security-level</td><td>Security level for message authentication and encryption.</td><td>option</td><td>-</td><td>no-auth-no-priv</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>no-auth-no-priv</td><td>No authentication and no encryption.</td></tr>
<tr><td>auth-no-priv</td><td>Authentication and no encryption.</td></tr>
<tr><td>auth-priv</td><td>Authentication and encryption.</td></tr>
</table>
</td></tr>
</table>

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:

```
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 88
- config hchk on page 88

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:

```
config hmon
    config interface-monitoring
        edit 1
            set interval 30
            set interface port1
            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 port1
            set src-type interface
            set src-iface port1
            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.
lo	Loopback as the outgoing interface.

Parameter	Description	Type	Size	Default
	Option	**Description**		
	port1	Port 1 as the outgoing interface.		
	port4	Port 4 as the outgoing interface.		
filter	Filter types.	option	-	none
	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
	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
	Option	**Description**		
	lan	LAN as the outgoing interface.		

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>lo</td><td>Loopback as the outgoing interface.</td></tr><tr><td>port1</td><td>Port 1 as the outgoing interface.</td></tr><tr><td>port4</td><td>Port 4 as the outgoing interface.</td></tr></table></td></tr>
<tr><td>src-type</td><td>The way to set the source address for probes.</td><td>option</td><td>-</td><td>none</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>filter</td><td>Filter type.</td><td>option</td><td>-</td><td>rtt loss</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>rtt</td><td>Round trip time.</td></tr><tr><td>loss</td><td>Packet loss.</td></tr></table></td></tr>
</table>

VPN

This section shows the syntax of the following commands:

- config ipsec on page 92
- config vpn certificate on page 99

config ipsec

Description: Configure IPsec VPN settings.

- config phase1-interface on page 92
- config phase2-interface on page 96

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 port1
    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

Option	Description
1	Version 1
2	Version 2

Parameter	Description	Type	Size	Default
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

Option	Description
des-md5	
des-sha1	
des-sha256	
3des-md5	
3des-sha1	

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>3des-sha256</td><td></td></tr>
<tr><td>aes128-md5</td><td></td></tr>
<tr><td>aes128-sha1</td><td></td></tr>
<tr><td>aes128-sha256</td><td></td></tr>
<tr><td>aes256-md5</td><td></td></tr>
<tr><td>aes256-sha1</td><td></td></tr>
<tr><td>aes256-sha256</td><td></td></tr>
</table>
</td></tr>
<tr><td>dhgrp</td><td>DH group.</td><td>option</td><td>-</td><td>14, 5</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table>
</td></tr>
<tr><td>interface</td><td>The outgoing interface.</td><td>option</td><td>-</td><td>none</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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>port1</td><td>Port 1 as the outgoing interface.</td></tr></table></td></tr>
<tr><td>remote-gw</td><td>The IPv4 address of the remote gateway's external interface.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>authmethod</td><td>Authentication method.</td><td>option</td><td>-</td><td>psk</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>psk</td><td>Preshared key.</td></tr><tr><td>signature</td><td>Signature certificate.</td></tr></table></td></tr>
<tr><td>psksecret</td><td>Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>localid</td><td>Local ID.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>peerid</td><td>Peer identity.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>add-gw-route</td><td>Whether to automatically add a route to the remote gateway.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><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></table></td></tr>
<tr><td>dev-id-notification</td><td>Whether to enable device ID notification for the first IKE message.</td><td>option</td><td>-</td><td>disable</td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable device ID notification.</td></tr><tr><td>disable</td><td>Disable device ID notification.</td></tr></table></td></tr>
<tr><td>dev-id</td><td>The Device ID carried by the device ID notification.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>monitor</td><td>Specify the IPsec phase1 interface as primary.</td><td>string</td><td>-</td><td>none</td></tr>
</table>

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:

```
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
```

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>phase1name</td><td>Phase 1 name (which determines the options required for phase 2).</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>proposal</td><td>Phase 2 proposal.</td><td>option</td><td>-</td><td>aes128-sha1
aes256-sha1
3des-sha1
aes128-sha256
aes256-sha256
3des-sha256</td></tr>
<tr><td>pfs</td><td>Status of the PFS feature.</td><td>option</td><td>-</td><td>enable</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable PFS.</td></tr>
<tr><td>disable</td><td>Disable PFS.</td></tr>
</table></td></tr>
<tr><td>dhgrp</td><td>Phase 2 DH group.</td><td>option</td><td>-</td><td>14, 5</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table></td></tr>
</table>

Parameter	Description	Type	Size	Default
	Option	**Description**		
	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.		
	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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>subnet</td><td>IPv4 subnet.</td></tr><tr><td>range</td><td>IPv4 range.</td></tr><tr><td>ip</td><td>IPv4 IP.</td></tr><tr><td>name</td><td>IPv4 network address name.</td></tr></table></td></tr>
<tr><td>dst-subnet</td><td>Remote proxy ID subnet.</td><td>IPv4 address</td><td>-</td><td>0.0.0.0/0</td></tr>
<tr><td>dst-port</td><td>Quick mode source port.</td><td>integer</td><td>1 - 65535, or 0 for all</td><td>0</td></tr>
<tr><td>src-start-ip</td><td>Local proxy ID start.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>src-end-ip</td><td>Local proxy ID end.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>dst-start-ip</td><td>Remote proxy ID start.</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>dst-end-ip</td><td>Remote proxy ID end</td><td>IPv4 address</td><td>-</td><td>none</td></tr>
<tr><td>src-name</td><td>Local proxy ID name.</td><td>string</td><td>-</td><td>none</td></tr>
<tr><td>dst-name</td><td>Remote proxy ID name.</td><td>string</td><td>-</td><td>none</td></tr>
</table>

config vpn certificate

Description: Configure VPN certificates.

- config vpn certificate ca on page 99
- config vpn certificate local on page 100

config vpn certificate ca

Description: Configure CA certificates.

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

```
      end
```

Sample command:

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

config vpn certificate local

Description: Configure local keys and certificates.

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

Sample command:

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

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

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>factory</td><td>From the manufacturer.</td></tr><tr><td>user</td><td>From the user.</td></tr></table></td></tr>
<tr><td>enroll-protocol</td><td>Certificate enrollment protocol.</td><td>option</td><td>-</td><td></td></tr>
<tr><td></td><td colspan="4"><table><tr><th>Option</th><th>Description</th></tr><tr><td>None</td><td>None.</td></tr><tr><td>scep</td><td>Use SCEP.</td></tr></table></td></tr>
</table>

Network

This section shows the syntax of the following commands:

- config address on page 102
- config service-custom on page 103

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:

```
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 command:

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

<table>
<tr><th>Parameter</th><th>Size</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>protocol</td><td>Protocol type based on IANA numbers.</td><td>option</td><td>-</td><td>ip</td></tr>
<tr><td></td><td colspan="4">
<table>
<tr><th>Option</th><th>Description</th></tr>
<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>
</table>
</td></tr>
<tr><td>protocol-number</td><td>IP protocol number.</td><td>integer</td><td>0 - 254</td><td>0</td></tr>
</table>

Execute

This section shows the syntax of the following command:

- execute SSH username serverip on page 105
- execute vpn certificate local generate rsa on page 105

execute SSH username serverip

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

```
#execute ssh username serverip
```

Sample command:

```
execute ssh admin 192.168.1.115
```

execute vpn certificate local generate rsa

Description: Generate a Certificate Signing Request.

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

Sample command:

```
# execute vpn certificate local generate rsa test1 1024 cert US CA Sunnyvale Fortinet
102,203,303 test@fortinet.com null http://192.168.100.99/app/cert/scep/ fortinet
```

Field	Description	Mandatory	Type	Value Range
cert_name	Specify the certificate name.	Yes	String	
key_size	Specify the key size.	Yes	Number	1024, 1536, 2048, 4096

Field	Description	Mandatory	Type	Value Range
subject	Specify the subject(Host-IP/Domain Name/E-Mail).	Yes	String	
country name	Specify the country name.	No	String	
state	Specify the state name.	No	String	
city	Specify the city name.	No	String	
org	Specify the organization name.	No	String	
Units	Specify the unit name. If there are multiple units, use ',' as a delimiter.	No	String	
email	Specify the email address.	No	String	
subject_alter_name	Specify the subject alternative name.	No	String	
URL	Specify the URL.	Yes	String	
challenge	Specify the challenge password.	No	String	

WiFi

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

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>
```

FortiBranchSASE 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 fbs-home-2g-1
        set ssid fbs-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 fbs-home-5g-1
        set ssid fbs-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 fbs-home-2g-1
        set ssid fbs-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 fbs-home-5g-1
        set ssid fbs-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:

```
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 fbs-home-2g-1 fbs-home-2g-3 fbs-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

Configure the FortiBranchSASE to access a RADIUS server.

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

Sample command:

```
config user radius
  edit example_radius
    set server fortinet.com
    set secret ********
    set auth-type auto
    set timeout 5
    set transport-protocol udp
    set nas-ip 0.0.0.0
    set nas-identifier
    set port 1812
    set source-ip 1.1.1.4
  next
end
```

Parameter	Description	Type	Size	Default
name	Name of the RADIUS server table.	string	-	none
server	Primary RADIUS FQDN or IP address.	string	-	none
secret	Pre-shared secret key used to access the primary RADIUS server.	password	1-128	none
auth-type	Authentication protocols permitted for this RADIUS server. You can select the following options: • `auto` • `ms_chap_v2` • `ms_chap` • `chap` • `pap` If the authentication type is set to `auto`, FortiBranchSASE uses the following protocols in sequence: PAP → MSCHAP_v2 → CHAP FortiBranchSASE will only try the next protocol once it receives a RADIUS-reject message	option	-	auto
timeout	Time in seconds to retry connecting to the RADIUS server.	integer	-	5
transport-protocol	Transport protocol to be used. • `udp`	option	-	udp
nas-ip	IPv4 address used for the FortiBranchSASE to communicate with the RADIUS server. It is also used as the NAS-IP-Address and Called-Station-ID attributes.	string	-	none
nas-identifier	Optional NAS-Identifier string for RADIUS messages	string	-	none
port	Primary RADIUS server port number	integer	-	none
source-ip	Source IP address for communications to the RADIUS server.	IPv4 address	-	0.0.0.0

config user 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 FortiBranchSASE user group.
`member`	Names of users and RADIUS server tables you want to add to the user group. You can apply multiple RADIUS server tables to a user group.

config user security-exempt-list

Configure security exemption list.

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

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

config rule

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

DNS Filter

This section includes syntax for the following commands:

- config dnsfilter domain-filter on page 116
- config dnsfilter profile on page 117

config dnsfilter domain-filter

Description: Configure a set of domain filter entries.

```
config dnsfilter domain-filter
  edit <name>
    set comments <string>
    config entries
      edit <name>
        set domain <string>
        set type [simple | wildcard | regex]
        set action [block | allow]
        set status [enable | disable]
      next
    end
  next
end
```

Parametrer	Description	Type	Size	Default
comments	Comments for this set of domain filter entries	string	-	

config entries

Parameter	Description	Type	Size	Default
entries	A set of DNS filter entries.	table	-	
domain	A string for domain name, or wildcard, or regression expression.	string	-	
type	Select an entry type	option	-	

Option	Description
simple	Matches an exact string.

<table>
<tr><th>Parameter</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>wildcard</td><td>Matches using regex rules for advanced pattern matching.
<b>Note:</b> If the domain string contains the character ?, it can only be configured through the GUI.</td></tr>
<tr><td>regex</td><td>Matches patterns using wildcards (e.g., *.example.com).
<b>Note:</b> Only the * wildcard is supported.</td></tr>
</table></td></tr>
<tr><td>action</td><td>Select if you want to Block or Allow this entry.</td><td>option</td><td>-</td><td></td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>block</td><td>If the local domain filter action is set to block and an entry matches, then that DNS query is blocked or redirected.</td></tr>
<tr><td>allow</td><td>If the local domain filter action is set to allow and an entry matches, it will directly return to the client DNS resolver.</td></tr>
</table></td></tr>
<tr><td>status</td><td>Enable/Disable this domain filter entry.</td><td>option</td><td>-</td><td></td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>enable</td><td>Enable this domain filter to take effect.</td></tr>
<tr><td>disable</td><td>Disable this domain filter.</td></tr>
</table></td></tr>
</table>

config dnsfilter profile

Description: Configure the DNS filter profile.

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

<table>
<tr><th>Parametrer</th><th>Description</th><th>Type</th><th>Size</th><th>Default</th></tr>
<tr><td>block-action</td><td>Action to take for blocked domains.</td><td>option</td><td>-</td><td></td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>block</td><td>The DNS request is blocked and a DNS response with NXDOMAIN is returned.</td></tr>
<tr><td>redirect</td><td>A DNS response containing the portal IP address is returned, redirecting blocked domains to the SDNS portal.</td></tr>
<tr><td>block-sevrfail</td><td>The DNS request is blocked, and a DNS response with SERVFAIL is returned.</td></tr>
</table></td></tr>
<tr><td>block-botnet</td><td>Enable/disable blocking botnet C&C DNS lookups.</td><td>option</td><td></td><td>disabled</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>disable</td><td>Disable blocking botnet C&C DNS lookups.</td></tr>
<tr><td>enable</td><td>Enable blocking botnet C&C DNS lookups.</td></tr>
</table></td></tr>
<tr><td>safe-search</td><td>Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.</td><td>option</td><td></td><td>disabled</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>disable</td><td>Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.</td></tr>
<tr><td>enable</td><td>Enable to avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines.</td></tr>
</table></td></tr>
<tr><td>youtube-restrict</td><td>When <code>safe-search</code> is enabled, you can set safe search for YouTube restriction level.</td><td>option</td><td></td><td>disabled</td></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>strict</td><td>Enable strict safe search for YouTube.
This restricts YouTube access by responding to DNS resolutions with CNAME restrict.youtube.com.</td></tr>
<tr><td>moderate</td><td>Enable moderate safe search for YouTube.
This restricts YouTube access by responding to DNS resolutions with CNAME restrictmoderate.youtube.com.</td></tr>
</table></td></tr>
<tr><td>redirect-portal</td><td>Enter the IP address of the SDNS redirect portal</td><td>ip-address</td><td></td><td>0.0.0.0</td></tr>
</table>

config domain filter

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

FORTINET®

www.fortinet.com

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.