FortiSwitchOS

CLI Reference

Version 3.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, February 25, 2015

FortiSwitchOS-3.0 CLI Reference

TABLE OF CONTENTS

Change Log

Date	Change Description
Oct 24, 2014	Initial release.
Feb 25, 2015	Convert to latest Fortinet document template. Removed trunk fields that are no longer supported (max-miss-heartbeats, port-extension). Removed "execute upload image" command, as this is not supported.

Introduction

This manual describes the command line interface (CLI) commands for FortiSwitchOS

FortiSwitch models

This guide is applicable to all FortiSwitch models that are supported by FortiSwitchOS. This includes: FS-108D-POE, FS-224D-POE, FS-1024D, FS-1048D, and FS-3032D.

Model FS-124D and FortiSwitch Rugged model FSR-112D-POE are supported in release 3.0.1. See the Release Notes for information about build numbers for these models.

How this guide is organized

The chapters in this document describe the commands available for each of the top-level CLI commands:

- the following chapters describe the configuration commands:
  - "log" on page 13 - set the logging type, the logging severity level and the logging location.
  - "router" on page 19 - configure static routes and access lists.
  - "switch" on page 25 - configure Layer 2 interfaces, VLANs, trunks, STP.
  - "system" on page 33 - global parameters, system interfaces, NTP, and SNMP.
  - "user" on page 77 - create users and user groups and control authentication.
- "execute" on page 89 - commands that perform immediate operations.
- "get" on page 135 - commands that provide information about FortiSwitch operation.

Typographical conventions

This document uses the following typographical conventions:

Convention	Example

CLI input	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system setting`
	`comments  : (No default)`
	`opmode  : nat`

Convention	Example
Emphasis	HTTP connections are **not** secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
Hyperlink	Visit the Fortinet Technical Support web site: https://support.fortinet.com
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Publication	For details, see the FortiOS Handbook.

CLI command syntax conventions

This guide uses the following conventions to describe the syntax to use when entering commands in the Command Line Interface (CLI).

Convention	Description
Angle brackets `< >`	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`.
Data types include:	
`<xxx_name>`	A name referring to another part of the configuration, such as `policy_A`.
`<xxx_index>`	An index number referring to another part of the configuration, such as `0` for the first static route.
`<xxx_pattern>`	A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`.
`<xxx_fqdn>`	A fully qualified domain name (FQDN), such as `mail.example.com`.

Convention	Description
<xxx_email>	An email address, such as admin@mail.example.com. <xxx_url>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as http://www.fortinet./com/.
<xxx_ipv4>	An IPv4 address, such as 192.168.1.99.
<xxx_v4mask>	A dotted decimal IPv4 netmask, such as 255.255.255.0.
<xxx_ipv4mask>	A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.
<xxx_ipv4/mask>	A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as 192.168.1.99/24.
<xxx_ipv6>	A colon(:)-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234.
<xxx_v6mask>	An IPv6 netmask, such as /96. <xxx_ipv6mask>: An IPv6 address and netmask separated by a space.
<xxx_str>	A string of characters that is **not** another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.
<xxx_int>	An integer number that is **not** another data type, such as 15 for the number of minutes.
Square brackets [ ]	A non-required word or series of words. For example: [verbose {1 | 2 | 3}] indicates that you may either omit or type both the verbose word and its accompanying option, such as: verbose 3
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
Options delimited by vertical bars |	Mutually exclusive options. For example: {enable | disable} indicates that you must enter either enable or disable, but must not enter both.

Convention	Description
Options delimited by spaces	Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: `ping https ssh` Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type: `ping https snmp ssh` If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Entering configuration data

The switch configuration is stored as a series of configuration settings in the FortiSwitchOS configuration database. To change the configuration you can use the CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

Entering text strings (names)

Text strings are used to name entities in the configuration, such as an administrative user name. You can enter any character in a text string with the following exceptions (to prevent cross-site scripting vulnerabilities):

" (double quote), & (ampersand), ' (single quote), < (less than) and < (greater than)

You can determine the limit to the number of characters that are allowed in a text string by determining how many characters the CLI allows for a given name field. From the CLI, you can also use the `tree` command to view the number of characters that are allowed. For example, firewall address names can contain up to 64 characters. From the CLI you can do the following to confirm that the firewall address name field allows 64 characters.

```
config firewall address
   tree
         -- [address] --*name (64)
         |- subnet
         |- type
         |- start-ip
         |- end-ip
         |- fqdn (256)
         |- cache-ttl (0,86400)
         |- wildcard
         |- comment (64 xss)
         |- associated-interface (16)
         +- color (0,32)
```

Note that the tree command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (`fqdn`) field can contain up to 256 characters.

Entering numeric values

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or as in the case of MAC or IPv6 addresses separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again such as MAC addresses) require hexadecimal numbers.

CLI help includes information about allowed numeric value ranges.The CLI prevents you from entering invalid numbers.

log

Use the log commands to set the logging type, the logging severity level and the logging location for the system.

custom-field

Use the following command to customize the log fields with a name and/or value. The custom name and/or value will appear in the log message.

Syntax

```
config log custom-field
   edit <id>
   set name <name>
   set value <int>
end
```

Variable	Description	Default
<id >	Enter the identification string for the custom log .	No default
name <name>	Enter a name to identify the log. You can use letters, numbers, (‘_‘), but no special characters such as the number symbol (#). The name cannot exceed 16 characters.	No default
value <int>	Enter an integer value to associate with the log.	No default

Example

This example shows how to configure a customized field for a log.

```
config log custom-field
   edit 1
      set name "Vlan"
      set value 3
```

eventfilter

Use this command to configure event logging.

Syntax

```
config log eventfilter
   set event {enable | disable}
   set router {enable | disable}
   set system {enable | disable}
   set user {enable | disable}
end
```

Variable	Description	Default
event {enable | disable}	Log event messages. Must be enabled to make the following fields available.	enable
router {enable | disable}	Log router activity messages.	enable
system {enable | disable}	Log system activity messages.	enable
user {enable | disable}	Log user activity messages.	enable

gui

Use this command to select the device from which logs are displayed in the web-based manager.

Syntax

```
config log gui
   set logdevice {memory | disk}
end
```

Variable	Description	Default
logdevice {memory | disk}	Select the device from which logs are displayed in the web-based manager. Currently, only logging to memory is available.	memory

memory global-setting

Use this command to configure log threshold warnings, as well as the maximum buffer lines, for the FortiSwitch system memory.

The FortiSwitch system memory has a limited capacity and displays only the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the system begins to overwrite the oldest log messages. All log entries are deleted when the system restarts.

Syntax

```
config log memory global-setting
   set full-final-warning-threshold <int>
   set full-first-warning-threshold <int>
   set full-second-warning-threshold <int>
   set hourly-upload {disable | enable}
   set max-size <int>
end
```

Variable	Description	Default
full-final-warning-threshold <int>	Enter to configure the final warning before reaching the threshold. You can enter a number between 3 and 100.	95
full-first-warning-threshold <int>	Enter to configure the first warning before reaching the threshold. You can enter a number between 1 and 98.	75
full-second-warning-threshold <int>	Enter to configure the second warning before reaching the threshold. You can enter a number between 2 and 99.	90
hourly-upload {disable | enable}	Enter `enable` to have log uploads occur hourly.	disable
max-size <int>	Enter the maximum size of the memory buffer log, in bytes.	98304

{memory | syslogd | syslogd2 | syslogd3} filter

Use this command to configure log filter options. Log filters define the types of log messages sent to each log location.

Syntax

```
config log {memory | syslogd | syslogd2 | syslogd3} filter
   set severity {alert | critical | debug | emergency | error |
       information | notification | warning}
end
```

Variable	Description	Default
severity {alert | critical | debug | emergency | error | information | notification | warning}	Select the logging severity level. The system logs all messages at and above the logging severity level you select. For example, if you select `error`, the system logs `error`, `critical`, `alert` and `emergency` level messages. • `emergency` - The system is unusable. • `alert` - Immediate action is required. • `critical` - Functionality is affected. • `error` - An erroneous condition exists and functionality is probably affected. • `warning` - Functionality might be affected. • `notification` - Information about normal events. • `information` - General information about system operations. • `debug` - Information used for diagnosing or debugging the system.	information

{memory | syslogd | syslogd2 | syslogd3} setting

Use this command to configure log settings for logging to the system memory.

The system memory has a limited capacity and only displays the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the system begins to overwrite the oldest messages. All log entries are deleted when the system restarts.

Syntax

```
config log {memory | syslogd | syslogd2 | syslogd3} setting
   set diskfull {overwrite}
   set status {disable | enable}
end
```

Variable	Description	Default
diskfull {overwrite}	Enter the action to take when the memory is reaching its capacity. The only option available is `overwrite`, which means that the system will begin overwriting the oldest file. `overwrite` is only available for `memory` logging.	overwrite
status {disable | enable}	Enter `enable` to enable logging to system memory.	disable

router

Use the router commands to configure options related to routing protocols and packet forwarding:

access-list, access-list6

Use this command to add, edit, or delete access lists. Access lists are filters used by FortiSwitch routing processes. Use `access-list6` for IPv6 routing.

Each rule in an access list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and whether to match the prefix exactly or to match the prefix and any more specific prefix.

If you are setting a prefix of 128.0.0.0, use the format 128.0.0.0/1. The default route, 0.0.0.0/0 can not be exactly matched with an access-list. A prefix-list must be used for this purpose.

The system attempts to match a packet against the rules in an access list starting at the top of the list. If it finds a match for the prefix, it takes the action specified for that prefix. If no match is found, the default action is deny.

Syntax

```
config router access-list, access-list6
   edit <access_list_name>
      set comments <string>
      config rule
         edit <access_list_id>
            set action {deny | permit}
            set exact-match {enable | disable}
            set prefix { <prefix_ipv4mask> | any }
            set prefix6 { <prefix_ipv6mask> | any }
         end
      end
```

The **action** and **prefix** fields are required. The **exact-match** field is optional.

Variable	Description	Default
edit <access_list_name>	Enter a name for the access list. An access list and a prefix list cannot have the same name.	No default

Variable	Description	Default
comments <string>	Enter a descriptive comment. The max length is 127 characters.	No default
config rule variables		
edit <access_list_id>	Enter an entry number for the rule. The number must be an integer.	No default
action {deny | permit}	Set the action to take for this prefix.	permit
exact-match {enable | disable}	By default, access list rules are matched on the prefix or any more specific prefix. Enable `exact-match` to match only the configured prefix.	disable
prefix { <prefix_ipv4mask> | any }	Enter the prefix for this access list rule. Enter either: • IPv4 address and network mask • `any` — match any prefix.	No default
prefix6 { <prefix_ipv6mask> | any }	Enter the prefix for this IPv6 access list rule. Enter either: • IPv6 address and network mask • `any` — match any prefix. This variable is only used with `config access-list6`.	No default

static

Use this command to add, edit, or delete static routes for IPv4 traffic. For IPv6 traffic, use the **static6** command.

You add static routes to manually control traffic exiting the FortiSwitch. You configure routes by specifying destination IP addresses and network masks and adding gateways for these destination addresses. Gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.

You can adjust the administrative distance of a route to indicate preference when more than one route to the same destination is available. The lower the administrative distance, the greater the preferability of the route. If the routing table contains several entries that point to the same destination (the entries may have different gateways or interface associations), the system compares the administrative distances of those entries, selects the entries having the lowest distances, and installs them as routes in the FortiSwitch forwarding table. Any ties are resolved by comparing the routes' priority, with lowest priority being preferred. As a result, the forwarding table only contains routes having the lowest distances to every possible destination.

After the system selects static routes for the forwarding table based on their administrative distances, the sequence numbers of those routes determines routing priority. When two routes to the same destination exist in the forwarding table, the system selects the route having the lowest sequence number.

Syntax

```
config router static
   edit <sequence_number>
      set blackhole {enable | disable}
      set comment <comment_str>
      set device <interface_name>
      set distance <distance>
      set dst <destination-address_ipv4mask>
      set dynamic-gateway {enable | disable}
      set gateway <gateway-address_ipv4>
      set priority <integer>
      set weight <integer>
   end
```

The dst and gateway fields are required when blackhole is disabled. When blackhole is enabled, the dst field is required. All other fields are optional.

Variable	Description	Default
<sequence_number>	Enter a sequence number for the static route. The sequence number may influence routing priority in the forwarding table.	No default
blackhole {enable | disable}	Enable or disable dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route.	disable

Variable	Description	Default
comment <comment_str>	Optionally enter a descriptive comment.	No default
device <interface_name>	This field is available when `blackhole` is set to `disable`. Enter the name of the interface through which to route traffic. Use '?' to see a list of interfaces.	No default
distance <distance>	Enter the administrative distance for the route. The distance value may influence route preference in the routing table. The range is an integer from 1-255.	10
dst <destination-address_ipv4mask>	Enter the destination IPv4 address and network mask for this route. You can enter `0.0.0.0/0` to create a new static default route.	0.0.0.0/0
dynamic-gateway {enable | disable}	When enabled, dynamic-gateway hides the gateway variable for a dynamic interface, such as a DHCP or PPPoE interface. When the interface connects or disconnects, the corresponding routing entries are updated to reflect the change.	disable
gateway <gateway-address_ipv4>	This field is available when `blackhole` is set to `disable`. Enter the IPv4 address of the next-hop router to which traffic is forwarded.	0.0.0.0
priority <integer>	The administrative priority value is used to resolve ties in route selection. In the case where both routes have the same priority, such as equal cost multi-path (ECMP), the IP source hash for the routes will be used to determine which route is selected.The priority range is an integer from 0 to 4294967295. Lower priority routes are preferred routes.	0
weight <integer>	Enter weights for ECMP routes. More traffic is directed to routes with higher weights. This option is available when the `v4-ecmp-mode` field of the `config system settings` command is set to `weight-based`.	0

static6

Use this command to add, edit, or delete static routes for IPv6 traffic. For IPv4 static routes,use the **static** command

You add static routes to specify the destination of traffic exiting the system. You configure routes by adding destination IP addresses and network masks and adding gateways for these destination addresses. The gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.

Syntax

```
config router static6
   edit <sequence_number>
      set comment <comment_str>
      set device <interface_name>
      set distance <distance>
      set dst <destination-address_ipv6mask>
      set gateway <gateway-address_ipv6>
      set priority <integer>
end
```

The **device**, **dst**, and **gateway** fields are all required.

Variable	Description	Default
<sequence_number>	Enter a sequence number for the static route.	No default
comment <comment_str>	Optionally enter a descriptive comment.	No default
device <interface_name>	The name of the interface through which to route traffic.	No default
distance <distance>	Enter the administrative distance for the route. The distance value may influence route preference in the routing table. The range is an integer from 1-255.	10
dst <destination-address_ipv6mask>	The destination IPv6 address and netmask for this route. You can enter `::/0` to create a new static default route for IPv6 traffic.	::/0
gateway <gateway-address_ipv6>	The IPv6 address of the next-hop router to which traffic is forwarded.	::
priority <integer>	The administrative priority value is used to resolve ties in route selection. The priority range is an integer from 0 to 4294967295. Lower priority routes are preferred routes.	0

switch

Use the switch commands to configure options related to switching functionality:

global

Use this command to configure system-wide settings.

Syntax

```
config switch global
   set mac-aging-interval <seconds>
   set name <name>
end
```

Variable	Description	Default
mac-aging-interval <seconds>	Set the time period after which an unused MAC address is removed from the MAC table. Range 10 to 1,000,000 seconds. 0 disables.	0
name <name>	Enter a name for the switch.	No default

interface

Use this command to configure switch features on an interface.

Command

```
config switch interface
   edit ><interface_name>
      set allowed-vlans {vlan1 vlan2 ...}
      set edge-port {enabled | disabled}
      set native-vlan <vlan_int>
      set private-vlan {disabled | promisiscous | sub-vlan}
      set security-mode {none | 802.1x}
      set security-groups <group_name>
      set stp-state {enabled | disabled}
end
```

Variable	Description	Default
<interface_name>	Enter the name of the interface.	No default
allowed-vlans {vlan1 vlan2 ...}	Enter the names of the VLANs permitted on this interface.	No default
edge-port {enabled | disabled}	Enable if the port does not have another switch connected to it.	disabled
loop-guard	Enable or disable loop guard for this interface	disabled
native-vlan <vlan_int>	Enter the native (untagged) VLAN for this interface.	1
private-vlan {disabled | promis-iscous | sub-vlan}	Enable private VLAN functionality. **Note:** Private VLANs are not supported on the FortiSwitch-28C.	disabled
security-mode {none | 802.1X	Set the security mode.	none
security-groups <group_ name>	Set the security group name. This option is only available when `security-mode` is set to `802.1x`.	No default
stp-state {enabled | disabled}	Enable or disable Spanning Tree Protocol (STP) on this interface.	enabled

mirror

Use this command to configure port mirroring.

Syntax

```
config switch mirror
   edit <mirror name>
      set dst <interface>
      set status {active | inactive}
      set switching-packet {enable | disable}
   end
```

Variable	Description	Default
<mirror name>	Enter the mirror to be configured (or a new mirror name)	No default
dst <interface>	Enter the port that will act as a mirror.	No default
status {active | inactive}	Set mirroring active or inactive.	inactive
switching-packet {enable | disable}	Enable or disable switching functionality when mirroring.	disable

physical-port

Use this command to configure a switch interface.

Syntax

```
config switch physical-port
   edit <interface>
      set description <description_str>
      set flow-control {tx | rx | both | disable}
      set max-frame-size <bytes_int>
      set poe-reset reset
      set poe-status enable
      set speed <speed_str>
      set status {down | up}
   end
```

Variable	Description	Default
<interface>	Enter the interface name.	No default
description <description_str>	Optionally enter a description.	No default
flow-control {tx | rx | both | disable}	Set flow control: `tx` — enable transmit pause only `rx` — enable receive pause only `both` — enable both transmit and receive pause `disable` — disable flow control	No default
max-frame-size <bytes_int>	Set the maximum frame size. Range 68 to 16360.	16360
poe-reset reset	Reset the Power Over Ethernet power supply. This option is only available with the FortiSwitch-324B-POE.	No default
poe-status enable	Enable Power Over Ethernet.This option is only available with the FortiSwitch-324B-POE.	No default
speed <speed_str>	Set the speed of this port. Enter `set speed ?` to list acceptable values for `<speed_str>`.	auto
status {down | up}	Set the administrative status of this interface: `up` or `down`.	up

stp instance

Use this command to configure an STP instance.

Syntax

```
config switch stp instance
   edit <instance_id>
      set set priority <priority_int>
      set set vlan-range <vlan_map>
      config stp-port
         edit <port name>
         set cost <cost_int>
         set priority <priority_int>
      end
   end
```

Variable	Description	Default
<instance_id>	Enter a number to identify the table entry.	No default
set priority <priority_int>	Set STP priority. Use `set priority ?` to list the acceptable priority values.	32768
set vlan-range <vlan_map>	Enter the VLANs to which STP applies. <vlan_map> is a comma-separated list of VLAN IDs or VLAN ID ranges, for example “1,3-4,6,7,9-100” .	No default
config stp-port fields		
<port name>	Enter the name of the port.	No default
cost <cost_int>	Enter the cost of using this interface. Use `set cost ?` for suggested cost values based on link speed.	0
priority <priority_int>	Enter the priority of this interface. Use `set priority ?` to list the acceptable priority values.	128

stp settings

Use this command to configure STP settings.

Syntax

```
config switch stp settings
   set forward-time <fseconds_int>
   set hello-time <hseconds_int>
   set max-age <age>
   set max-hops <hops_int>
   set name <name_str>
   set revision <rev_int>
   set status {enable | disable}
end
```

Variable	Description	Default
forward-time <fseconds_int>	Enter the forwarding delay in seconds. Range 4 to 30.	15
hello-time <hseconds_int>	Enter the hello time in seconds. Range 1 to 10.	2
max-age <age>	Enter the maximum age. Range 6 to 40.	20
max-hops <hops_int>	Enter the maximum number of hops. Range 1 to 40.	20
name <name_str>		No default
revision <rev_int>	Range 0 to 65535.	0
status {enable | disable}	Enable or disable status report.	enable

trunk

Use this command to configure link aggregation.

Syntax

```
config switch trunk
   edit <trunk name>
      set description <description_str>
      set lacp-speed {fast | slow}
      set members <intf1 ... intfn>
      set member-withdrawal-behaviour {block | forward}
      set mode {fortinet-trunk | lacp-active | lacp-passive | static}
      set port-selection-criteria {src-ip | dst-ip | src-dst-ip}
```

Variable	Description	Default
<trunk name>	Enter a name for the trunk.	No default
description <description_str>	Optionally, enter a description.	No default
lacp-speed {fast | slow}	Select fast (one message per second) or slow (one message every 10 seconds) LACP speed. This is available only for LACP modes.	slow
members <intf1 … intfn>	Enter the names of the interfaces that belong to this trunk. Separate names with spaces.	No default
member-withdrawal-behaviour {block | forward}	Select whether traffic is blocked or forwarded on member interfaces that are withdrawn from the trunk. This field not available when `mode` is static.	block
mode {fortinet-trunk | lacp-active | lacp-passive | static}	Select the link aggregation mode: `fortinet-trunk` — use heartbeat packets to negotiate Fortinet aggregation `lacp-active` — use active LACP 802.3ad aggregation `lacp-passive` — use passive LACP 802.3ad aggregation `static` — use static aggregation, ignoring and not sending control messages	static
port-selection-criteria {src-ip | dst-ip | src-dst-ip}	Select port selection criteria: `src-ip` — source IP address `dst-ip` — destination IP address `src-dst-ip` — both source and destination IP addresses	src-dst-ip

vlan

Use this command to configure VLANs.

Syntax

```
config switch vlan
   edit <vlan id>
      set description <description_str>
      set private-vlan {enable | disable}
```

Variable	Description	Default
<vlan id>	Enter a VLAN identifier.	No default
description <description_str>	Optionally, enter a description.	No default
private-vlan	Set to enable if this is a private VLAN.	disable

system

Use system commands to configure options related to the overall operation of the FortiSwitch.

accprofile

Use this command to add access profile groups that control administrator access to FortiSwitch features. Each FortiSwitch administrator account must include an access profile. You can create access profiles that deny access, allow read only, or allow both read and write access to FortiSwitch features.

Syntax

```
config system accprofile
   edit <profile-name>
      set admingrp {none | read | read-write}
      set loggrp {none | read | read-write}
      set netgrp {none | read | read-write}
      set routegrp {none | read | read-write}
      set sysgrp {none | read | read-write}
   end
```

Variable	Description	Default
<profile-name>	Enter the name for the profile.	No default
admingrp {none | read | read-write}	Set the access permission for admingrp.	none
loggrp {none | read | read-write}	Set the access permission for loggrp.	none
netgrp {none | read | read-write}	Set the access permission for netgrp.	none
routegrp {none | read | read-write}	Set the access permission for routegrp.	none
sysgrp {none | read | read-write}	Set the access permission for sysgrp.	none

admin

Use the default admin account or an account with system configuration read and write privileges to add new administrator accounts and control their permission levels. Each administrator account except the default admin must include an access profile. You cannot delete the default super admin account or change the access profile (super_admin). In addition, there is also an access profile that allows read-only super admin privileges, super_admin_readonly. The super_admin_readonly profile cannot be deleted or changed, similar to the super_admin profile. This read-only super-admin may be used in a situation where it is necessary to troubleshoot a customer configuration without making changes.

You can authenticate administrators using a password stored on the FortiSwitch or you can use a RADIUS server to perform authentication. When you use RADIUS authentication, you can authenticate specific administrators or you can allow any account on the RADIUS server to access the FortiSwitch as an administrator.

Syntax

```
config system admin
   edit <admin_name>
      set accprofile <profile-name>
      set allow-remove-admin-session {enable | disable}
      set comments <comments_string>
      set gui-detail-panel-location {bottom | ide | side}
      set {ip6-trusthost1 | ip6-trusthost2 | ip6-trusthost3 |
      ip6-trusthost4 | ip6-trusthost5 | ip6-trusthost6 |
      ip6-trusthost7 | ip6-trusthost8 | ip6-trusthost9 |
      ip6-trusthost10} <address_ipv6mask>
      set password <admin_password>
      set peer-auth {disable | enable}
      set peer-group <peer-grp>
      set remote-auth {enable | disable}
      set remote-group <name>
      set schedule <schedule-name>
      set ssh-public-key1 "<key-type> <key-value>"
      set ssh-public-key2 "<key-type> <key-value>"
      set ssh-public-key3 "<key-type> <key-value>"
      set {trusthost1 | trusthost2 | trusthost3 | trusthost4 |
      trusthost5 | trusthost6 | trusthost7 | trusthost8 | trusthost9
      | trusthost10} <address_ipv4mask>
      end
   end
```

Variable	Description	Default
<admin_name>	Enter the name for the admin account.	No default
accprofile <profile-name>	Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiSwitch features.	No default
allow-remove-admin-session {enable | disable}	Allow admin session to be removed by privileged admin users	disable

Variable	Description	Default
comments <comments_string>	Enter the last name, first name, email address, phone number, mobile phone number, and pager number for this administrator. Separate each attribute with a comma, and enclose the string in double-quotes. The total length of the string can be up to 128 characters. (Optional)	No default
gui-detail-panel-location {bottom | hide | side}	Choose the position of the log detail window.	bottom
{ip6-trusthost1 | ip6-trusthost2 | ip6-trusthost3 | ip6-trusthost4 | ip6-trusthost5 | ip6-trusthost6 | ip6-trusthost7 | ip6-trusthost8 | ip6-trusthost9 | ip6-trusthost10} <address_ipv6mask>	Any IPv6 address and netmask from which the administrator can connect to the FortiSwitch. If you want the administrator to be able to access the system from any address, set the trusted hosts to ::/0.	::/0
password <admin_password>	Enter the password for this administrator. It can be up to 256 characters in length.	No default
peer-auth {disable | enable}	Set to enable peer certificate authentication (for HTTPS admin access).	disable
peer-group <peer-grp>	Name of peer group defined under `config user peergrp` or user group defined under `config user group`. Used for peer certificate authentication (for HTTPS admin access).	No default
remote-auth {enable | disable}	Enable or disable authentication of this administrator using a remote RADIUS, LDAP, or TACACS+ server.	disable
remote-group <name>	Enter the administrator user group name, if you are using RADIUS, LDAP, or TACACS+ authentication. This is only available when `remote-auth` is enabled.	No default
schedule <schedule-name>	Restrict times that an administrator can log in. Defined in `config firewall schedule`. No default indicates that the administrator can log in at any time.	No default

Variable	Description	Default
ssh-public-key1 "<key-type> <key-value>"	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. `<key type>` is `ssh-dss` for a DSA key or `ssh-rsa` for an RSA key. `<key-value>` is the public key string of the SSH client.	No default
ssh-public-key2 "<key-type> <key-value>"		No default
ssh-public-key3 "<key-type> <key-value>"		No default
{trusthost1 | trusthost2 | trusthost3 | trusthost4 | trusthost5 | trusthost6 | trusthost7 | trusthost8 | trusthost9 | trusthost10} <address_ipv4mask>	Any IPv4 address or subnet address and netmask from which the administrator can connect to the system. If you want the administrator to be able to access the system from any address, set the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0.	0.0.0.0 0.0.0.0

arp-table

Use this command to manually add ARP table entries to the FortiSwitch. ARP table entries consist of a interface name, an IP address, and a MAC address.

Syntax

```
config system arp-table
   edit <table_value>
      set interface <port>
      set ip <address_ipv4>
      set mac <mac_address>
   end
```

Variable	Description	Default
<table_value>	Enter the identification number for the table.	No default
interface <port>	Enter the interface to associate with this ARP entry	No default
ip <address_ipv4>	Enter the IP address of the ARP entry.	No default
mac <mac_address>	Enter the MAC address of the device entered in the table, in the form of xx:xx:xx:xx:xx:xx.	No default

bug-report

Use this command to configure a custom email relay for sending problem reports to Fortinet customer support.

Syntax

```
config system bug-report
   set auth {no | yes}
   set mailto <email_address>
   set password <password>
   set server <servername>
   set username <name>
   set username-smtp <account_name>
end
```

Variable	Description	Default
auth {no | yes}	Enter `yes` if the SMTP server requires authentication or `no` if it does not.	no
mailto <email_address>	The email address for bug reports. The default is `bug_report@fortinetvirussubmit.com`.	See description
password <password>	If the SMTP server requires authentication, enter the required password.	No default
server <servername>	The SMTP server to use for sending bug report email. The default server is `fortinetvirussubmit.com`	See description
username <name>	A valid user name on the specified SMTP server. The default user name is `bug_report`.	See description
username-smtp <account_name>	A valid user name on the specified SMTP server. The default user name is `bug_report`.	See description

console

Use this command to set the console command mode, the number of lines displayed by the console, and the baud rate.

Syntax

```
config system console
   set baudrate <speed>
   set mode {batch | line}
   set output {standard | more}
end
```

Variable	Description	Default
`baudrate <speed>`	Set the console port baudrate. Select one of 9600, 19200, 38400, 57600, or 115200.	9600
mode {batch | line}	Set the console mode to line or batch. Used for autotesting only.	line
output {standard | more}	Set console output to standard (no pause) or more (pause after each screen is full, resume on keypress). This setting applies to `show` or `get` commands only.	more

dns

Use this command to set the DNS server addresses. Several FortiSwitch functions, including sending email alerts and URL blocking, use DNS.

Syntax

```
config system dns
   set cache-notfound-responses {enable | disable}
   set dns-cache-limit <integer>
   set dns-cache-ttl <int>
   set domain <domain_name>
   set ip6-primary <dns_ipv6>
   set ip6-secondary <dns_ip6>
   set primary <dns_ipv4>
   set secondary <dns_ip4>
   set source-ip <ipv4_addr>
end
```

Variable	Description	Default
cache-notfound-responses {enable | disable}	Enable to cache NOTFOUND responses from the DNS server.	disable
dns-cache-limit <integer>	Set maximum number of entries in the DNS cache.	5000
dns-cache-ttl <int>	Enter the duration, in seconds, that the DNS cache retains information.	1800
domain <domain_name>	Set the local domain name (optional).	No default
ip6-primary <dns_ipv6>	Enter the primary IPv6 DNS server IP address.	::
ip6-secondary <dns_ip6>	Enter the secondary IPv6 DNS server IP address.	::
primary <dns_ipv4>	Enter the primary DNS server IP address.	0.0.0.0
secondary <dns_ip4>	Enter the secondary DNS IP server address.	0.0.0.0
source-ip <ipv4_addr>	Enter the IP address for communications to DNS server.	0.0.0.0

global

Use this command to configure global settings that affect various FortiSwitch systems and configurations.

Syntax

```
config system global
   set admin-concurrent {enable | disable}
   set admin-https-pki-required {enable | disable}
   set admin-lockout-duration <time_int>
   set admin-lockout-threshold <failed_int>
   set admin-maintainer {enable | disable}
   set admin-port <port_number>
   set admin-scp {enable | disable}
   set admin-server-cert { self-s ign | <certificate> }
   set admin-sport <port_number>
   set admin-ssh-grace-time <time_int>
   set admin-ssh-port <port_number>
   set admin-ssh-v1 {enable | disable}
   set admin-telnet-port <port_number>
   set admintimeout <admin_timeout_minutes>
   set allow-subnet-overlap {enable | disable}
   set cfg-save {automatic | manual | revert}
   set csr-ca-attribute {enable | disable}
   set daily-restart {enable | disable}
   set dst {enable | disable}
   set gui-lines-per-page <gui_lines>
   set hostname <unithostname>
   set language <language>
   set ldapconntimeout <ldaptimeout_msec>
   set log-user-in-upper {enable | disable}
   set radius-port <radius_port>
   set refresh <refresh_seconds>
   set registration-notification {disable | enable}
   set remoteauthtimeout <timeout_sec>
   set send-pmtu-icmp {enable | disable}
   set service-expire-notification {disable | enable}
   set strong-crypto {enable | disable}
   set timezone <timezone_number>
   set user-server-cert <cert_name>
end
```

Variable	Description	Default
admin-concurrent {enable | disable}	Enable to enforce concurrent administrator logins. When enabled, the FortiSwitch restricts concurrent access from the same admin user name but on different IP addresses. Use `policy-auth-concurrent` for firewall authenticated users.	enable

Variable	Description	Default
admin-https-pki-required {enable | disable}	Enable to allow user to login by providing a valid certificate if PKI is enabled for HTTPS administrative access. Default setting `disable allows admin users to log in by providing a valid certificate or password.`	disable
admin-lockout-duration <time_int>	Set the administration account's lockout duration in seconds for the firewall. Repeated failed login attempts will enable the lockout. Use admin-lockout-threshold to set the number of failed attempts that will trigger the lockout.	60
admin-lockout-threshold <failed_int>	Set the threshold, or number of failed attempts, before the account is locked out for the admin-lockout-duration.	3
admin-maintainer {enable | disable}	Enabled by default.	enable
admin-port <port_number>	Enter the port to use for HTTP administrative access.	80
admin-scp {enable | disable}	Enable to allow system configuration download by the secure copy (SCP) protocol.	disable
admin-server-cert { self-sign | <certificate> }	Select the admin https server certificate to use. Choices include self-sign, and the filename of any installed certificates. Default setting is `Fortinet_Factory`, if available, otherwise `self-sign`.	See definition under Description.
admin-sport <port_number>	Enter the port to use for HTTPS administrative access.	443
admin-ssh-grace-time <time_int>	Enter the maximum time permitted between making an SSH connection to the FortiSwitch and authenticating. Range is 10 to 3600 seconds.	120
admin-ssh-port <port_number>	Enter the port to use for SSH administrative access.	22
admin-ssh-v1 {enable | disable}	Enable compatibility with SSH v1.0.	disable
admin-telnet-port <port_number>	Enter the port to use for telnet administrative access.	23
admintimeout <admin_timeout_minutes>	Set the number of minutes before an idle administrator times out. This controls the amount of inactive time before the administrator must log in again. The maximum `admin-timeout` interval is 480 minutes (8 hours). To improve security keep the idle timeout at the default value of 5 minutes.	5

Variable	Description	Default
allow-subnet-overlap {enable | disable}	Enable limited support for interface and VLAN subinterface IP address overlap for this VDOM. Use this command to enable limited support for overlapping IP addresses in an existing network configuration. **Caution: for advanced users only**. Use this only for existing network configurations that cannot be changed to eliminate IP address overlapping.	disable
cfg-save {automatic | manual | revert}	Set the method for saving the FortiSwitch system configuration and enter into runtime-only configuration mode. Methods for saving the configuration are: `automatic` automatically save the configuration after every change. `manual` manually save the configuration using the "execute" on page 89 command. `revert` manually save the current configuration and then revert to that saved configuration after `cfg-revert-timeout` expires. Switching to automatic mode disconnects your session. This command is used as part of the runtime-only configuration mode.	automatic
csr-ca-attribute {enable | disable}	Enable to use the CA attribute in your certificate. Some CA servers reject CSRs that have the CA attribute.	enable
daily-restart {enable | disable}	Enable to restart the FortiSwitch every day. The time of the restart is controlled by `restart-time`.	disable
dst {enable | disable}	Enable or disable daylight saving time. If you enable daylight saving time, the FortiSwitch adjusts the system time when the time zone changes to daylight saving time and back to standard time.	enable
gui-lines-per-page <gui_lines>	Set the number of lines displayed on table lists. Range is from 20 - 1000 lines per page.	50

Variable	Description	Default
hostname <unithostname>	Enter a name to identify this FortiSwitch. A hostname can only include letters, numbers, hyphens, and underlines. No spaces are allowed. While the hostname can be longer than 16 characters, if it is longer than 16 characters it will be truncated and end with a ‘‘~” to indicate it has been truncated. This shortened hostname will be displayed in the CLI, and other locations the hostname is used. Some models support hostnames up to 35 characters. By default the hostname of your system is its serial number which includes the model.	FortiSwitch serial number.
language <language>	Set the display language. You can set `<language>` to one of `english`, `french`, `japanese`, `korean`, `portuguese`, `spanish`, `simch` (Simplified Chinese) or `trach` (Traditional Chinese).	english
ldapconntimeout <ldap-timeout_msec>	LDAP connection timeout in msec	500
log-user-in-upper {`enable | disable`}	Log username in uppercase letters.	disable
radius-port <radius_port>	Change the default RADIUS port. The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645 you can use the CLI to change the default RADIUS port on your system.	1812
refresh <refresh_seconds>	Set the Automatic Refresh Interval, in seconds, for the System Status Monitor. Enter 0 for no automatic refresh.	0
registration-notification {disable | enable}	Enable or disable displaying the registration notification on the Web GUI if the FortiSwitch is not registered.	enable
remoteauthtimeout <timeout_sec>	The number of seconds that the FortiSwitch waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. The range is 0 to 300 seconds, 0 means no timeout. To improve security keep the remote authentication timeout at the default value of 5 seconds. However, if a RADIUS request needs to traverse multiple hops or several RADIUS requests are made, the default timeout of 5 seconds may not be long enough to receive a response.	5
revision-backup-on-logout {disable | enable}	Enable or disable backing up the latest configuration revision when the administrator logs out of the CLI or Web GUI.	enable

Variable	Description	Default
send-pmtu-icmp {enable | disable}	path maximum transmission unit (PMTU) - ICMP destination unreachable packet. Enable if you need to support PTMUD protocol on your network to reduce fragmentation of packets. Disabling this command will likely result PMTUD packets being blocked by the FortiSwitch.	disable
service-expire-notification {disable | enable}	Enable or disable displaying a notification on the Web GUI 30 days before the FortiSwitch support contract expires.	enable
strong-crypto {enable | disable}	strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption.	disable
timezone <timezone_number>	The number corresponding to your time zone from 00 to 72. Press `?` to list time zones and their numbers. Choose the time zone for the FortiSwitch from the list and enter the correct number.	00
user-server-cert <cert_name>	Select the certificate to use for https user authentication. Default setting is `Fortinet_Factory`, if available, otherwise `self-sign`.	See definition under Description.

interface

Use this command to edit the configuration of an interface.

Entering a name string in the **edit** command that is not the name of a physical interface adds a VLAN subinterface.

Syntax

```
config system interface
edit <interface name>
   set allowaccess <access_types>
   set alias <name_string>
   set arpforward {enable | disable}
   set bfd {enable | d isable | global}
   set bfd-desired-min-tx <interval_msec>
   set bfd-detect-mult <multiplier>
   set bfd-required-min-rx <interval_msec>
   set broadcast-forward {enable | disable}
   set defaultgw {enable | disable}
   set description <text>
   set dhcp-client-identifier <client_name_str>
   set dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}
   set dhcp-relay-service {enable | disable}
   set dhcp-relay-type {ipsec | regular}
   set disc-retry-timeout <pppoe_retry_seconds>
   set distance <admin_distance>
   set dns-server-override {enable | disable}
   set elbc-default-gw <ipv4_addr>
   set explicit-ftp-proxy {enable | disable}
   set explicit-web-proxy {enable | disable}
   set external {enable | disable)
   set fail-detect {enable | disable}
   set fail-detect-option {link-down | detectserver}
   set fail-alert-method {link-d own | link-failed-signal}
   set fail-alert-interfaces {port1 port2 ...}
   set forward-domain <collision_group_number>
   set fp-anomaly [...]
   set gi-gk {enable | disable}
   set icmp-redirect {enable | disable}
   set ident-accept {enable | disable}
   set idle-timeout <pppoe_timeout_seconds>
   set inbandwidth <bandwidth_integer>
   set interface <port_name>
   set ip <interface_ipv4mask>
   set ipmac {enable | disable}
   set ips-sniffer-mode {enable | disable}
   set ipunnumbered <unnumbered_ipv4>
   set l2forward {enable | disable}
   set l2tp-client {enable | disable}
   set lacp-ha-slave {enable | disable}
   set lacp-mode {active | passive | static}
```

```
set lacp-speed {fast | slow
set lcp-echo-interval <lcp_interval_seconds>
set lcp-max-echo-fails <missed_echoes>
set log {enable | disable}
set macaddr <mac_address>
set mediatype {serdes-sfp | sgmii-sfp}
set member <if_name1> <if_name2> ...
set mode <interface_mode>
set mtu <mtu_bytes>
set mtu-override {enable | disable}
set netbios-forward {disable | enable}
set nontp-web-proxy {disable | enable}
set outbandwidth <bandwidth_integer>
set padt-retry-timeout <padt_retry_seconds>
set password <pppoe_password>
set poe {disable | enable}
set polling-interval <interval_int>
set pppoe-unnumbered-negotiate {disable | enable}
set pptp-client {disable | enable}
set pptp-user <pptp_username>
set pptp-password <pptp_userpassword>
set pptp-server-ip <pptp_serverid>
set pptp-auth-type <pptp_authtype>
set pptp-timeout <pptp_idletimeout>
set priority <learned_priority>
set remote-ip <ipv4>
set sample-direction {both | rx | tx}
set sample-rate <rate_int>
set secondary-IP {enable | disable}
set sflow-sampler {disable | enable}
set speed <interface_speed>
set spillover-threshold <threshold_int>
set status {down | up}
set stpforward {enable | disable}
set subst {enable | disable}
set substitute-dst-mac <destination_mac_addres>
set tcp-mss <max_send_bytes>
set type {aggregate | hard-s witch | l oopback | physical
| r edundant | v dom-link | vlan}
set username <pppoe_username>
set vlanforward {enable | disable}
set vlanid <id_number>
set vrrp-virtual-mac {enable | disable}
set wccp {enable | disable}
set weight <int>
set wins-ip <wins_server_ip>

config ipv6
   set autoconf {enable | disable}
   set ip6-address <if_ipv6mask>
   set ip6-allowaccess <access_types>
   set ip6-default-life <ipv6_life_seconds>
   set ip6-hop-limit <ipv6_hops_limit>
   set ip6-link-mtu <ipv6_mtu>
   set ip6-manage-flag {disable | enable}
   set ip6-max-interval <adverts_max_seconds>
   set ip6-min-interval <adverts_min_seconds>
```

```
      set ip6-other-flag {disable | enable}
      set ip6-reachable-time <reachable_msecs>
      set ip6-retrans-time <retrans_msecs>
      set ip6-send-adv {enable | disable}
      config ip6-prefix-list
         edit <ipv6_prefix>
            set autonomous-flag {enable | disable}
            set onlink-flag {enable | disable}
            set preferred-life-time <seconds>
            set valid-life-time <seconds>
         end
      end
      config ip6-extra-address
         edit <prefix_ipv6>
      end
   end
config l2tp-client-settings
   set auth-type {auto | chap | mschapv1 | mschapv2 | pap}
   set defaultgw {enable | disable}
   set distance <admin_distance>
   set mtu <integer>
   set password <password>
   set peer-host <ipv4_addr>
   set peer-mask <netmask>
   set peer-port <port_num>
   set priority <integer>
   set user <string>
end
config secondaryip
   edit <secondary_ip_id>
      set allowaccess <access_types>
      set ip <interface_ipv4mask>
   end
end
config vrrp
   edit <VRID_int>
      set adv-interval <seconds_int>
      set preempt {enable | disable}
      set priority <prio_int>
      set start-time <seconds_int>
      set status {enable | disable}
      set vrdst <ipv4_addr>
      set vrip <ipv4_addr>
   end
```

A VLAN cannot have the same name as a zone or a virtual domain.

Variable	Description	Default
allowaccess <access_types>	Enter the types of management access permitted on this interface or secondary IP address. Valid types are: `http https ping snmp ssh telnet`. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	Varies for each interface.
alias <name_string>	Enter an alias name for the interface. Once configured, the alias will be displayed with the interface name to make it easier to distinguish. The alias can be a maximum of 25 characters. This option is only available when interface type is `physical`.	No default.
arpforward {enable | disable}	Enable or disable forwarding of ARP packets on this interface. ARP forwarding is required for DHCP relay and MS Windows Client browsing.	enable
bfd {enable | disable | global}	The status of Bidirectional Forwarding Detection (bfd) on this interface: `enable` — enable BFD and ignore global BFD configuration. `disable` — disable BFD on this interface. `global` — use the BFD configuration in `system settings` for the virtual domain to which this interface belongs. The BFD-related fields below are available only if `bfd` is enabled.	global
bfd-desired-min-tx <interval_msec>	Enter the minimum desired interval for the BFD transmit interval. Valid range is from 1 to 100 000 msec.This is available only if `bfd` is `enable`.	50
bfd-detect-mult <multiplier>	Select the BFD detection multiplier. This is available only if `bfd` is `enable`.	3
bfd-required-min-rx <interval_msec>	Enter the minimum required interface for the BFD receive interval. Valid range is from 1 to 100 000 msec. This is available only if `bfd` is `enable`.	50
broadcast-forward {enable | disable}	Select to enable automatic forwarding of broadcast packets. Use with caution. Enabling this option may make the system vulnerable to broadcast-based DoS attacks such as ping floods.	disable
defaultgw {enable | disable}	Enable to get the gateway IP address from the DHCP or PPPoE server. This is valid only when the mode is one of DHCP or PPPoE.	disable

Variable	Description	Default
description <text>	Optionally, enter up to 63 characters to describe this interface.	No default
dhcp-client-identifier <client_name_str>	Override the default DHCP client identifier used by this interface.The DHCP client identifier is used by DHCP to identify individual DHCP clients (in this case individual interfaces). By default the DHCP client identifier for each interface is created based on the model name and the interface MAC address. In some cases you may want to specify your own DHCP client identifier using this command. This is available if `mode` is set to `dhcp`.	No default
dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}	Set DHCP relay IP addresses. You can specify up to eight DHCP relay servers for DHCP coverage of sub-nets. Replies from all DHCP servers are forwarded back to the client. The client responds to the offer it wants to accept. Do not set `dhcp-relay-ip` to 0.0.0.0.	No default
dhcp-relay-service {enable | disable}	Enable to provide DHCP relay service on this interface. The DHCP type relayed depends on the setting of `dhcp-relay-type`. There must be no other DHCP server of the same type (regular or ipsec) configured on this interface.	disable
dhcp-relay-type {ipsec | regular}	Set `dhcp_type` to `ipsec` or `regular` depending on type of firewall traffic.	regular
disc-retry-timeout <pppoe_retry_seconds>	Set the initial PPPoE discovery timeout in seconds. This is the time to wait before retrying to start a PPPoE discovery. Set to 0 to disable this feature. This field is only available in NAT/Route mode when `mode` is set to `pppoe`.	1
distance <admin_distance>	Configure the administrative distance for routes learned through PPPoE or DHCP. Use the administrative distance to specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255. For more information, see router on page 19. This variable is only available in NAT/Route mode when `mode` is set to `dhcp` or `pppoe`.	5
dns-server-override {enable | disable}	Disable to prevent this interface from using DNS server addresses it acquires via DHCP or PPPoe. This variable is only displayed if `mode` is set to `dhcp` or `pppoe`.	enable

Variable	Description	Default
edit <interface_name>	Edit an existing interface or create a new VLAN interface.	None.
edit <ipv6_prefix>	Enter the IPv6 prefix you want to configure. For settings, see the system section of this table.	None.
edit <secondary_ip_id>	Enter an integer identifier, e.g., 1, for the secondary ip address that you want to configure.	None.
elbc-default-gw <ipv4_addr>	Use to add a default gateway to hidden front panel ports in ELBC mode. When in ELBC mode the front panel ports are placed in a secret hidden VDOM. This prevents the user from adding routes to that interface. Using the `elbc-default-gw` attribute present on front panel ports the user can add a default gateway to these interfaces.	None.
explicit-ftp-proxy {enable | disable}	Enable explicit FTP proxy on this interface.	disable
explicit-web-proxy {enable | disable}	Enable explicit Web proxy on this interface.	disable
external {enable | disable)	Enable to indicate that an interface is an external interface connected to an external network. This option is used for SIP NAT when the `config VoIP profile` SIP `contact-fixup` option is disabled.	disable
fail-detect {enable | disable}	Enable interface failure detection.	disable
fail-detect-option {`link-down | detectserver`}	Select whether the system detects interface failure by port detection (`link-down`) or ping server (`detect-server`).	link-down
fail-alert-method {link-down | link-failed-signal}	Select the signal that the system uses to signal the link failure: Link Down or Link Failed.	link-down
fail-alert-interfaces {port1 port2 ...}	Select the interfaces to which failure detection applies.	No default

Variable	Description	Default
forward-domain <collision_group_number>	Specify the collision domain to which this interface belongs. Layer 2 broadcasts are limited to the same group. By default, all interfaces are in group 0. Collision domains prevent the forwarding of ARP packets to all VLANs on an interface. Without collision domains, duplicate MAC addresses on VLANs may cause ARP packets to be duplicated. Duplicate ARP packets can cause some switches to reset. This command is only available in Transparent mode.	0
fp-anomaly […]	Enable NP2 hardware fast path anomaly checking on an interface and specify whether to drop or allow (pass) different types of anomalies.When no options are specified, anomaly checking performed by the network processor is disabled. If pass options are specified, packets may still be rejected by other anomaly checks, including policy-required IPS performed using the FortiSwitch main processing resources.Log messages are generated when packets are dropped due to options in this setting. The fp-anomaly option is available for NP2-enabled interfaces.	No options specified (disabled)
gi-gk {enable | disable}	Enable Gi Gatekeeper to enable the Gi firewall on this interface as part of the anti-overbilling configuration.	disable
icmp-redirect {enable | disable}	Disable to stop ICMP redirect from sending from this interface. ICMP redirect messages are sent by a router to notify the original sender of packets that there is a better route available.	enable
ident-accept {enable | disable}	Enable or disable passing ident packets (TCP port 113) to the firewall policy. If set to disable, the system sends a TCP reset packet in response to an ident packet.	disable
idle-timeout <pppoe_timeout_seconds>	Disconnect if the PPPoE connection is idle for the specified number of seconds. Set to zero to disable this feature. This is available when `mode` is set to `pppoe`.	0

Variable	Description	Default
inbandwidth <bandwidth_integer>	Enter the KB/sec limit for incoming traffic for this interface.Use this command to configure inbound traffic shaping for an interface. Inbound traffic shaping limits the bandwidth accepted by the interface. Limiting inbound traffic takes precedence over traffic shaping applied by firewall policies. You can set inbound traffic shaping for any FortiSwitch interface and it can be active for more than one interface at a time. Setting `<bandwidth_integer>` to 0 (the default) means unlimited bandwidth or no traffic shaping.	0
interface <port_name>	Enter the physical interface this virtual interface is linked to. This is available only when adding virtual interfaces such as VLANs and VPNs.	None.
ip <interface_ipv4mask>	Enter the interface IP address and netmask.This is not available if `mode` is set to `dhcp` or `pppoe`. You can set the IP and netmask, but it will not display.This is only available in NAT/Route mode.The IP address cannot be on the same subnet as any other interface.	Varies for each interface.
ipmac {enable | disable}	Enable or disable IP/MAC binding for the specified interface.	disable
ips-sniffer-mode {enable | disable}	Enable to configure this interface to operate as a one-armed sniffer as part of configuring a FortiSwitch to operate as an IDS appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets. Once the interface is enabled for sniffing you cannot use the interface for other traffic. You must add sniffer policies for the interface to actually sniff packets.	disable
ipunnumbered <unnumbered_ipv4>	Enable IP unnumbered mode for PPPoE. Specify the IP address to be borrowed by the interface. This IP address can be the same as the IP address of another interface or can be any IP address.This is only available when `mode` is `pppoe`.The Unnumbered IP may be used for PPPoE interfaces for which no unique local address is provided. If you have been assigned a block of IP addresses by your ISP for example, you can add any of these IP addresses to the Unnumbered IP.	No default

Variable	Description	Default
l2forward {enable | disable}	Enable to allow layer-2 forwarding for this interface. If there are layer-2 protocols such as IPX, PPTP or L2TP in use on your network, you need to configure your FortiSwitch interfaces to pass these protocols without blocking.Enabling l2forward may cause packets to repeatedly loop through the network, much like a broadcast storm. In this case either disable l2forward, or enable Spanning Tree Protocol (STP) on your network's switches and routers.	disable
l2tp-client {enable | disable}	Enable or disable this interface as a Layer 2 Tunneling Protocol (L2TP) client. Enabling makes config l2tp-client-settings visible. You may need to enable `l2forward` on this interface. The interface can not be part of an aggregate interface.	disable
lcp-echo-interval <lcp_interval_seconds>	Set the interval in seconds between PPPoE Link Control Protocol (LCP) echo requests. This is available only when `mode` is `pppoe`.	5
lcp-max-echo-fails <missed_echoes>	S et the maximum number of missed LCP echoes before the PPPoE link is disconnected. This is only available when `mode` is `pppoe`.	3
log {enable | disable}	Enable or disable traffic logging of connections to this interface. Traffic will be logged only when it is on an administrative port. All other traffic will not be logged. Enabling this setting may reduce system performance, and is normally used only for troubleshooting.	disable
macaddr <mac_address>	Override the factory set MAC address of this interface by specifying a new MAC address. Use the form xx:xx:xx:xx:xx:xx. This is only used for physical interfaces.	Factory set.
mediatype {serdes-sfp | sgmii-sfp}	Some FortiSwitch SFP interfaces can operate in SerDes (Serializer/Deserializer) or SGMII (Serial Gigabit Media Independent Interface) mode. The mode that the interface operates in depends on the type of SFP transceiver installed. Use this field to switch the interface between these two modes. Set `mediatype` to: `serdes-sfp` if you have installed a SerDes transceiver. In SerDes mode an SFP interface can only operate at 1000 Mbps. `sgmii-sfp` if you have installed an SGMII transceiver. In SGMII mode the interface can operate at 10, 100, or 1000 Mbps. This field is available for some FortiSwitch SFP interfaces.	serdes-sfp

Variable	Description	Default
mode <interface_mode>	Configure the connection mode for the interface as one of: `static` — configure a static IP address for the interface. `dhcp` — configure the interface to receive its IP address from an external DHCP server. `pppoe` — configure the interface to receive its IP address from an external PPPoE server. This is available only in NAT/Route mode.	static
mtu <mtu_bytes>	Set a custom maximum transmission unit (MTU) size in bytes. Ideally set `mtu` to the size of the smallest MTU of all the networks between this FortiSwitch and the packet destination. `<mtu_bytes>` valid ranges are: 68 to 1 500 bytes in `static` mode 576 to 1 500 bytes in `dhcp` mode 576 to 1 492 bytes in `pppoe` mode up to 9 000 bytes for NP2-accelerated interfaces If you enter an MTU that is not supported, an error message informs you of the valid range for this interface. In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces to match the new MTU. If you configure an MTU size larger than 1 500, all other network equipment on the route to the destination must also support that frame size. You can set the MTU of a physical interface and some tunnel interfaces (not IPsec). All virtual interfaces inherit the MTU of the parent physical interface. The variable `mtu` is only available when `mtu-override` is enabled.	1 500
mtu-override {enable | disable}	Select enable to use custom MTU size instead of default (1 500). This is available only for physical interfaces and some tunnel interfaces (not IPsec). If you change the MTU size, you must reboot the FortiSwitch to update the MTU values of the VLANs on this interface. Some models support MTU sizes larger than the standard 1 500 bytes.	disable
netbios-forward {disable | enable}	Enable to forward Network Basic Input/Output System (NetBIOS) broadcasts to a Windows Internet Name Service (WINS) server. Use to set the WINS server IP address. This variable is only available in NAT/Route mode.	disable
nontp-web-proxy {disable | enable}	Enable to turn on web cache support for this interface, such as accepting HTTP proxies and DNS requests. Web caching accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. This variable is only available when this interface is in NAT/Route mode.	disable

Variable	Description	Default
outbandwidth <bandwidth_integer>	Enter the KB/sec limit for outgoing (egress) traffic for this interface. Use this command to configure outbound traffic shaping for an interface. Outbound traffic shaping limits the bandwidth accepted by the interface. Limiting outbound traffic takes precedence over traffic shaping applied by firewall policies. You can set outbound traffic shaping for any FortiSwitch interface and it can be active for more than one FortiSwitch interface at a time. Setting `<bandwidth_integer>` to 0 (the default) means unlimited bandwidth or no traffic shaping.	0
padt-retry-timeout <padt_retry_seconds>	Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP. This is available in NAT/Route mode when `mode` is `pppoe`.	1
password <pppoe_password>	Enter the password to connect to the PPPoE server. This is available in NAT/Route mode when `mode` is `pppoe`.	No default
poe {disable | enable}	Enable or disable PoE (Power over Ethernet). This option is only available on models with PoE feature.	disable
polling-interval <interval_int>	Set the amount of time in seconds that the sFlow agent waits between sending collected data to the sFlow collector. The range is 1 to 255 seconds. A higher `polling-interval` means less data is sent across the network but also means that the sFlow collector's picture of the network may be out of date.	20
pppoe-unnumbered-negotiate {disable | enable}	Disable to resolve problems when mode is set to PPPoE, and ipunnumbered is set. The default configuration may not work in some regions, such as Japan. This is only available when `mode` is `pppoe` and `ipunnumbered` is set.	enable
pptp-client {disable | enable}	Enable to configure and use a point-to-point tunneling protocol (PPTP) client. You may need to enable `l2forward` on this interface. This command is not available when in HA mode. If the pptp-client is enabled on an interface, the system will not enter HA mode until that pptp-client is disabled.	disable
pptp-user <pptp_username>	Enter the name of the PPTP user.	No default
pptp-password <pptp_user-password>	Enter the password for the PPTP user.	No default

Variable	Description	Default
pptp-server-ip <pptp_serverid>	Enter the IP address for the PPTP server.	No default
pptp-auth-type <pptp_auth-type>	Enter the authentication type for the PPTP user.	No default
pptp-timeout <pptp_idle-timeout>	Enter the idle timeout in minutes. Use this timeout to shut down the PPTP user session if it is idle for this number of seconds. 0 for disabled.	No default
priority <learned_priority>	Enter the priority of routes using this interface. For more information on priority, see "static". This is only available when `mode` is `pppoe` or `dhcp`.	No default
remote-ip <ipv4>	Enter an IP address for the remote end of a tunnel interface. If you want to use dynamic routing with the tunnel, or be able to ping the tunnel interface, you must specify an address for the remote end of the tunnel in `remote-ip` and an address for this end of the tunnel in `ip`. This is only available if `type` is `tunnel`.	No default
sample-direction {both | rx | tx}	Configure the sFlow agent to sample traffic received by the interface (`rx`) or sent from the interface (`tx`) or `both`.	both
sample-rate <rate_int>	Set the sample rate for the sFlow agent added to this interface. The sample rate defines the average number of packets to wait between samples. For example, the default `sample-rate` of 2000 samples 1 of every 2000 packets. The `sample-rate` range is 10 to 99999 packets between samples. The lower the `sample-rate` the higher the number of packets sampled. Sampling more packets increases the accuracy of the sampling data but also increases the CPU and network bandwidth required to support sFlow. The default `sample-rate` of 2000 provides high enough accuracy in most cases. You can increase the `sample-rate` to reduce accuracy. You can also reduce the `sample-rate` to increase accuracy.	2000
secondary-IP {enable | disable}	Enable to add a secondary IP address to the interface. This option must be enabled before configuring a secondary IP address. When disabled, the web-based manager interface displays only the option to enable secondary IP.	diable

Variable	Description	Default
sflow-sampler {disable | enable}	Add an sFlow agent to an interface. You can also configure the sFlow agent's `sample-rate`, `polling-interval`, and `sample-direction`. You can add sFlow agents to any interface, including physical interfaces, VLAN interfaces, and aggregate interfaces. After adding the sFlow agent you can configure the sFlow For more information about sFlow see "system" on page 33.	disable
speed <interface_speed>	The interface speed: **auto** — the default speed. The interface uses auto-negotiation to determine the connection speed. Change the speed only if the interface is connected to a device that does not support auto-negotiation. **10full** — 10 Mbps, full duplex **10half** — 10 Mbps, half duplex **100full** — 100 Mbps, full duplex **100half** — 100 Mbps, half duplex **1000full** — 1000 Mbps, full duplex **1000half** — 1000 Mbps, half duplex Speed options vary for different models and interfaces. Enter a space and a "?" after the `speed` field to display a list of speeds available for your model and interface. You cannot change the speed for switch interfaces. Note: XG2 interfaces on models 3140B and 3950B cannot be configured for 1000Mbps.	auto
spillover-threshold <threshold_int>	Set the `spillover-threshold` to limit the amount of bandwidth processed by the Interface. The range is 0-2097000 KBps. Set the spillover-threshold for an interface if the ECMP route failover and load balance method, configured by the `v4-ecmp-mode` field of the `config system settings` command is set to `usage-based`. The system sends all ECMP-routed sessions to the lowest numbered interface until the bandwidth being processed by this interface reaches its spillover threshold. The system then spills additional sessions over to the next lowest numbered interface.	0
status {down | up}	Start or stop the interface. If the interface is stopped, it does not accept or send packets. If you stop a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.	`up` (`down` for VLANs)
stpforward {enable | disable}	Enable to forward Spanning Tree Protocol (STP) packets through this interface. STP maps the network to provide the least-cost-path from point to point while blocking all other ports for that path. This prevents any loops which would flood the network. If your network uses layer-2 protocols, and has looping issues STP will stop this.	disable

Variable	Description	Default
subst {enable | disable}	Enable to use a substitute destination MAC address for this address. This feature may be used with virtual interfaces to prevent network loops.	disable
substitute-dst-mac <destination_mac_addres>	Enter the substitute destination MAC address to use when `subst` is enabled. Use the xx:xx:xx:xx:xx:xx format.	No default
tcp-mss <max_send_bytes>	Enter the FortiSwitch maximum sending size for TCP packets.	No default
type {aggregate | hard-switch | loopback | physical | redundant | vlan}	Enter the type of interface. Note: Some types are read only, and are set automatically by hardware. **aggregate** — available only on some FortiSwitch models. Aggregate links use the 802.3ad standard to group up to 8 interfaces together. **hard-switch** — used when a switch-interface is configured and hardware provides switch functionality such as with the 224B model. **loopback** — a virtual interface that is always up. This interface's status and link status are not affected by external changes. It is primarily used for blackhole routing - dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route. loopback interfaces have no dhcp settings, no forwarding, no mode, or dns settings. You can create a loopback interface from the CLI or web-based manager. **physical** — for reference only. All physical interfaces and only these interfaces have `type` set to `physical` and the type cannot be changed. **redundant** — used to group 2 or more interfaces together for reliability. Only one interface is in use at any given time. If the first interface fails, traffic continues uninterrupted as it switches to the next interface in the group. This is useful in HA configurations. The order interfaces become active in the group is determined by the order you specify using the `set member` field. **vlan** — a virtual LAN interface. This is the type of interface created by default on any existing physical interface. VLANs increase the number of network interfaces beyond the physical connections on the system. VLANs cannot be configured on a switch mode interface in Transparent mode.	`vlan` for newly created interface, `physical` otherwise.

Variable	Description	Default
username <pppoe_user-name>	Enter the user name used to connect to the PPPoE server. This is only available in NAT/Route mode when `mode` is set to `pppoe`.	No default
vlanforward {enable | disable}	Enable or disable forwarding of traffic between VLANs on this interface. When disabled, all VLAN traffic will only be delivered to that VLAN only.	enable
vlanid <id_number>	Enter a VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. The VLAN ID can be any number between 1 and 4094, as 0 and 4095 are reserved, but it must match the VLAN ID added by the IEEE 802.1Q-compliant router on the other end of the connection. Two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN ID to different physical interfaces, and you can add more multiple VLANs with different VLAN IDs to the same physical interface. This is available only when editing an interface with a type of `VLAN`.	No default
vrrp-virtual-mac {enable | disable}	Enable VRRP virtual MAC addresses for the VRRP routers added to this interface. See RFC 3768 for information about the VRRP virtual MAC addresses.	disable
wccp {enable | disable}	Enable to WCCP on an interface. This setting specifies the interface the system sends and receives WCCP packets and redirected traffic.	disable
weight <int>	Set the default weight for static routes on this interface. This applies if a route has no weight configured.	0
wins-ip <wins_server_ip>	Enter the IP address of a WINS server to which to forward NetBIOS broadcasts. This WINS server address is only used if `netbios-forward` is enabled. This variable is only available in NAT/Route mode.	No default
config ipv6 variables		
autoconf {enable | disable}	Enable or disable automatic configuration of the IPv6 address. When enabled, and `ip6-send-adv` is disabled, the FortiSwitch acts as a stateless address autoconfiguration client (SLAAC).	disable
>ip6-address <if_ipv6mask>	The interface IPv6 address and netmask. The format for IPv6 addresses and netmasks is described in RFC 3513. This is available in NAT/Route mode only.	::/0

Variable	Description	Default
ip6-allowaccess <access_types>	Enter the types of management access permitted on this IPv6 interface. Valid types are: `fgfm`, `http`, `https`, `ping`, `snmp`, `ssh`, and `telnet`. Separate the types with spaces. If you want to add or remove an option from the list, retype the list as required. >	Varies for each interface.
ip6-default-life <ipv6_life_seconds>	Enter the number, in seconds, to add to the Router Lifetime field of router advertisements sent from the interface. The valid range is 0 to 9000. This is available in NAT/Route mode only.	1800
ip6-hop-limit <ipv6_hops_limit>	Enter the number to be added to the Cur Hop Limit field in the router advertisements sent out this interface. Entering 0 means no hop limit is specified. This is available in NAT/Route mode only. This is available in NAT/Route mode only.	0
ip6-link-mtu <ipv6_mtu>	Enter the MTU number to add to the router advertisements options field. Entering 0 means that no MTU options are sent. This is available in NAT/Route mode only.	0
ip6-manage-flag {disable | enable}	Enable or disable the managed address configuration flag in router advertisements. This is available in NAT/Route mode only.	disable
ip6-max-interval <adverts_max_seconds>	Enter the maximum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800. This is available in NAT/Route mode only.	600
ip6-min-interval <adverts_min_seconds>	Enter the minimum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800. This is available in NAT/Route mode only.	198
ip6-other-flag {disable | enable}	Enable or disable the other stateful configuration flag in router advertisements. This is available in NAT/Route mode only.	disable
ip6-reachable-time <reachable_msecs>	Enter the number to be added to the reachable time field in the router advertisements. The valid range is 0 to 3600. Entering 0 means no reachable time is specified. This is available in NAT/Route mode only.	0
ip6-retrans-time <retrans_msecs>	Enter the number to be added to the Retrans Timer field in the router advertisements. Entering 0 means that the Retrans Timer is not specified. This is available in NAT/Route mode only.	0

Variable	Description	Default
ip6-send-adv {enable | disable}	Enable or disable the flag indicating whether or not to send periodic router advertisements and to respond to router solicitations. When enabled, this interface's address will be added to all-routers group (`FF02::02`) and be included in an Multi Listener Discovery (MLD) report. If no interfaces on the system have `ip6-send-adv` enabled, the system will only listen to the all-hosts group (FF02::01) which is explicitly excluded from MLD reports according to RFC 2710 section 5. When disabled, and autoconf is enabled, the system acts as a stateless address auto-configuration client (SLAAC). This is available in NAT/Route mode only.	disable
edit <ipv6_prefix> variables		
autonomous-flag {enable | disable}	Set the state of the autonomous flag for the IPv6 prefix.	disable
onlink-flag {enable | disable}	Set the state of the on-link flag ("L-bit") in the IPv6 prefix.	No default
preferred-life-time <seconds>	Enter the preferred lifetime, in seconds, for this IPv6 prefix.	604800
valid-life-time <seconds>	Enter the valid lifetime, in seconds, for this IPv6 prefix.	2592000
config ip6-extra-addr	Configure a secondary address for this IPv6 interface.	No default
<prefix_ipv6>	IPv6 address prefix.	No default
config l2tp-client-settings		
auth-type {auto | chap | mschapv1 | mschapv2 | pap}	Select the type of authorization used with this client: auto — automatically choose type of authorization. chap — use Challenge-Handshake Authentication Protocol. mschapv1 — use Microsoft version of CHAP version 1. mschapv2 — use Microsoft version of CHAP version 2. pap — use Password Authentication Protocol.	`auto`
defaultgw {enable | disable}	Enable to use the default gateway.	disable
distance <admin_distance>	Enter the administration distance of learned routes.	2
mtu <integer>	Enter the Maximum Transmission Unit (MTU) for L2TP.	1460

Variable	Description	Default
password <password>	Enter the password for L2TP.	n/a
peer-host <ipv4_addr>	Enter the IP address of the L2TP host.	n/a
peer-mask <netmask>	Enter the netmask used to connect to L2TP peers connected to this interface.	255.255.255.255
peer-port <port_num>	Enter the port used to connect to L2TP peers on this interface.	1701
priority <integer>	Enter the priority of routes learned through L2TP. This will be used to resolve any ties in the routing table.	0
user <string>	Enter the L2TP user name used to connect.	n/a
variables for aggregate and redundant interfaces (some models) These variables are available only when `type` is `aggregate or redundant`		
algorithm {L2 | L3 | L4}	Enter the algorithm used to control how frames are distributed across links in an aggregated interface (also called a Link Aggregation Group (LAG)). The choice of algorithm determines what information is used to determine frame distribution. Enter one of: **L2** — use source and destination MAC addresses. **L3** — use source and destination IP addresses, fall back to L2 algorithm if IP information is not available. **L4** — use TCP, UDP or ESP header information.	L4
lacp-ha-slave {enable | disable}	This option affects how the aggregate interface participates in Link Aggregation Control Protocol (LACP) negotiation when HA is enabled for the VDOM. It takes effect only if Active-Passive HA is enabled and `lacp-mode` is not `static`. Enter `enable` to participate in LACP negotiation as a `slave` or `disable` to not participate.	enable
lacp-mode {active | passive | static}	Enter one of active, passive, or static. **active** — send LACP PDU packets to negotiate link aggregation connections. This is the default. **passive** — respond to LACP PDU packets and negotiate link aggregation connections **static** — link aggregation is configured statically	active
lacp-speed {fast | slow}	**slow** — sends LACP PDU packets every 30 seconds to negotiate link aggregation connections. This is the default. **fast** — sends LACP PDU packets every second, as recommended in the IEEE 802.3ad standard. This is available only when `type` is `aggregate`.	slow

Variable	Description	Default
member <if_name1> <if_name2> ...	Specify a list of physical interfaces that are part of an aggregate or redundant group. To modify a list, enter the complete revised list. If VDOMs are enabled, then `vdom` must be set the same for each interface before you enter the `member` list. An interface is available to be part of an aggregate or redundant group only if This is only available when `type` is `aggregate` or `redundant`.	No default
`config vrrp` fields	Add one or more VRRP virtual routers to a interface. For information about VRRP, see RFC 3768.	
<VRID_int>	VRRP virtual router ID (1 to 255). Identifies the VRRP virtual router.	None
adv-interval <seconds_int>	VRRP advertisement interval (1-255 seconds).	1
preempt {enable | disable}	Enable or disable VRRP preempt mode. In preempt mode a higher priority backup system can preempt a lower priority master system.	enable
priority <prio_int>	Priority of this virtual router (1-255). The VRRP virtual router on a network with the highest priority becomes the master.	100
start-time <seconds_int>	The startup time of this virtual router (1-255 seconds). The startup time is the maximum time that the backup system waits between receiving advertisement messages from the master system.	3
status {enable | disable}	Enable or disable this virtual router.	enable
vrdst <ipv4_addr>	Monitor the route to this destination.	0.0.0.0
vrip <ipv4_addr>	IP address of the virtual router.	0.0.0.0

ntp

Use this command to configure Network Time Protocol (NTP) servers.

Syntax

```
config system ntp
   set allow-unsync-source {enable | disable}
   set ntpsync {enable | disable}
   set source-ip <ipv4_addr>
   set syncinterval <interval_int>
   config ntpserver
      edit <serverid_int>
         set ntpv3 {enable | disable}
         set server <ipv4_addr>[/<hostname_str>]
      end
   end
```

Variable	Description	Default
allow-unsync-source	Allow or do not allow an unsychronized NTP source.	disable
ntpsync {enable | disable}	Enable to synchronize system time with the ntp server.	disable
source-ip <ipv4_addr>	Enter the source IP for communications to the NTP server.	0.0.0.0
syncinterval <interval_int>	Enter the interval in minutes between contacting NTP server to synchronize time. The range is from 1 to 1440 minutes. Only valid when `ntpsync` is enabled.	0
edit <serverid_int>	Enter the number for this NTP server	No default
ntpv3 {enable | disable}	Use NTPv3 protocol instead of NTPv4.	disable
server <ipv4_addr>[/<host-name_str>]	Enter the IPv4 address and hostname (optional) for this NTP server.	No default

password-policy

Use this command to configure higher security requirements for administrator passwords and IPsec VPN pre-shared keys.

Syntax

```
config system password-policy
   set status {enable | disable}
   set apply-to [admin-password ipsec-preshared-key]
   set change-4-characters {enable | disable}
   set expire <days>
   set minimum-length <chars>
   set min-lower-case-letter <num_int>
   set min-upper-case-letter <num_int>
   set min-non-alphanumeric <num_int>
   set min-number <num_int>
   set expire-status {enable | disable}
   set expire-day <num_int>
end
```

Variable	Description	Default
apply-to [admin-password ipsec-preshared-key]	Select where the policy applies: administrator passwords or IPSec preshared keys.	admin-password
change-4-characters {enable | disable}	Enable to require the new password to differ from the old password by at least four characters.	disable
expire <days>	Set time to expiry in days. Enter zero for no expiry.	0
minimum-length <chars>	Set the minimum length of password in characters. Range 8 to 32.	8
min-lower-case-letter <num_int>	Enter the minimum number of required lower case letters in every password.	0
min-upper-case-letter <num_int>	Enter the minimum number of required upper case letters in every password.	0
min-non-alphanumeric <num_int>	Enter the minimum number of required non-alpha-numeric characters in every password.	0
min-number <num_int>	Enter the minimum number of number characters required in every password.	0
expire-status {enable | disable}	Set to Enable to have passwords expire.	enable

Variable	Description	Default
expire-day <num_int>	Enter the number of days before the current password is expired and the user will be required to change their password. This option is available only when `expire-status` is set to enable.	90
status {enable | disable}	Enable password policy.	disable

sflow

Use this command to add or change the IP address and UDP port that FortiSwitch sFlow agents use to send sFlow datagrams to an sFlow collector.

sFlow is a network monitoring protocol described in http://www.sflow.org. FortiSwitch implements sFlow version 5. You can configure one or more FortiSwitch interfaces as sFlow agents that monitor network traffic and send sFlow datagrams containing information about traffic flow to an sFlow collector.

sFlow is normally used to provide an overall traffic flow picture of your network. You would usually operate sFlow agents on switches, routers, and firewall on your network, collect traffic data from all of them and use a collector to show traffic flows and patterns.

Syntax

```
config system sflow
   set collector-ip <collector_ipv4>
   set collector_port <port_int>
end
```

Variable	Description	Default
collector-ip <collector_ipv4>	The sFlow agents send sFlow datagrams to the sFlow collector at this IP address.	0.0.0.0
collector_port <port_int>	The UDP port number used for sending sFlow datagrams. Change this setting only if required by your sFlow collector or your network configuration.	6343

snmp community

Use this command to configure SNMP communities on your FortiSwitch. You add SNMP communities so that SNMP managers can connect to the system to view system information and receive SNMP traps. SNMP traps are triggered when system events occur.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the system for a different set of events. You can also the add IP addresses of up to 8 SNMP managers for each community.

Whey you configure an SNMP manager, ensure that you list it as a host in a community on the FortiSwitch that it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiSwitch, and will not be able to query it.

Syntax

```
config system snmp community
   edit <index_number>
      set events <events_list>
      set name <community_name>
      set query-v1-port <port_number>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_number>
      set query-v2c-status {enable | disable}
      set status {enable | disable}
      set trap-v1-lport <port_number>
      set trap-v1-rport <port_number>
      set trap-v1-status {enable | disable}
      set trap-v2c-lport <port_number>
      set trap-v2c-rport <port_number>
      set trap-v2c-status {enable | disable}
      config hosts
         edit <host_number>
            set ha-direct {enable | disable}
            set interface <if_name>
            set ip <address_ipv4>
            set source-ip <address_ipv4/mask>
         end
      config hosts6
         edit <host_number>
            set ha-direct {enable | disable}
            set interface <if_name>
            set ip6 <address_ipv6>
            set source-ip6 <address_ipv6>
         end
      end
```

Variable	Description	Default
edit <index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.	No default
events <events_list>	Enable the events for which the system should send traps to the SNMP managers in this community.	All events enabled.
name <community_name>	Enter the name of the SNMP community.	No default
query-v1-port <port_number>	Enter the SNMP v1 query port number used for SNMP manager queries.	161
query-v1-status {enable | disable}	Enable or disable SNMP v1 queries for this SNMP community.	enable
query-v2c-port <port_number>	Enter the SNMP v2c query port number used for SNMP manager queries.	161
query-v2c-status {enable | disable}	Enable or disable SNMP v2c queries for this SNMP community.	enable
status {enable | disable}	Enable or disable the SNMP community.	enable
trap-v1-lport <port_number>	Enter the SNMP v1 local port number used for sending traps to the SNMP managers.	162
trap-v1-rport <port_number>	Enter the SNMP v1 remote port number used for sending traps to the SNMP managers.	162
trap-v1-status {enable | disable}	Enable or disable SNMP v1 traps for this SNMP community.	enable
trap-v2c-lport <port_number>	Enter the SNMP v2c local port number used for sending traps to the SNMP managers.	162
trap-v2c-rport <port_number>	Enter the SNMP v2c remote port number used for sending traps to the SNMP managers.	162
trap-v2c-status {enable | disable}	Enable or disable SNMP v2c traps for this SNMP community.	enable
hosts, hosts6 variables		
edit <host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.	No Default
ha-direct {enable | disable}	Enable direct management of cluster members.	disable

Variable	Description	Default
interface <if_name>	Enter the name of the FortiSwitch interface to which the SNMP manager connects.	No Default
ip <address_ipv4>	Enter the IPv4 IP address of the SNMP manager (for `hosts`).	0.0.0.0
ip6 <address_ipv6>	Enter the IPv6 IP address of the SNMP manager (for `hosts6`).	::
source-ip <address_ipv4/mask>	Enter the source IPv4 IP address for SNMP traps sent by the FortiSwitch (for `hosts`).	0.0.0.0/ 0.0.0.0
source-ip6 <address_ipv6>	Enter the source IPv6 IP address for SNMP traps sent by the FortiSwitch (for `hosts6`).	::

snmp sysinfo

Use this command to enable the FortiSwitch SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the system to identify it. When your SNMP manager receives traps from this FortiSwitch, you will know which system sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

Syntax

```
config system snmp sysinfo
   set contact-info <info_str>
   set description <description>
   set engine-id <engine-id_str>
   set location <location>
   set status {enable | disable}
   set trap-high-cpu-threshold <percentage>
   set trap-log-full-threshold <percentage>
   set trap-low-memory-threshold <percentage>
end
```

Variable	Description	Default
contact-info <info_str>	Add the contact information for the person responsible for this FortiSwitch. The contact information can be up to 35 characters long.	No default
description <description>	Add a name or description of the system. The description can be up to 35 characters long.	No default
engine-id <engine-id_str>	Each SNMP engine maintains a value, snmpEngineID, which uniquely identifies the SNMP engine. This value is included in each message sent to or from the SNMP engine. In FortiOS, the snmpEngineID is composed of two parts: • Fortinet prefix 0x8000304404 • the optional engine-id string, 24 characters maximum, defined in this command Optionally, enter an engine-id value.	No default
location <location>	Describe the physical location of the system. The system location description can be up to 35 characters long.	No default
status {enable | disable}	Enable or disable the FortiSwitch SNMP agent.	disable
trap-high-cpu-threshold <percentage>	Enter the percentage of CPU used that will trigger the threshold SNMP trap for the high-cpu. There is some smoothing of the high CPU trap to ensure the CPU usage is constant rather than a momentary spike. This feature prevents frequent and unnecessary traps.	80

Variable	Description	Default
trap-log-full-threshold <percentage>	Enter the percentage of disk space used that will trigger the threshold SNMP trap for the log-full.	90
trap-low-memory-threshold <percentage>	Enter the percentage of memory used that will be the threshold SNMP trap for the low-memory.	80

snmp user

Use this command to configure an SNMP user including which SNMP events the user wants to be notified about, which hosts will be notified, and if queries are enabled which port to listen on for them.

FortiSwitchOS implements the user security model of RFC 3414. You can require the user to authenticate with a password and you can use encryption to protect the communication with the user.

Available events include:

cpu-high — cpu usage too high

ent-conf-change — entity config change (rfc4133)

fm-conf-change — config change (FM trap)

fm-if-change — interface IP change (FM trap)

intf-ip — interface IP address changed

log-full — available log space is low

mem-low — available memory is low

Syntax

```
config system snmp user
   edit <username>
      set auth-proto {md5 | sha}
      set auth-pwd <password>
      set events <event_string>
      set ha-direct {enable | disable}
      set notify-hosts <hosts_string>
      set notify-hosts6 <hosts_string>
      set priv-proto {aes | des}
      set priv-pwd <key>
      set queries {enable | disable}
      set query-port <port_int>
      set security-level <slevel>
   end
```

Variable	Description	Default
edit <username>	Edit or add selected user.	No default

Variable	Description	Default
auth-proto {md5 | sha}	Select authentication protocol: **md5** — use HMAC-MD5-96 authentication protocol. **sha** — use HMAC-SHA-96 authentication protocol. This is only available if `security-level` is `auth-priv` or `auth-no-priv`.	sha
auth-pwd <password>	Enter the user's password. Maximum 32 characters.This is only available if `security-level` is `auth-priv` or `auth-no-priv`.	No default
events <event_string>	Select which SNMP notifications to send. (Available events are listed above this table). Select each event that will generate a notification, and add to the string. Separate multiple events by a space. Note: On the `events` field, the `unset` command clears all options.	No default
ha-direct {enable | disable}	Enable direct management of cluster members.	disable
notify-hosts <hosts_string>	Enter IPv4 IP addresses to send SNMP notifications (SNMP traps) to when events occur. Separate multiple addresses with a space.	No default
notify-hosts6 <hosts_string>	Enter IPv6 IP addresses to send SNMP notifications (SNMP traps) to when events occur. Separate multiple addresses with a space.	No default
priv-proto {aes | des}	Select privacy (encryption) protocol: **aes** — use CFB128-AES-128 symmetric encryption. **des** — use CBC-DES symmetric encryption. This is available if `security-level` is `auth-priv`.	aes
priv-pwd <key>	Enter the privacy encryption key. Maximum 32 characters. This is available if `security-level` is `auth-priv`.	No default
queries {enable | disable}	Enable or disable SNMP v3 queries for this user. Queries are used to determine the status of SNMP variables.	`enable`
query-port <port_int>	Enter the number of the port used for SNMP v3 queries. If multiple versions of SNMP are being supported, each version should listen on a different port.	161

Variable	Description	Default
security-level <slevel>	Set security level to one of: **no-auth-no-priv** — no authentication or privacy **auth-no-priv** — authentication but no privacy **auth-priv** — authentication and privacy	no-auth-no-priv

user

The user commands provide configuration of user accounts and user groups for firewall policy authentication, administrator authentication and some types of VPN authentication

group

Use this command to add or edit user groups.

Syntax

```
config user group
   edit <groupname>
      set authtimeout <timeout>
      set group-type <grp_type>
      set http-digest-realm <attribute>
      set member <names>
      config match
         edit <match_id>
            set group-name <gname_str>
            set server-name <srvname_str>
      end
   end
```

Variable	Description	Default
edit <groupname>	Enter a new name to create a new group or enter an existing group name to edit that group.	No default
authtimeout <timeout>	Set the authentication timeout for the user group, range 1 to 480 minutes. If set to 0, the global authentication timeout value is used.	0
group-type <grp_type>	Enter the group type. `<grp_type>` determines the type of users and is one of the following: `firewall` - FortiSwitch users defined in user local, user ldap or user radius `fsso-service` - Directory Service users	firewall
http-digest-realm <attribute>	Enter the realm attribute for MD5-digest authentication	No default
member <names>	Enter the names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Separate the names with spaces. To add or remove names from the group you must re-enter the whole list with the additions or deletions required.	No default

Variable	Description	Default
config match fields	Specify the user group names on the authentication servers that are members of this FortiSwitch user group. If no matches are specified, all users on the server can authenticate.	
<match_id>	Enter an ID for the entry.	No default
group-name <gname_str>	The name of the matching group on the remote authentication server.	No default
server-name <srvname_str>	The name of the remote authentication server.	No default

ldap

Use this command to add or edit the definition of an LDAP server for user authentication.

To authenticate with the FortiSwitch, the user enters a user name and password. The system sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiSwitch. If the LDAP server cannot authenticate the user, the connection is refused by the FortiSwitch.

Syntax

```
config user ldap
edit <server_name>
   set cnid <id>
   set dn <dname>
   set group-member-check {user-attr | group-object}
   set member-attr <attr_name>
   set port <number>
   set server <domain>
   set type <auth_type>
   set username <ldap_username>
   set password <ldap_passwd>
   set password-expiry-warning {disable | enable}
   set password-renewal {disable | enable}
   set secure <auth_port>
end
```

Variable	Description	Default
edit <server_name>	Enter a name to identify the LDAP server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	No default
cnid <id>	Enter the common name identifier for the LDAP server. The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid. Maximum 20 characters.	cn
dn <dname>	Enter the distinguished name used to look up entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the Common Name Identifier. The FortiSwitch passes this distinguished name unchanged to the server. You must provide a `dn` value if `type` is `simple`. Maximum 512 characters.	No default
group-member-check {user-attr | group-object}	Select the group membership checking method: user attribute or group object.	user-attr

Variable	Description	Default
member-attr <attr_name>	An attribute of the group that is used to authenticate users.	No default
port <number>	Enter the port number for communication with the LDAP server.	389
server <domain>	Enter the LDAP server domain name or IP address.	No default
type <auth_type>	Enter the authentication type for LDAP searches. One of: `anonymous`, `regular` or `simple` See the notes below the table for additional information.	simple
username <ldap_username>	This field is available only if `type` is `regular`. For `regular` authentication, you need a user name and password. See your server administrator for more information.	No default
password <ldap_passwd>	This field is available only if `type` is `regular`. For `regular` authentication, you need a user name and password. See your server administrator for more information.	No default
password-expiry-warning {disable | enable}	Enable or disable password expiry warnings.	disable
password-renewal {disable | enable}	Enable or disable online password renewal.	disable
secure <auth_port>{disable | starttls | ldaps}	Select the port to be used in authentication: disable — port 389 ldaps— port 636 starttls — port 389	disable

Notes on Authentication Type

The authentication types for LDAP searches include:

`anonymous` — bind using anonymous user search

`regular` — bind using username/password and then search

`simple` — simple password authentication without search

You can use `simple` authentication if the user records are all under one `dn` that you know. If the users are under more than one `dn`, use the `anonymous` or `regular` type, which can search the entire LDAP database for the required user name.

If your LDAP server requires authentication to perform searches, use the `regular` type and provide values for `username` and `password`.

local

Use this command to add local user names and configure user authentication for the system. To add authentication by LDAP or RADIUS server you must first add servers using the `config user ldap` and `config user radius` commands.

Syntax

```
config user local
   edit <username>
      set ldap-server <servername>
      set passwd <password_str>
      set radius-server <servername>
      set status {enable | disable}
      set type <auth-type>
end
```

Variable	Description	Default
edit <username>	Enter the user name. Enter a new name to create a new user account or enter an existing user name to edit that account.	No default
ldap-server <servername>	Enter the name of the LDAP server with which the user must authenticate. You can only select an LDAP server that has been added to the list of LDAP servers. This is available when `type` is set to `ldap`.	No default
passwd <password_str>	Enter the password with which the user must authenticate. Passwords at least 6 characters long provide better security than shorter passwords. This is available when `type` is set to `password`.	No default
radius-server <servername>	Enter the name of the RADIUS server with which the user must authenticate. You can only select a RADIUS server that has been added to the list of RADIUS servers. This is available when `type` is set to `radius`.	No default
status {enable | disable}	Enter `enable` to allow the local user to authenticate with the FortiSwitch.	enable
type <auth-type>	Enter one of the following to specify how this user's password is verified: **ldap**: The LDAP server specified in ldap-server verifies the password. **password**: The system verifies the password against the value of the password. **radius**: The RADIUS server specified in radius-server verifies the password.	No default

radius

Use this command to add or edit the information used for RADIUS authentication.

The default port for RADIUS traffic is 1812. If your RADIUS server is using a different port you can change the default RADIUS port. You may set a different port for each of your RADIUS servers. The maximum number of remote RADIUS servers that can be configured for authentication is 10.

The RADIUS server is now provided with more information to make authentication decisions, based on values in server, use-management-vdom, use-group-for-profile, and nas-ip ,and the config user group subcommand config match . Attributes include:

NAS-IP-Address - RADIUS setting or IP address of FortiSwitch interface used to talk to RADIUS server, if not configured

NAS-Port - physical interface number of the traffic that triggered the authentication

Called-Station-ID - same value as NAS-IP Address but in text format

Fortinet-Vdom-Name - name of VDOM of the traffic that triggered the authentication

NAS-Identifier - configured hostname in non-HA mode; HA cluster group name in HA mode

Acct-Session-ID - unique ID identifying the authentication session

Connect-Info - identifies the service for which the authentication is being performed (web-auth, vpn-ipsec, vpn-pptp, vpn-l2tp, vpn-ssl, admin-login, test)

You may select an alternative authentication method for each server. These include CHAP, PAP, MS-CHAP, and MS-CHAP-v2.

Syntax

```
config user radius
   edit <server_name>
      set all-usergroup {enable | disable}
      set auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}
      set endpoint-translation {enable | disable}
      set nas-ip <use_ip>
      set radius-port <radius_port_num>
      set secret <server_password>
      set server <domain>
      set source-ip <ipv4_addr>
      set dynamic-profile {enable | disable}
      set dp-context-timeout <timeout_seconds>
      set dp-carrier-endpoint-attribute <RADIUS_attribute>
      set dp-flush-ip-session {enable | disable}
      set dp-hold-time <proxy_hold_time>
      set dp-log-dyn-flags <lflags>
      set dp-log-period <log_time>
      set dp-mem-percent <memory_percent>
      set dp-profile-attribute <RADIUS_attribute>
      set dp-profile-attribute-key <profile_attribute_key>
      set dp-radius-response {enable | disable}
      set dp-radius-server-port <RADIUS_listen_port>
      set dp-secret <server_password>
      set dp-validate-request-secret {enable | disable}
```

```
end
```

Variable	Description	Default
edit <server_name>	Enter a name to identify the RADIUS server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	No default
all-usergroup {enable | disable}	Enable to automatically include this RADIUS server in all user groups.	disable
auth-type {auto | chap | ms_ chap | ms_chap_v2 | pap}	Select the authentication method for this RADIUS server. auto uses pap, ms_chap_v2, and chap.	auto
endpoint-translation {enable | disable}	This field is available when dynamic-profile is enabled.	disable
nas-ip <use_ip>	IP address used as NAS-IP-Address and Called-Station-ID attribute in RADIUS access requests. RADIUS setting or IP address of FGT interface used to talk with RADIUS server, if not configured.	No default
radius-port <radius_port_ num>	Change the default RADIUS port for this server. The default port for RADIUS traffic is 1812. Range is 0..65535	1812
secret <server_password>	Enter the RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length.	No default
server <domain>	Enter the RADIUS server domain name or IP address.	No default
source-ip <ipv4_addr>	Enter the source IP for communications to RADIUS server.	`0.0.0.0`
Dynamic Profile fields		
dynamic-profile {enable | disable}	Enable the dynamic profile and then configure dynamic profile settings. When you enable the dynamic profile, the system accepts connections on the `dp-` radius-server-port . As well, the system attempts to dynamically assign a pro-file group to all communication sessions accepted by any firewall policy that includes a profile group. Dynamically assigning a profile group occurs only if a match is found between the carrier end point and source IP address in the communication session and a carrier end point and source IP address received in a RADIUS Start record and then only if the RADIUS Start record includes a profile group name.	disable

Variable	Description	Default
dp-carrier-endpoint-attribute <RADIUS_attribute>	To extract the carrier end point from the RADIUS Start record, this field must be set to the name of the RADIUS attribute that contains the carrier end point. You can select the RADIUS `_attribute` from the list or enter an attribute name. The RADIUS `_attribute` must match one of the RADIUS attributes in the list. The RADIUS `_attribute` is case sensitive.	Calling-Station-Id
dp-carrier-endpoint-block-attribute <RADIUS_attribute>	RADIUS attribute to hold end point to block.	Calling-Station-Id
dp-context-timeout <timeout_seconds>	The number of seconds that a user context entry can remain in the user context list without the system receiving a communication session from the carrier end point. If a user context entry is not being looked up, then the user must no longer be connected to the network. See additional notes below the table.	28800
dp-flush-ip-session {enable | disable}	Enable to flush user IP sessions on RADIUS accounting stop messages.	disable
dp-hold-time <proxy_hold_time>	If the system receives a communication session and can't find a corresponding carrier end point and IP address in the user context list, the system waits for the user context creation timeout. If a match is not found after this timeout, the FortiSwitch applies the profile group in the firewall policy to the communication session. The default user context creation timeout is 5 seconds. You might want to increase this timeout if the default profile group is being applied to users instead of the profile group that should be dynamically assigned. This could be happening if there is a delay before the FortiSwitch receives the RADIUS Start record from the accounting server. If you set this timeout to `0` the system blocks communication sessions that do not have a matching entry in the user context list.	5
dp-log-dyn-flags <lflags>	Enter one or more of the dynamic flag options to configure the system to write event log messages for dynamic profile events. You can enter multiple options. Separate the options with a space. The dynamic flag values are listed below the table.	All options except none.

Variable	Description	Default
dp-log-period <log_time>	The time in seconds to group event log messages for dynamic profile events. For example, if the log message period is 30 seconds, the system generates groups of event log messages every 30 seconds instead of generating event log messages continuously. And the log messages generated each period contain a count of how many events of that type occurred. If set to 0, the system generates all event log messages in real time.	0
dp-mem-percent <memory_percent>	Maximum percentage of system memory to use for the user context tables. CLI only. The range is 1 to 25%.	4
dp-profile-attribute <RADIUS_attribute>	To extract a profile group name from the RADIUS Start record, this field must be set to the name of the RADIUS attribute that contains the profile group name. You can select the RADIUS `_attribute` from the list or enter an attribute name. The RADIUS `_attribute` must match one of the RADIUS attributes in the list. The RADIUS `_attribute` is case sensitive.	Class
dp-profile-attribute-key <profile_attribute_key>	Enter a string if the profile attribute contains more data than just the profile group name. The profile key is a text string that always comes directly before the profile group name in the profile attribute. For example, if the profile group name always follows the text string `profile`, the class attribute could include the string: `profile=<profile_name_str>`. Where `<profile_name_str>` is the name of the profile group. Maximum 36 characters.	No default
dp-radius-response {enable | disable}	Enable if you want the FortiSwitch to send RADIUS responses after receiving RADIUS Start and Stop records. This setting may be required by your accounting system.	disable
dp-radius-server-port <RADIUS_listen_port>	If required, change the UDP port number used by the RADIUS accounting server for sending RADIUS records. the FortiSwitch listens for RADIUS Start and Stop records on this port.	1813
dp-secret <server_password>	Enter the RADIUS secret used by the RADIUS accounting server.	No default
dp-validate-request-secret {enable | disable}	Enable if you want the system to verify that the RADIUS secret matches the RADIUS secret in the RADIUS Start or End record. You can verify the RADIUS secret to verify that the RADIUS record is valid.	disable

Notes on context timeout

The number of seconds that a user context entry can remain in the user context list without the system receiving a communication session from the carrier end point. If a user context entry is not being looked up, then the user must no longer be connected to the network.

This timeout is only required if the system doesn't receive the RADIUS Stop record. However, even if the accounting system does send RADIUS Stop records this timeout should be set in case the FortiSwitch misses a Stop record.

The default user context entry timeout is 28800 seconds (8 hours). You can keep this timeout relatively high because its not usually a problem to have a long list, but entries that are no longer used should be removed regularly.

You might want to reduce this timeout if the accounting server does not send RADIUS Stop records. Also if customer IP addresses change often you might want to set this timeout lower so that out of date entries are removed from the list.

If this timeout is too low the FortiSwitch could remove user context entries for users who are still connected.

Set the timeout to 0 if you do not want the FortiSwitch to remove entries from the list except in response to RADIUS Stop messages.

Dynamic Flag values:

`none` — Disable writing event log messages for dynamic profile events.

`accounting-event` — Enable to write an event log message when the system does not find the expected information in a RADIUS Record. For example, if a RADIUS record contains more than the expected number of addresses.

`accounting-stop-missed` — Enable to write an event log message whenever a user context entry timeout expires indicating that the system removed an entry from the user context list without receiving a RADIUS Stop message.

`context-missing` — Enable to write an event log message whenever a user context creation timeout expires indicating that the system was not able to match a communication session because a matching entry was not found in the user context list.

`profile-missing` — Enable to write an event log message whenever the system cannot find a profile group name in a RADIUS start message that matches the name of a profile group added to the system.

`protocol-error` — Enable to write an event log message if RADIUS protocol errors occur. For example, if a RADIUS record contains a RADIUS secret that does not match the one added to the dynamic profile.

`radiusd-other` — Enable to write event log messages for other events. The event is described in the log message. For example, write a log message if the memory limit for the user context list is reached and the oldest entries in the table have been dropped.

setting

Use this command to change user settings such as xxxxxxx

`user settings` differ from `system global settings` in that `system global settings` fields apply to the entire FortiSwitch, where `user settings` fields apply only to the user VDOM.

Syntax

```
config user setting
   set auth-blackout-time <blackout_time_int>
   set auth-cert <cert_name>
   set auth-http-basic {disable | enable}
   set auth-invalid-max <int>
   set auth-multi-group {enable | disable}
   set auth-secure-http {enable | disable}
   set auth-type {ftp | http | https | telnet}
   set auth-timeout <auth_timeout_minutes>
   set auth-timeout-type {idle-timeout | hard-timeout | new-session}
   config auth-ports
      edit <auth-table-entry-id>
      set port <port_int>
      set type {ftp | http | https | telnet}
      end
   end
```

Variable	Description	Default
auth-blackout-time <blackout_time_int>	When a firewall authentication attempt fails 5 times within one minute the IP address that is the source of the authentication attempts is denied access for the `<blackout_time_int>` period in seconds. The range is 0 to 3600 seconds.	0
auth-cert <cert_name>	HTTPS server certificate for policy authentication. Fortinet_Factory, Fortinet_Firmware (if applicable to your FortiSwitch), and self-sign are built-in certificates but others will be listed as you add them.	self-sign
auth-http-basic {disable | enable}	Enable or disable support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of displaying an authentication web page. Some basic web browsers, for example, web browsers on mobile devices, may only support HTTP basic authentication.	disable
auth-invalid-max <int>	Enter the maximum number of failed authentication attempts to allow before the client is blocked. Range: 1-100.	5

Variable	Description	Default
auth-multi-group {enable | disable}	This option can be disabled if the Active Directory structure is setup such that users belong to only 1 group for purpose of firewall authentication. (ECO 4-4021)	enable
auth-secure-http {enable | disable}	Enable to have http user authentication redirected to secure channel - https .	disable
auth-type {ftp | http | https | telnet}	Set the user authentication protocol support for firewall policy authentication. User controls which protocols should support the authentication challenge.	No Default
auth-timeout <auth_timeout_minutes>	Set the number of minutes before the firewall user authentication timeout requires the user to authenticate again. The maximum authtimeout interval is 480 minutes (8 hours). To improve security, keep the authentication timeout at the default value of 5 minutes.	5
auth-timeout-type {idle-timeout | hard-timeout | new-session}	Set the type of authentication timeout. `idle-timeout` — applies only to idle session `hard-timeout` — applies to all sessions `new-session` — applies only to new sessions	idle-timeout
config auth-ports variables		
<auth-table-entry-id>	Create an entry in the authentication port table if you are using non-standard ports.	No Default
port <port_int>	Specify the authentication port. Range 1 to 65535.	1024
type {ftp | http | https | telnet}	Specify the protocol to which `port` applies.	http

execute

Use the execute commands perform immediate operations on the FortiSwitch.

backup

Use the backup commands to back up the FortiSwitch configuration files or logs to a TFTP or FTP server, USB disk or a management station. Management stations can either be a FortiManager unit, or FortiGuard Analysis and Management Service.

Syntax

```
execute backup config flash <comment>
execute backup config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> [<password_str>]] [<backup_password_str>]
execute backup config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup config usb <filename_str> [<backup_password_str>]
execute backup full-config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_
    int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute backup full-config usb <filename_str> [<backup_password_str>]
execute backup memory alllogs ftp <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute backup memory alllogs tftp <server_ipv4>
execute backup memory log ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> <username_
    str> <password_str> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}
```

Variable	Description
config flash <comment>	Back up the system configuration to the flash disk. Optionally, include a comment.
config ftp <filename_str> <server_ipv4 [:port_int] | server_fqdn[:port_int]> [<user-name_str> [<password_str>]] [<backup_ password_str>]	Back up the system configuration to an FTP server. Optionally, you can specify a password to protect the saved data.
config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data.
config usb <filename_str> [<backup_pass-word_str>]	Back up the system configuration to a file on a USB disk. Option-ally, you can specify a password to protect the saved data.

Variable	Description
full-config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the full system configuration to a file on an FTP server. You can optionally specify a password to protect the saved data.
full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the full system configuration to a file on a TFTP server. You can optionally specify a password to protect the saved data.
full-config usb <filename_str> [<backup_password_str>]	Back up the full system configuration to a file on a USB disk. You can optionally specify a password to protect the saved data.
memory alllogs ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]	Back up either all memory or all hard disk log files for to an FTP server. The disk option is available on FortiSwitch models that log to a hard disk.
memory alllogs tftp <server_ipv4>	Back up either all memory or all hard disk log files for this FortiSwitch to a TFTP server. he disk option is available on FortiSwitch models that log to a hard disk.
memory log ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> <username_str> <password_str> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}	Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option is available on FortiSwitch models that log to a hard disk.
memory log tftp <server_ipv4> {app-ctrl | event | ids | im | spam | virus | voip | web-filter}	Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option is available on FortiSwitch models that log to a hard disk.

Example

This example shows how to backup the FortiSwitch system configuration to a file named **fgt.cfg** on a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fgt.cfg 192.168.1.23
```

batch

Use the batch commands to execute a series of CLI commands.

The **execute batch** commands are controlled by the Maintenance (**mntgrp**) access control group.

Syntax

```
execute batch [<cmd_cue>]
```

The parameter <cmd_cue> includes the following values:

- **end** — exit session and run the batch commands
- **lastlog** — read the result of the last batch commands
- **start** — start batch mode
- **status** — batch mode status reporting if batch mode is running or stopped

Example

To start batch mode:

```
   execute batch start
Enter batch mode...
```

To enter commands to run in batch mode:

```
config system global
set refresh 5
end
```

To execute the batch commands:

```
   execute batch end
Exit and run batch commands...
```

central-mgmt

Update Central Management Service account information. Also used receive configuration file updates from an attached FortiManager unit.

Syntax

```
execute central-mgmt set-mgmt-id <management_id>
execute central-mgmt register-device <fmg-serial-number> <fmg-register-password> <fgt-
    user-name> <fgt-password>
execute central-mgmt unregister-device <fmg-serial-number>
execute central-mgmt update
```

set-mgmt-id is used to change or initially set the management ID, or your account number for Central Management Services. This account ID must be set for the service to be enabled.

register-device registers the FortiSwitch with a specific FortiManager unit specified by serial number. You must also specify the administrator name and password that the FortiManager unit uses to log on to the FortiSwitch.

unregister-device removes the FortiSwitch from the specified FortiManager unit's device list.

update is used to update your Central Management Service contract with your new management account ID. This command is to be used if there are any changes to your management service account.

update is also one of the steps in your FortiSwitch receiving a configuration file from an attached FortiManager unit.

Example

If you are registering with the Central Management Service for the first time, and your account number is 123456, you would enter the following:

```
execute central-mgmt set-mgmt-id 123456
execute central-mgmt update
```

cfg reload

Use this command to restore the saved configuration when the configuration change mode is `manual` or `revert`. This command has no effect if the mode is `automatic`, the default. The `set cfg-save` command in `system global` sets the configuration change mode.

When you reload the saved system configuration, the your session ends and the FortiSwitch performs a restart.

In the default configuration change mode, `automatic`, CLI commands become part of the saved system configuration when you execute them by entering either next or end.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the system restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are saved automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. You set the timeout in `system global` using the `set cfg-revert-timeout` command.

Syntax

```
execute cfg reload
```

Example

This is sample output from the command when successful:

```
# execute cfg reload
configs reloaded. system will reboot.This is sample output from the command when not in
    runtime-only configuration mode:
# execute cfg reload
no config to be reloaded.
```

cfg save

Use this command to save configuration changes when the configuration change mode is `manual` or `revert`. If the mode is `automatic`, the default, all changes are added to the saved configuration as you make them and this command has no effect. The `set cfg-save` command in `system global` sets the configuration change mode.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the system restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are reverted automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. To change the timeout from the default of 600 seconds, go to `system global` and use the `set cfg-revert-timeout` command.

Syntax

```
execute cfg save
```

Example

This is sample output from the command:

```
# execute cfg save
config saved.
This is sample output when not in runtime-only configuration mode. It also occurs when in
    runtime-only configuration mode and no changes have been made:
# execute cfg save
no config to be saved.
```

clear system arp table

Clear all the entries in the arp table.

Syntax

```
execute clear system arp table
```

cli check-template-status

Reports the status of the secure copy protocol (SCP) script template.

Syntax

```
execute cli check-template-status
```

cli status-msg-only

Enable or disable displaying standardized CLI error output messages. If executed, this command stops other debug messages from displaying in the current CLI session. This command is used for compatibility with ??????.

Syntax

```
execute cli 1915046 status-msg-only [enable | disable]
```

Variable	Description	Default
status-msg-only [enable | disable]	Enable or disable standardized CLI error output messages. Entering the command without enable or disable disables displaying standardized output.	enable

date

Get or set the system date.

Syntax

```
execute date [<date_str>]
```

date_str has the form `yyyy-mm-dd`, where:

- **yyyy** is the year. The range is: 2001 to 2037
- **mm** is the month. The range is 01 to 12
- **dd** is the day of the month. The range is 01 to 31

If you do not specify a date, the command returns the current system date. Shortened values, such as '06' instead of '2006' for the year or '1' instead of '01' for month or day, are not valid.

Example

This example sets the date to 17 September 2004:

```
execute date 2004-09-17
```

{dhcp | dhcp6} lease-clear

Clear all DHCP address leases.

Syntax

For IPv4:

```
execute dhcp lease-clear
```

For IPv6

```
execute dhcp6 lease-clear
```

{dhcp | dhcp6} lease-list

Display DHCP leases on a given interface

Syntax

For IPv4:

```
execute dhcp lease-list [interface_name]
```

For IPv6:

```
execute dhcp6 lease-list [interface_name]
```

If you specify an interface, the command lists only the leases issued on that interface. Otherwise, the list includes all leases issued by DHCP servers on the FortiSwitch.

If there are no DHCP leases in user on the FortiSwitch, an error will be returned.

disconnect-admin-session

Disconnect an administrator who is logged in.

Syntax

```
execute disconnect-admin-session <index_number>
```

To determine the index of the administrator that you want to disconnect, view the list of logged-in administrators by using the following command:

```
execute disconnect-admin-session ?
```

The list of logged-in administrators looks like this:

```
Connected:
INDEX   USERNAME     TYPE      FROM               TIME
    0       admin        WEB       172.20.120.51      Mon Aug 14 12:57:23 2006
    1       admin2       CLI       ssh(172.20.120.54) Mon Aug 14 12:57:23 2006
```

Example

This example shows how to disconnect the logged administrator `admin2` from the above list.

```
execute disconnect-admin-session 1
```

factoryreset

Reset the FortiSwitch configuration to factory default settings.

Syntax

```
execute factoryreset
```

This procedure deletes all changes that you have made to the FortiSwitch configuration and reverts the system to its original configuration, including resetting interface addresses.

firmware-list update

Use this command to update the list of firmware.

Syntax

```
execute firmware-list update
```

When the update is complete, the command reports:

```
Updating Image List. Done.
```

formatlogdisk

Format the FortiSwitch hard disk to enhance performance for logging.

Syntax

```
execute formatlogdisk
```

In addition to deleting logs, this operation will erase all other data on the disk, including system configuration.

fortiguard-log update

Update the FortiGuard Analysis and Management Service contract.

Syntax

```
execute fortiguard-log update
```

fsso refresh

Use this command to manually refresh user group information from Directory Service servers connected to the FortiSwitch using the Fortinet Single Sign On (FSSO) agent.

Syntax

```
execute fsso refresh
```

interface dhcpclient-renew

Renew the DHCP client for the specified DHCP interface and close the CLI session. If there is no DHCP connection on the specified port, there is no output.

Syntax

```
execute interface dhcpclient-renew <port>
```

Example

This is the output for renewing the DHCP client on port1 before the session closes:

```
# execute interface dhcpclient-renew port1
renewing dhcp lease on port1
```

interface pppoe-reconnect

Reconnect to the PPPoE service on the specified PPPoE interface and close the CLI session. If there is no PPPoE connection on the specified port, there is no output.

Syntax

```
execute interface pppoe-reconnect <port>
```

log delete

Use this command to clear all traffic log entries in memory. You will be prompted to confirm the command.

Syntax

```
execute log delete
```

log delete-all

Use this command to clear all log entries in memory and current log files on hard disk. If your system has no hard disk, only log entries in system memory will be cleared. You will be prompted to confirm the command.

Syntax

```
execute log delete-all
```

log display

Use this command to display log messages that you have selected with the `execute log filter` command.

Syntax

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the commands

```
execute log filter start-line 1
execute log display
```

You can restore the log filters to their default values using the command

```
execute log filter reset
```

log filter

Use this command to select log messages for viewing or deletion. You can view one log category on one device at a time. Optionally, you can filter the messages to select only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

Commands are cumulative. If you omit a required variable, the command displays the current setting.

Use as many **execute log filter** commands as you need to define the log messages that you want to view.

```
execute log filter category <category_name>
execute log filter device {memory | faz | fds}
execute log filter dump
execute log filter field <name>
execute log filter ha-member <unitsn_str>
execute log filter max-checklines <int>
execute log filter reset
execute log filter start-line <line_number>
execute log filter view-lines <count>
```

Variable	Description	Default
category <category_name>	Enter the type of log you want to select. For SQL logging and memory logging, one of: utm, content, event, or traffic	`event`
device {memory | faz | fds}	Device where the logs are stored.	memory
dump	Display current filter settings.	No default
field <name>	Press Enter to view the fields that are available for the associated category. Enter the fields you want, using commas to separate multiple fields.	No default
ha-member <unitsn_str>	Select logs from the specified HA cluster member. Enter the serial number of the system.	No default
max-checklines <int>	Set maximum number lines to check. Range 100 to 1 000 000. 0 disables.	No default
reset	Execute this command to reset all filter settings.	No default
start-line <line_number>	Select logs starting at specified line number.	1
view-lines <count>	Set lines per view. Range: 5 to 1000	10

log fortianalyzer

Use this command to test the connection to the FortiAnalyzer unit. This command is available only when FortiAnalyzer is configured.

Syntax

```
execute log fortianalyzer
```

Example

When FortiAnalyzer is connected, the output looks like this:

```
FortiAnalyzer Host Name: FortiAnalyzer-800B
FortiSwitch Device ID: FG50B3G06500085
Registration: registered
Connection: allow
Disk Space (Used/Allocated): 468/1003 MB
Total Free Space: 467088 MB
Log: Tx & Rx
Report: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
```

When FortiAnalyzer is not connected, the output is: `Connect Error`

log-report reset

Use this command to delete all logs, archives and user configured report templates.

Syntax

```
execute log-report reset
```

mac clear

Use this command to clear MAC addresses.

Syntax

```
execute mac clear by-interface <interface>
execute mac clear by-mac-address <mac_address>
execute mac clear by-vlan <vlan_int>
execute mac clear by-vlan-and-interface <vlan_int> <interface>
execute mac clear by-vlan-and-mac-address <vlan_int> <mac_address>
```

ping

The ping command sends one or more ICMP echo request (ping) to test the network connection between the FortiSwitch and another network device.

Syntax

```
execute ping {<address_ipv4> | <host-name_str>}
```

<host-name_str> should be an IP address, or a fully qualified domain name.

Example

This example shows how to ping a host with the IP address 172.20.120.16.

```
#execute ping 172.20.120.16

PING 172.20.120.16 (172.20.120.16): 56 data bytes
64 bytes from 172.20.120.16: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.20.120.16: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=4 ttl=128 time=0.2 ms

--- 172.20.120.16 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

ping-options, ping6-options

Use this command to set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiSwitch and another network device.

Syntax

```
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds>
execute ping-options tos <service_type>
execute ping-options ttl <hops>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
data-size <bytes>	Specify the datagram size in bytes.	56
df-bit {yes | no}	Set `df-bit` to `yes` to prevent the ICMP packet from being fragmented. Set `df-bit` to `no` to allow the ICMP packet to be fragmented.	no
pattern <2-byte_hex>	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the `data_size` parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default
repeat-count <repeats>	Specify how many times to repeat ping.	5
source {auto | <source-intf_ip>}	Specify the FortiSwitch interface from which to send the ping. If you specify `auto`, the system selects the source address and interface based on the route to the `<host-name_str>` or `<host_ip>`. Specifying the IP address of a FortiSwitch interface tests connections to different network segments from the specified interface.	auto
timeout <seconds>	Specify, in seconds, how long to wait until ping times out.	2
tos <service_type>	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted. lowdelay = minimize delay throughput = maximize throughput reliability = maximize reliability lowcost = minimize cost	0

Variable	Description	Default
ttl <hops>	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
validate-reply {yes | no}	Select `yes` to validate reply data.	`no`
view-settings	Display the current ping-option settings.	No default

Example

Use the following command to increase the number of pings sent.

```
execute ping-options repeat-count 10
```

Use the following command to send all pings from the FortiSwitch interface with IP address 192.168.10.23.

```
execute ping-options source 192.168.10.23
```

ping6

The ping6 command sends one or more ICMP echo request (ping) to test the network connection between the FortiSwitch and an IPv6 capable network device.

Syntax

```
execute ping6 {<address_ipv6> | <host-name_str>}
```

Example

This example shows how to ping a host with the IPv6 address `12AB:0:0:CD30:123:4567:89AB:CDEF`.

```
execute ping6 12AB:0:0:CD30:123:4567:89AB:CDEF
```

poe-reset

This command performs a poe reset on the specified port.

Syntax

```
execute poe-reset <port_number>
```

reboot

Use this command to restart the system.

Abruptly powering off your system may corrupt its configuration. Use the `reboot` or `shutdown` commands to ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute reboot <comment "comment_string">
```

`<comment "comment_string">` enables you to optionally add a message that will appear in the hard disk log indicating the reason for the reboot. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute reboot comment "December monthly maintenance"
```

restore

Use this command to restore configuration, firmware or IPS signature file. The following options are available:

- restore the configuration from a file
- change the FortiSwitch firmware
- restore the bios from a file

When virtual domain configuration is enabled, the content of the backup file depends on the administrator account that created it.

A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin account can restore the configuration from this file.

A backup file from a regular administrator account contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```
execute restore bios tftp <filename_str> <server_ipv4[:port_int]>
execute restore config flash <revision>
execute restore config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]
    > [<username_str> <password_str>] [<backup_password_str>]
execute restore config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute restore image flash <revision>
execute restore image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore image management-station <version_int>
execute restore image tftp <filename_str> <server_ipv4>
```

Variable	Description
bios tftp <filename_str> <server_ipv4 [:port_int]>	Restore the bios. Download the restore file from a TFTP server.
config flash <revision>	Restore the specified revision of the system configuration from the flash disk.
config ftp <filename_str> <server_ipv4 [:port_int] | server_fqdn[:port_int]> [<user-name_str> <password_str>] [<backup_ password_str>]	Restore the system configuration from an FTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password.
config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Restore the system configuration from a file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password.

Variable	Description
image flash <revision>	Restore specified firmware image from flash disk.
image ftp <filename_str> <server_ipv4 [:port_int] | server_fqdn[:port_int]> [<user-name_str> <password_str>]	Download a firmware image from an FTP server to the FortiSwitch. The FortiSwitch reboots, loading the new firmware. This command is not available in multiple VDOM mode.
image management-station <version_ int>	Download a firmware image from the central management station. This is available if you have configured a FortiManager unit as a central management server. This is also available if your account with FortiGuard Analysis and Management Service allows you to upload firmware images.
image tftp <filename_str> <server_ipv4>	Download a firmware image from a TFTP server to the FortiSwitch. The FortiSwitch reboots, loading the new firmware.

Example

This example shows how to upload a configuration file from a TFTP server to the FortiSwitch and restart the FortiSwitch with this configuration. The name of the configuration file on the TFTP server is `backupconfig`. The IP address of the TFTP server is 192.168.1.23.

```
execute restore config tftp backupconfig 192.168.1.23
```

revision

Use this command to manage configuration and firmware image files on the local disk.

Syntax

To delete a configuration file

```
execute revision delete config <revision>
```

To delete a firmware image file

```
execute revision delete image <revision>
```

To list the configuration files

```
execute revision list config
```

To delete a firmware image file

```
execute revision list image
```

set system session filter

Use this command to define the session filter for the **get system session** command.

Syntax

To clear the filter settings

```
execute set system session filter clear
    {all|dport|dst|duration|expire|policy|proto|sport|src|vd}
```

To specify destination port

```
execute set system session filter dport <port_range>
```

To specify destination IP address

```
execute set system session filter dst <ip_range>
```

To specify duration

```
execute set system session filter duration <duration_range>
```

To specify expiry

```
execute set system session filter expire <expire_range>
```

To list the filter settings

```
execute set system session filter list
```

To invert a filter setting

```
execute set system session filter negate
    {dport|dst|duration|expire|policy|proto|sport|src|vd}
```

To specify firewall policy ID

```
execute set system session filter policy <policy_range>
```

To specify protocol

```
execute set system session filter proto <protocol_range>
```

To specify source port

```
execute set system session filter sport <port_range>
```

To specify source IP address

```
execute set system session filter src <ip_range>
```

Variable	Description
<duration_range>	The start and end times (units?), separated by a space.
<expire_range>	The start and end times (units?), separated by a space.
<ip_range>	The start and end IP addresses, separated by a space.
<policy_range>	The start and end policy numbers, separated by a space.
<port_range>	The start and end port numbers, separated by a space.
<protocol_range>	The start and end protocol numbers, separated by a space.

set-next-reboot

Use this command to start the FortiSwitch with primary or secondary firmware after the next reboot. This command is available on models that can store two firmware images. By default, the FortiSwitch loads the firmware from the primary partition.

Syntax

```
execute set-next-reboot {primary | secondary}
```

shutdown

Use this command to shut down the system immediately. You will be prompted to confirm this command.

Abruptly powering off your system may corrupt its configuration. Using the reboot and shutdown options in the CLI or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute shutdown [comment <comment_string>]
```

The comment field is optional. Use it to add a message that will appear in the event log message that records the shutdown. The comment message does not appear on the Alert Message console. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute shutdown comment "emergency facility shutdown"
```

An event log message similar to the following is recorded:

```
2009-09-08 11:12:31 critical admin 41986 ssh(172.20.120.11) shutdown User admin shutdown
    the device from ssh(172.20.120.11). The reason is 'emergency facility shutdown'
```

ssh

Use this command to establish an SSH session with another system.

Syntax

```
execute ssh <destination>
```

`<destination>` - the destination in the form user@ip or user@host.

Example

```
execute ssh admin@172.20.120.122
```

To end an ssh session, type `exit`:

```
FGT-6028030112 # exit
Connection to 172.20.120.122 closed.
FGT-8002805000 #
```

telnet

Use this command to create a Telnet client. You can use this tool to test network connectivity.

Syntax

```
execute telnet <telnet_ipv4>
```

`<telnet_ipv4>` is the address to connect with.

Type `exit` to close the telnet session.

time

Get or set the system time.

Syntax

```
execute time [<time_str>]
```

time_str has the form **hh:mm:ss,** where:

- **hh** is the hour. The range is 00 to 23.
- **mm** is the minutes. The range is 00 to 59.
- **ss** is the seconds. The range is 00 to 59.

If you do not specify a time, the command returns the current system time.

You are allowed to shorten numbers to only one digit when setting the time. For example both 01:01:01 and 1:1:1 are allowed.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

traceroute

Use this command to test the connection between the FortiSwitch and another network device, and display information about the network hops between the FortiSwitch and the device.

Syntax

```
execute traceroute {<ip_address> | <host-name>}
```

Example

This example shows how to test the connection with http://docs.forticare.com. In this example the traceroute command times out after the first hop indicating a possible problem.

```
#execute traceoute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte packets
1 172.20.120.2 (172.20.120.2) 0.324 ms 0.427 ms 0.360 ms
 2  * * *
```

If your FortiSwitch is not connected to a working DNS server, you will not be able to connect to remote host-named locations with traceroute.

tracert6

Use this command to test the connection between the FortiSwitch and another network device using IPv6 protocol, and display information about the network hops between the FortiSwitch and the device.

Syntax

```
tracert6 [-Fdn] [-f first_ttl] [-i interface] [-m max_ttl]
[-s src_addr] [-q nprobes] [-w waittime] [-z sendwait]
host [paddatalen]
```

Variable	Description
-F	Set Don't Fragment bit.
-d	Enable debugging.
-n	Do not resolve numeric address to domain name.
-f <first_ttl>	Set the initial time-to-live used in the first outgoing probe packet.
-i <interface>	Select interface to use for tracert.
-m <max_ttl>	Set the max time-to-live (max number of hops) used in outgoing probe packets.
-s <src_addr>	Set the source IP address to use in outgoing probe packets.
-q <nprobes>	Set the number probes per hop.
-w <waittime>	Set the time in seconds to wait for response to a probe. Default is 5.
-z <sendwait>	Set the time in milliseconds to pause between probes.
host	Enter the IP address or FQDN to probe.
<paddatalen>	Set the packet size to use when probing.

upload

Use this command to upload system configurations to the flash disk from FTP or TFTP sources.

Syntax

To upload configuration files:

```
execute upload config ftp <filename_str> <comment> <server_ipv4[:port_int] | server_fqdn
    [:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute upload config tftp <filename_str> <comment> <server_ipv4>
```

Variable	Description
<comment>	Comment string.
<filename_str>	Filename to upload.
<server_fqdn[:port_int]>	Server fully qualified domain name and optional port.
<server_ipv4[:port_int]>	Server IP address and optional port number.
<username_str>	Username required on server.
<password_str>	Password required on server.
<backup_password_str>	Password for backup file.

get

The get commands provide information about the operation of the FortiSwitch.

firewall iprope list

Use this command to list all of the FortiSwitch iprope firewall policies. Optionally include a group number in hexadecimal format to display a single policy. Policies are listed in FortiOS format.

Syntax

get firewall iprope list [<group_number_hex>]

Example output

```
get firewall iprope list 0010000c

policy flag (20): auth
flag2 (8000):
imflag: sockport: 0 action: accept index: 0
schedule() group=00000003 av=00000000 au=00000000 host=0 split=00000000
chk_client_info=0x0 app_list=0 ips_view=0 misc=0 grp_info=0 seq=0 hash=0
tunnel=
zone(1): 0 ->zone(1): 0
source(1): 0.0.0.0-255.255.255.255,
dest(1): 0.0.0.0-255.255.255.255,
source wildcard(0):
destination wildcard(0):
service(1):
[17:0x0:0/(0,65535)->(53,53)]
nat(0):
mms: 0 0
```

firewall proute, proute6

Use these commands to list policy routes.

Syntax

For IPv4 policy routes:

```
get firewall proute
```

For IPv6 policy routes:

```
get firewall proute6
```

Example output

```
get firewall proute
list route policy info(vf=root):
iff=5 src=1.1.1.0/255.255.255.0 tos=0x00 tos_mask=0x00 dst=0.0.0.0/0.0.0.0 protocol=80
    port=1:65535
oif=3 gwy=1.2.3.4
```

hardware cpu

Use this command to display detailed information about the CPUs in your FortiSwitch.

Syntax

```
get hardware cpu
```

Example output

```
FS108D3W14000369 # get hardware cpu
Processor       : Feroceon 88FR131 rev 1 (v5l)
BogoMIPS        : 499.71
Features        : swp half thumb fastmult edsp
CPU implementer : 0x56
CPU architecture: 5TE
CPU variant     : 0x2
CPU part        : 0x131
CPU revision    : 1

Hardware        : Feroceon-KW
Revision        : 0000
Serial          : 0000000000000000
```

hardware memory

Use this command to display information about FortiSwitch memory use. Information includes the total memory, memory in use, and free memory.

Syntax

```
get hardware memory
```

Example output

```
get hardware memory
total: used: free: shared: buffers: cached: shm:
Mem: 3703943168 348913664 3355029504 0 192512 139943936 137314304
Swap: 0 0 0
MemTotal: 3617132 kB
MemFree: 3276396 kB
MemShared: 0 kB
Buffers: 188 kB
Cached: 136664 kB
SwapCached: 0 kB
Active: 22172 kB
Inactive: 114740 kB
HighTotal: 1703936 kB
HighFree: 1443712 kB
LowTotal: 1913196 kB
LowFree: 1832684 kB
SwapTotal: 0 kB
SwapFree: 0 kB
```

hardware nic

Use this command to display hardware and status information about each FortiSwitch interface. The hardware information includes details such as the driver name and version and chip revision. Status information includes transmitted and received packets, and different types of errors.

Syntax

```
get hardware nic <interface_name>
```

Variable	Description
<interface_name>	A FortiSwitch interface name.

Example output

```
# get hardware nic
The following NICs are available:
internal
mgmt

# get hardware nic mgmt
Driver Name :Fortinet Nplite Driver
Version :1.0
Admin :up
Current_HWaddr 00:09:0f:ee:f5:29
Permanent_HWaddr 00:09:0f:ee:f5:29
Status :up
Speed :100
Duplex :Full
Host Rx Pkts :2388534
Host Rx Bytes :373419510
Host Tx Pkts :12876
Host Tx Bytes :1275606
Rx Pkts :2954556
Rx Bytes :657649553
Tx Pkts :12874
Tx Bytes :1177684
rx_buffer_len :2048
Hidden :No
cmd_in_list :0
> | setting <device_name_str>}
```

hardware status

Report information about the FortiSwitch hardware including ASIC version, CPU type, amount of memory, flash drive size, hard disk size (if present), and USB flash size (if present). Use this information to troubleshoot, to provide to Fortinet Support, or to confirm the features that your FortiSwitch model supports.

Syntax

```
get hardware status
```

Example output

```
# get hardware status
Model name: FortiSwitch-324B-POE
ASIC version: CP0
ASIC SRAM: 64M
CPU: FortiSOC
RAM: 443 MB
Compact Flash: 3838 MB /dev/sda
Hard disk: not available
USB Flash: not available
```

log {custom field | eventfilter | gui}

Use this command to get information about your log settings.

Syntax

```
get log {custom field | eventfilter | gui}
```

Example output

```
# get log eventfilter
event : enable
router : enable
system : enable
user : enable
```

log memory global-setting

Use this command to get information about your logging to memory global settings.

Syntax

```
get log memory global-setting
```

Example output

```
# get log memory global-setting
full-final-warning-threshold: 95
full-first-warning-threshold: 75
full-second-warning-threshold: 90
hourly-upload : disable
max-size : 98304
```

log {memory | syslogd | syslogd2 | syslogd3} filter

Use this command to get information about your log filter settings.

Syntax

```
get log {memory | syslogd | syslogd2 | syslogd3} filter
```

Example output

```
# get log memory filter
severity : information
```

log {memory | syslogd | syslogd2 | syslogd3} setting

Use this command to get information about your log settings.

Syntax

```
get log {memory | syslogd | syslogd2 | syslogd3} setting
```

Example output

```
# get log memory setting
diskfull : overwrite
status : enable
```

switch global

Use this command to get information about the global settings of your FortiSwitch.

Syntax

```
get switch global
```

Example output

```
# get switch global
mac-aging-interval : 300
name : (null)
```

switch interface

Use this syntax to get information about the interfaces.

Syntax

```
get switch interface
```

switch mirror

Use this syntax to get information about the mirror settings of your FortiSwitch.

Syntax

```
get switch mirror
```

Example output

```
# get switch mirror
dst : (null)
status : inactive
switching-packet : disable
```

switch physical-port

Use this command to get information about the physical ports of your FortiSwitch.

Syntax

```
get switch physical-port
```

Example output

```
# get switch physical-port
== [ port1 ]
name: port1 link-status: down poe-status: 0.00W status: up
== [ port2 ]
name: port2 link-status: down poe-status: 0.00W status: up
== [ port3 ]
name: port3 link-status: down poe-status: 0.00W status: up
```

switch poe inline

Use this command to get information about the system's power over Ethernet (PoE) functions.

Syntax

```
get switch poe inline
```

Example output

```
# get switch poe inline
Unit Power Budget: 75.00W
Unit Power Consumption: 0.00W
Unit Temperature: 60.00 Centigrade
```

switch stp instance

Use this command to get information about STP instances on your FortiSwitch.

Syntax

```
get switch stp instance
```

Example output

```
# get switch stp instance
== [ 0 ]
id: 0
== [ 1 ]
id: 1
```

switch stp settings

Use this command to get information about STP settings on your FortiSwitch.

Syntax

```
get switch stp settings
```

Example output

```
# get switch stp settings
forward-time : 15
hello-time : 2
max-age : 20
max-hops : 20
name : (null)
revision : 0
status : enable
```

switch trunk

Use this command to get information about the trunks on the FortiSwitch.

Syntax

```
get switch trunk
```

Example output

```
# get switch trunk
== [ 1 ]
name: 1 members:
== [ port3 ]
member-name: port3
== [ port10 ]
member-name: port10
== [ port1 ]
member-name: port1
```

switch vlan

Use this command to get information about VLANs on the FortiSwitch.

Syntax

```
get switch vlan
```

Example output

```
# get switch vlan
== [ 1 ]
id: 1 private-vlan-type: primary isolated-vlan: 2 community-vlans: 3
== [ 2 ]
id: 2 private-vlan-type: isolated sub-VLAN primary-vlan: 1
== [ 3 ]
id: 3 private-vlan-type: community sub-VLAN primary-vlan: 1
```

system admin list

Use this command to view a list of all the current administration sessions.

Syntax

```
get system admin list
```

Example output

```
# get system admin list
username local  device                   remote                 started
admin    sshv2  port1:172.20.120.148:22  172.20.120.16:4167     2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443 172.20.120.161:56365 2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443 172.20.120.16:4214    2006-08-09 12:25:29
```

Variable	Description
username	Name of the admin account for this session
local	The protocol this session used to connect to the system.
device	The interface, IP address, and port used by this session to connect to the system.
remote	The IP address and port used by the originating computer to connect to the system.
started	The time the current session started.

system admin status

Use this command to view the status of the currently logged in admin and their session.

Syntax

```
get system admin status
```

Example

The output looks like this:

```
# get system admin status
username: admin
login local: sshv2
login device: port1:172.20.120.148:22
login remote: 172.20.120.16:4167
login vdom: root
login started: 2006-08-09 12:24:20
current time: 2006-08-09 12:32:12
```

Variable	Description
username	Name of the admin account currently logged in.
login local	The protocol used to start the current session.
login device	The login information from the FortiSwitch including interface, IP address, and port number.
login remote	The computer the user is logging in from including the IP address and port number.
login vdom	The virtual domain the admin is current logged into.
login started	The time the current session started.
current time	The current time of day on the system

system arp

Use this command to view the ARP table entries on the FortiSwitch.

Syntax

```
get system arp
```

Example output

```
# get system arp
Address Age(min) Hardware Addr Interface
172.20.120.16 0 00:0d:87:5c:ab:65 internal
172.20.120.138 0 00:08:9b:09:bb:01 internal
```

system arp-table

Use this command to view the ARP tables on the FortiSwitch.

Syntax

```
get system arp-table
```

Example output

```
# get system arp-table
== [ 1 ]
id: 1 interface: internal ip: 10.10.10.10 mac: 01:02:03:04:05:aa
```

system auto-update

Use this command to get information about auto-update status

Syntax

```
get system auto-update status
```

system bug-report

Use this command to get information about configuration related to bug reporting.

Syntax

```
get system bug-report
```

Example output

```
auth : no
mailto : bug_report@fortinetvirussubmit.com
password : (null)
server : fortinetvirussubmit.com
username : bug_report
username-smtp : bug_report
```

system central-mgmt

Use this command to get information about configuration related to central management

Syntax

```
get system central-mgmt
```

system checksum status

Use this command to view system checksum values

Syntax

```
get system checksum status
```

Example

```
# get system checksum status
global: 6a da e7 8e 4b 0a 9a 44 8a 9f c8 1d 74 60 1f 58
root: f1 8d 2d d2 db 0b b8 57 a9 46 0a 90 d6 43 98 76
all: e9 b9 3a 21 ff 7d fb fd a4 ca c4 91 71 a9 3c bf
```

system cmdb status

Use this command to view information about cmdbsvr on the FortiSwitch.

Syntax

```
get system cmdb status
```

Example output

```
# get system cmdb status
version: 1
owner id: 18
update index: 6070
config checksum: 12879299049430971535
last request pid: 68
last request type: 29
last request: 78
```

Variable	Description
version	Version of the cmdb software.
owner id	Process ID of the cmdbsvr daemon.
update index	The updated index shows how many changes have been made in cmdb.
config checksum	The config file version used by FortiManager.
last request pid	The last process to access the cmdb.
last request type	Type of the last attempted access of cmdb.
last request	The number of the last attempted access of cmdb.

system console

Use this command to get information about the console connection.

Syntax

```
get system console
```

Example output

```
# get system console
baudrate : 9600
mode : line
output : more
```

system dns

Use this command to get information about the DNS settings.

Syntax

```
get system dns
```

Example output

```
# get system dns
primary : 208.91.112.53
secondary : 208.91.112.52
domain : (null)
ip6-primary : ::
ip6-secondary : ::
dns-cache-limit : 5000
dns-cache-ttl : 1800
cache-notfound-responses: disable
source-ip : 0.0.0.0
```

system global

Use this command to get the global settings of your FortiSwitch.

Syntax

```
get system global
```

Example output

```
# get system global
admin-concurrent : enable
admin-https-pki-required: disable
admin-lockout-duration: 60
admin-lockout-threshold: 3
admin-maintainer : enable
admin-port : 80
admin-scp : disable
admin-server-cert : self-sign
admin-sport : 443
admin-ssh-grace-time: 120
admin-ssh-port : 22
admin-ssh-v1 : disable
admin-telnet-port : 23
admintimeout : 5
allow-subnet-overlap: disable
cfg-save : automatic
csr-ca-attribute : enable
daily-restart : disable
dst : enable
gui-lines-per-page : 50
hostname : FS324P3W11000127
language : english
ldapconntimeout : 500
log-user-in-upper : disable
radius-port : 1812
refresh : 0
registration-notification: enable
remoteauthtimeout : 5
revision-backup-on-logout: enable
send-pmtu-icmp : enable
service-expire-notification: enable
strong-crypto : disable
switch-mgmt-mode : local
timezone : (GMT-8:00)Pacific Time(US&Canada)
user-server-cert : self-sign
```

system ha-nonsync-csum

Use this command to display the system checksums.

Syntax

```
get system ha-nonsync-csum
```

Example

```
# get system ha-nonsync-csum
debugzone
global: f1 d7 ea 74 d1 a4 12 f2 44 a6 de 63 3b 72 68 4a
root: cb f5 51 b2 f8 da 64 41 23 69 bb 00 60 25 b6 ca
all: 38 1b c0 bc fe e9 88 77 30 fc 80 5d 59 d8 0c 7b

checksum
global: f1 d7 ea 74 d1 a4 12 f2 44 a6 de 63 3b 72 68 4a
root: cb f5 51 b2 f8 da 64 41 23 69 bb 00 60 25 b6 ca
all: 38 1b c0 bc fe e9 88 77 30 fc 80 5d 59 d8 0c 7b

FS324P3W11000005 #
```

system info admin ssh

Use this command to display information about the SSH configuration on the FortiSwitch such as:

- the SSH port number
- the interfaces with SSH enabled
- the hostkey DSA fingerprint
- the hostkey RSA fingerprint

Syntax

```
get system info admin ssh
```

Example output

```
# get system info admin ssh
SSH v2 is enabled on port 22
SSH is enabled on the following 1 interfaces:
mgmt
SSH hostkey DSA fingerprint = cd:e1:87:70:bb:f0:9c:7d:e3:7b:73:f7:44:23:a5:99
SSH hostkey RSA fingerprint = c9:5b:49:1d:7c:ba:be:f3:9d:39:33:4d:48:9d:b8:49
```

system info admin status

Use this command to display administrators that are logged into the FortiSwitch.

Syntax

```
get system info admin status
```

Example

This shows sample output.

```
Index User name Login type From
0 admin CLI ssh(172.20.120.16)
1 admin WEB 172.20.120.16
```

Variable	Description
Index	The order the administrators logged in.
User name	The name of the user account logged in.
Login type	Which interface was used to log in.
From	The IP address this user logged in from.

system interface physical

Use this command to list information about the physical network interfaces.

Syntax

```
get system interface physical
```

Example output

```
# get system interface physical
== [onboard]
==[internal]
mode: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
==[mgmt]
mode: static
ip: 172.20.120.129 255.255.255.0
ipv6: ::/0
status: up
speed: 1000Mbps (Duplex: full)
```

system mgmt-csum

Use this command to display system checksum values.

Syntax

```
get system mgmt-csum
```

Example

```
# get system mgmt-csum
debugzone
global: 6a da e7 8e 4b 0a 9a 44 8a 9f c8 1d 74 60 1f 58
root: f1 8d 2d d2 db 0b b8 57 a9 46 0a 90 d6 43 98 76
all: e9 b9 3a 21 ff 7d fb fd a4 ca c4 91 71 a9 3c bf

checksum
global: 6a da e7 8e 4b 0a 9a 44 8a 9f c8 1d 74 60 1f 58
root: f1 8d 2d d2 db 0b b8 57 a9 46 0a 90 d6 43 98 76
all: e9 b9 3a 21 ff 7d fb fd a4 ca c4 91 71 a9 3c bf
```

system ntp

Use this command to get information about the NTP settings.

Syntax

```
get system ntp
```

Example output

```
ntpserver:
== [ 1 ]
id: 1
== [ 2 ]
id: 2
ntpsync : enable
source-ip : 0.0.0.0
syncinterval : 1
```

system password-policy

Use this command to view the password policy.

Syntax

```
get system password-policy
```

Example output

```
# get system password-policy
status : enable
apply-to : admin-password
minimum-length : 8
min-lower-case-letter: 2
min-upper-case-letter: 2
min-non-alphanumeric: 0
min-number : 2
change-4-characters : disable
expire-status : disable
```

system performance firewall

Use this command to display packet distribution and traffic statistics information for the FortiSwitch firewall.

Syntax

```
get system performance firewall packet-distribution
get system performance firewall statistics
```

Variable	Description
packet-distribution	Display a list of packet size ranges and the number of packets of each size accepted by the firewall since the system restarted. You can use this information to learn about the packet size distribution on your network.
statistics	Display a list of traffic types (browsing, email, DNS etc) and the number of packets and number of payload bytes accepted by the firewall for each type since the system was restarted.

Example output

```
get system performance firewall packet-distribution
getting packet distribution statistics...
0 bytes - 63 bytes: 655283 packets
64 bytes - 127 bytes: 1678278 packets
128 bytes - 255 bytes: 58823 packets
256 bytes - 383 bytes: 70432 packets
384 bytes - 511 bytes: 1610 packets
512 bytes - 767 bytes: 3238 packets
768 bytes - 1023 bytes: 7293 packets
1024 bytes - 1279 bytes: 18865 packets
1280 bytes - 1500 bytes: 58193 packets
> 1500 bytes: 0 packets

get system performance firewall statistics
getting traffic statistics...
Browsing: 623738 packets, 484357448 bytes
DNS: 5129187383836672 packets, 182703613804544 bytes
E-Mail: 23053606 packets, 2 bytes
FTP: 0 packets, 0 bytes
Gaming: 0 packets, 0 bytes
IM: 0 packets, 0 bytes
Newsgroups: 0 packets, 0 bytes
P2P: 0 packets, 0 bytes
Streaming: 0 packets, 0 bytes
TFTP: 654722117362778112 packets, 674223966126080 bytes
VoIP: 16834455 packets, 10 bytes
Generic TCP: 266287972352 packets, 8521215115264 bytes
Generic UDP: 0 packets, 0 bytes
Generic ICMP: 0 packets, 0 bytes
Generic IP: 0 packets, 0 bytes
```

system performance status

Use this command to display FortiSwitch CPU usage, memory usage, network usage, sessions, virus, IPS attacks, and system up time.

Syntax

```
get system performance status
```

Variable	Description
`CPU states`	The percentages of CPU cycles used by user, system, nice and idle categories of processes. These categories are: `user` -CPU usage of normal user-space processes `system` -CPU usage of kernel `nice` - CPU usage of user-space processes having other-than-normal running priority `idle` - Idle CPU cycles Adding user, system, and nice produces the total CPU usage as seen on the CPU widget on the web-based system status dashboard.
`Memory states`	The percentage of memory used.
Average network usage	The average amount of network traffic in kbps in the last 1, 10 and 30 minutes.
Average sessions	The average number of sessions connected to the FortiSwitch over the list 1, 10 and 30 minutes.
Average session setup rate	The number of sessions set up per second.
Uptime	How long since the system has been restarted.

Example output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
Memory states: 18% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 1 kbps in 30 minutes
Average sessions: 5 sessions in 1 minute, 6 sessions in 10 minutes, 5 sessions in 30
    minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 9days, 22 hours, 0 minutes
```

system performance top

Use this command to display the list of processes running on the system (similar to the Linux `top` command).

The following commands are available when **get system performance top** is running:

• Press Q or Ctrl+C to quit.

• Press P to sort the processes by the amount of CPU that the processes are using.

• Press M to sort the processes by the amount of memory that the processes are using.

Syntax

```
get system performance top [<delay_int>] <max_lines_int>]]
```

Variable	Description
<delay_int>	The delay, in seconds, between updating the process list. The default is 5 seconds.
<max_lines_int>	The maximum number of processes displayed in the output. The default is 20 lines.

system session list

This command returns a list of all the sessions active on the system.

Syntax

```
get system session list
```

Example output

```
PROTO     EXPIRE  SOURCE          SOURCE-NAT   DESTINATION    DESTINATION-NAT
tcp 0 127.0.0.1:1083 -          127.0.0.1:514 -
tcp 0 127.0.0.1:1085 -          127.0.0.1:514 -
tcp 10 127.0.0.1:1087 -          127.0.0.1:514 -
tcp 20 127.0.0.1:1089 -          127.0.0.1:514 -
tcp 30 127.0.0.1:1091 -          127.0.0.1:514 -
tcp 40 127.0.0.1:1093 -          127.0.0.1:514 -
tcp 60 127.0.0.1:1097 -          127.0.0.1:514 -
tcp 70 127.0.0.1:1099 -          127.0.0.1:514 -
tcp 80 127.0.0.1:1101 -          127.0.0.1:514 -
tcp 90 127.0.0.1:1103 -          127.0.0.1:514 -
tcp 100 127.0.0.1:1105 -          127.0.0.1:514 -
tcp 110 127.0.0.1:1107 -          127.0.0.1:514 -
tcp 103 172.20.120.16:3548 -        172.20.120.133:22 -
tcp 3600 172.20.120.16:3550 -        172.20.120.133:22 -
udp 175 127.0.0.1:1026 -          127.0.0.1:53 -
tcp 5 127.0.0.1:1084 -          127.0.0.1:514 -
tcp 5 127.0.0.1:1086 -          127.0.0.1:514 -
tcp 15 127.0.0.1:1088 -          127.0.0.1:514 -
tcp 25 127.0.0.1:1090 -          127.0.0.1:514 -
tcp 45 127.0.0.1:1094 -          127.0.0.1:514 -
tcp 59 127.0.0.1:1098 -          127.0.0.1:514 -
tcp 69 127.0.0.1:1100 -          127.0.0.1:514 -
tcp 79 127.0.0.1:1102 -          127.0.0.1:514 -
tcp 99 127.0.0.1:1106 -          127.0.0.1:514 -
tcp 109 127.0.0.1:1108 -          127.0.0.1:514 -
tcp 119 127.0.0.1:1110 -          127.0.0.1:514 -
```

Variable	Description
PROTO	The transfer protocol of the session.
EXPIRE	How long before this session will terminate.
SOURCE	The source IP address and port number.
SOURCE-NAT	The source of the NAT. '-' indicates there is no NAT.
DESTINATION	The destination IP address and port number.
DESTINATION-NAT	The destination of the NAT. '-' indicates there is no NAT.

system session status

Use this command to display the number of active sessions on the system.

Syntax

```
get system session status
```

Example output

```
The total number of sessions for the current VDOM: 3100
```

system session-helper-info list

Use this command to list the FortiSwitch session helpers and the protocol and port number configured for each one.

Syntax

```
get system sesion-helper-info list
```

Example output

```
list builtin help module:
mgcp
dcerpc
rsh
pmap
dns-tcp
dns-udp
rtsp
pptp
sip
mms
tns
h245
h323
ras
tftp
ftp
list session help:
help=pmap, protocol=17 port=111
help=rtsp, protocol=6 port=8554
help=rtsp, protocol=6 port=554
help=pptp, protocol=6 port=1723
help=rtsp, protocol=6 port=7070
help=sip, protocol=17 port=5060
help=pmap, protocol=6 port=111
help=rsh, protocol=6 port=512
help=dns-udp, protocol=17 port=53
help=tftp, protocol=17 port=69
help=tns, protocol=6 port=1521
help=mgcp, protocol=17 port=2727
help=dcerpc, protocol=17 port=135
help=rsh, protocol=6 port=514
help=ras, protocol=17 port=1719
help=ftp, protocol=6 port=21
help=mgcp, protocol=17 port=2427
help=dcerpc, protocol=6 port=135
help=mms, protocol=6 port=1863
help=h323, protocol=6 port=1720
```

system session-info

Use this command to display session information.

Syntax

```
get system session-info expectation
get system session-info full-stat
get system session-info list
get system session-info statistics
get system session-info ttl
```

Variable	Description
expectation	Display expectation sessions.
full-stat	Display detailed information about the session table including a session table and expect session table summary, firewall error statistics, and other information.
list	Display detailed information about all current sessions. For each session the command displays the protocol number, traffic shaping information, policy information, state information, statistics and other information.
statistics	Display the same information as the `full-stat` command except for the session table and expect session table summary.
ttl	Display the current setting of the `config system session-ttl` command including the overall session timeout as well as the timeouts for specific protocols.

Example output

```
get system session-info statistics
misc info: session_count=15 exp_count=0 clash=0 memory_tension_drop=0 ephemeral=1/32752
    removeable=14
delete=0, flush=0, dev_down=0/0
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000001
tcp reset stat:
syncqf=0 acceptqf=0 no-listener=227 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

system snmp sysinfo

Use this command to get information about your system's SNMP settings.

Syntax

```
get system snmp sysinfo
```

Example output

```
# get system snmp sysinfo
contact-info : (null)
description : (null)
engine-id : (null)
location : (null)
status : disable
trap-high-cpu-threshold: 80
trap-log-full-threshold: 90
trap-low-memory-threshold: 80
```

system source-ip status

Use this command to list defined source-IPs.

Syntax

```
get system source-ip status
```

Example output

```
# get sys source-ip status
The following services force their communication to use
a specific source IP address:

service=NTP source-ip=172.18.19.101
service=DNS source-ip=172.18.19.101
vdom=root service=RADIUS name=server-pc25 source-ip=10.1.100.101
vdom=root service=TACACS+ name=tac_plus_pc25 source-ip=10.1.100.101
vdom=root service=FSAE name=pc26 source-ip=172.18.19.101
vdom=V1 service=RADIUS name=pc25-Radius source-ip=172.16.200.101
vdom=V1 service=TACACS+ name=pc25-tacacs+ source-ip=172.16.200.101
vdom=V1 service=FSAE name=pc16 source-ip=172.16.200.101
```

system startup-error-log

Use this command to display information about system startup errors. This command only displays information if an error occurs when the system starts up.

Syntax

```
get system startup-error-log
```

system status

Use this command to display FortiSwitch status information including:

firmware version, build number and branch point

- serial number
- host name
- system time and date and related settings

Syntax

```
get system status
```

Example output

```
# get system status
Version: FortiSwitch-324B-POE v1.0,build0102,111125 (GA)
Serial-Number: FS324P3W11000005
BIOS version: 04000005
System Part-Number: P09835-01
Hostname: FS324P3W11000005
Distribution: International
Branch point: 102
Release Version Information: GA
System time: Mon Jan 30 11:27:15 2012
```

test

Use this command to display information about applications on this FortiSwitch:

Syntax

```
get test {acd | dnsproxy | fsd | radiusd | sflowd | snmpd} <test_level_int>
```

Variable	Description
{acd | dnsproxy | fsd | radiusd | sflowd | snmpd}	Set the application to be tested. Tests can be run on the following applications: <acd> Aggregate Controller <dnsproxy> dns proxy <fsd> FortiExplorer daemon <radiusd> radius daemon <sflowd> sflowd <snmpd> snmpd daemon
<test_level_int>	Set the level for the test.

user setting

Use this command to get information on all the system's user settings.

Syntax

```
get user setting
```

Example output

```
# get user setting
auth-blackout-time : 0
auth-cert : (null)
auth-http-basic : disable
auth-invalid-max : 5
auth-multi-group : enable
auth-ports:
auth-secure-http : disable
auth-timeout : 5
auth-timeout-type : idle-timeout
auth-type : http https ftp telnet
```