FortiController-5000 Series
CLI Reference for FortiSwitch-ATCA v5.2.3 build 166

FortiController-5913C

FortiController-5903C

FortiController-5103B

FortiController-5000 Series CLI Reference for FortiSwitch-ATCA v5.2.3 build 166

April 28, 2016

10-523-266433-20160428

Technical Documentation	docs.fortinet.com
FortiGate Cookbook	cookbook.fortinet.com
Video Library	video.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Contents

Change Log

Date	Description
28 April, 2016	Second version released on 28 April with more changes to the description of the `link-failure-threshold` option of the `config system ha` command and with changes to the `min-links` option of the `config switch fabric-channel trunk` command.
28 April, 2016	`pptp-mode` option added to `config load-balance protocol-pin` command. More information added and corrections made to the descriptions of the `max-miss-heartbeats` and `max-miss-mgmt-heartbeats` options of the `config load-balance settings` command. More speeds added to the `speed` option of the `config switch fabric-channel physical-port` command. Corrected the description of the `link-failure-threshold` option of the `config system ha` command.

Date	Description

2 March 2016	New version of this document for FortiSwitch-ATCA OS v5.2.3 build 166. This update to 5.2.3 includes the following changes:
	• Switch mode and load balance mode commands covered in this document. For FortiSwitch-ATCA OS v5.1.x we produced different documents for load balance mode and switch mode.
	• Corrected the `config loadbalance setting` description for "session-sync {disable | enable}" on page 22.
	New commands and command options added:
	`config load-balance session-setup`
	`  set gre-session {enable | disable}`
	`  set ipsec-session {disable | forward-to-master | load-balance}`
	`  set sctp-session {disable | enable}`
	
	`config load-balance setting`
	`  set board-init-holddown <delay>`
	`  set max-miss-mgmt-heartbeats <heartbeats>`
	`  set weight-load-balance {disable | enable}`
	`  set session-sync {disable | enable}`
	
	`config switch fabric-channel flow rule`
	
	`config system snmp user`
	
	`config system global`
	`  set admin-server-cert`
	
	`config switch fabric-channel trunk`
	`  edit trunkname`
	`  set min-links <number>`
	
	`config system ha`
	`  set l3-gateway-failure-failover-interval <time>`
	`  set link-failure-threshold <number>`
	`  set chassis-id {1 | 2}`
	`  set session-sync-port {disable | <interface-name>}`
	`  set board-failover-tolerance <number-of-workers>`
	`  set minimize-chassis-failover {disable | enable}`
	
	`execute user certificate`

Introduction

This manual describes the CLI commands for the FortiController-5000 Series products running FortiSwitch-ATCA OS v5.2.3 build 166:

- FortiController-5913C
- FortiController-5903C
- FortiController-5103B

Load balance mode and switch mode

FortiController-5000 Series products can operate in load balance mode and switch mode. This document describes the FortiController CLI commands and options available in load balance mode and in switch mode. Most of the commands and options described in this document are available in both modes. A note has been added to commands or options that are only available in one mode.

Load balance mode is the default. In this mode the FortiController-5000 Series products are configured for session-aware load balancing (SLBC), are installed in FortiGate-5000 series chassis slots 1 and 2, and distribute traffic to multiple workers installed in the chassis.

You can use the following command to change to switch mode:

```
config system global
  set load-balance disable
end
```

The FortiController restarts in switch mode and can operate as a fabric and base backplane switch in a FortiGate-5000 series chassis. In switch mode you can use one or two FortiControllers in chassis slots 1 and 2 to provide backplane communication between FortiGate-5000 series boards in chassis slots 2 to 14. You can also use switch mode to provide backplane switching to support FortiGate boards in the chassis operating as FGCP HA clusters.

From switch mode, you can use the following command to change to back to load balance mode:

```
config system global
  set load-balance enable
end
```

The FortiController restarts in load balance mode.

How this guide is organized

Most of the chapters in this document describe the commands for each configuration branch of the CLI. The command branches and commands are in alphabetical order.

This document contains the following chapters:

admin describes administrator commands.

load-balance describes SLBC load balancing commands.

log describes logging commands.

route describes routing commands.

switch describes base and fabric channel switch commands.

system describes system setting commands.

execute describes execute commands.

get describes get commands.

diagnose introduces some useful troubleshooting commands.

Connecting to the CLI

Connecting to and working with the FortiController-5000 Series CLI is the same as working with the FortiOS CLI. You can use a direct console connection, SSH, Telnet or the web-based manager to connect to the FortiController CLI. Using SSH or Telnet you connect to the CLI through the mgmt interface.

Connect to the FortiController console using the FortiController front panel console port. You need:

- a computer with an available communications port
- a null modem cable, with an RJ-45 connector as provided with your FortiController
- terminal emulation software such as HyperTerminal for Windows

Use the following port settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Setting administrative access on the mgmt interface

To perform administrative functions through a the FortiController mgmt network interface, you must enable the required types of administrative access. Access to the CLI requires SSH or Telnet access.

Use the following command to configure the mgmt interface to accept SSH connections:

```
config system interface
  edit mgmt
    set allowaccess ping ssh telnet
  end
```

To confirm that you have configured SSH or Telnet access correctly, enter the following command to view the access settings for the interface:

```
get system interface mgmt
```

The CLI displays the settings, including `allowaccess`, for the named interface:

```
name                 : mgmt
status               : up
ip                   : 172.20.120.178 255.255.255.0
allowaccess          : ping ssh telnet
```

Secure Shell (SSH) provides strong secure authentication and secure communications to the FortiSwitch-5003A CLI from your internal network or the internet. Once the FortiController is

configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiController CLI.

admin

Configure administrator settings. The following admin commands are available:

radius-server

user

radius-server

Use this command to configure access to a RADIUS authentication server.

Syntax

```
config admin radius-server
  edit <server-name-string>
    set auth-type {auto | auto-legacy | chap | ms_chap_v2 | pap}
    set port <port_integer>
    set secret <password>
    set server <ip_address>
  end
```

Variables	Description	Default
auth-type {auto | auto-legacy | chap | ms_chap_v2 | pap}	Select the authentication protocol used by the RADIUS server. `auto` and `auto` legacy cycles through multiple protocols.	1812
port <port_integer>	Enter the RADIUS port for this server. Range is 0 to 65535.	1812
secret <password>	Enter the RADIUS server shared secret. Maximum 16 characters.	
server <ip_address>	Enter the RADIUS server domain name or IP address.	

user

Use this command to add and configure administrator accounts.

Syntax

```
config admin user
   edit <userid>
      set description <description_str>
      set password <admin_password>
      set user-type {local | radius}
      set radius-server <server_str>
      set trusthost[1-50]
   end
```

Variables	Description	Default
description <description_str>	Describe the administrator account.	
password <admin_password>	Enter the password for this administrator. The password can be up to 19 characters. This is available if `user-type` is `local`.	
user-type {local | radius}	Specify how this user's password is verified using the local user database or a RADIUS server.	local
radius-server <server_str>	Enter the name of the RADIUS server (added using the `config admin radius-server` command) with which the administrator must authenticate.	
trusthost[1-50]	Specify the IP address and netmask of up to 50 trusted hosts that this administrator can login from.	0.0.0.0 0.0.0.0

load-balance

Configure load balancing settings. These commands are only available when the FortiController is operating in load balance mode. The following load balance commands are available:

protocol-pin

session-age

session-setup

setting

protocol-pin

Use this command to configure a FortiController to enable or disable load balancing BGP, PPTP, DHCP, IKE, Kerberos and RIP traffic. If a protocol is set to enable all of that protocol's traffic is handled by the primary worker. If set to disable the traffic is load balanced among all of the workers.

If your FortiController receives IKE or kerberos traffic on a non-standard port you can enable override for these protocols and select a different port.

Syntax

```
config load-balance protocol-pin
   set bgp-mode {disable | enable}
   set dhcp-mode {disable | enable}
   set ike-mode {disable | enable}
   set ike-natt-mode {disable | enable}
   set ike-override {disable | enable}
   set ike-override-port <port-number>
   set kerberos-mode {disable | enable}
   set kerberos-override {disable | enable}
   set kerberos-override-port <port-number>
   set pptp-mode {disable | enable}
   set rip-mode {disable | enable}
end
```

Variables	Description	Default
bgp-mode {disable | enable}	Enable to have all BGP traffic processed by the primary worker. Disable to load balance BGP traffic to all workers.	enable
dhcp-mode {disable | enable}	Enable to have all DHCP traffic processed by the primary worker. Disable to load balance DHCP traffic to all workers.	enable
ike-mode {disable | enable}	Enable to have all IKE traffic processed by the primary worker. Disable to load balance IKE traffic to all workers.	enable
ike-natt-mode {disable | enable}	Enable to have all IKE NAT Traversal (NATT) traffic processed by the primary worker.	
ike-override {disable | enable}	Enable to change the port number on which to expect IKE traffic.	disable
ike-override-port <port-number>	Specify the port number on which to expect IKE traffic. Available when ike-override is enabled.	500
kerberos-mode {disable | enable}	Enable to have all Kerberos traffic processed by the primary worker. Disable to load balance Kerberos traffic to all workers.	disable
kerberos-override {disable | enable}	Enable to change the port number on which to expect IKE traffic.	disable
kerberos-override-port <port-number>	Specify the port number on which to expect Kerberos traffic. Available when kerberos-override is enabled.	88

Variables	Description	Default
pptp-mode {disable | enable}	Enable to have all PPTP traffic processed by the primary worker. Disable to load balance PPTP traffic to all workers.	disable
rip-mode {disable | enable}	Enable to have all RIP traffic processed by the primary worker. Disable to load balance RIP traffic to all workers.	enable

session-age

Use this command to configure FortiController load balance session timers. In most cases you do not have to adjust these timers, but the timers are configurable for performance tuning. The timer range can be 1 to 15,300 seconds

Syntax

```
config load-balance session-age
   set fragment <age-interval>
   set pin-hole <age-interval>
   set rsync <age-interval>
   set tcp-half-close <age-interval>
   set tcp-half-open <age-interval>
   set tcp-normal <age-interval>
   set tcp-timewait <age-interval>
   set udp <age-interval>
end
```

Variables	Description	Default
fragment <age-interval>	Set the session age in seconds for fragmented sessions.	120
pin-hole <age-interval>	Set the session age in seconds for pinhole sessions.	120
rsync <age-interval>	Set the session age in seconds for rsync sessions.	300
tcp-half-close <age-interval>	Set the session age in seconds for tcp-half-close sessions.	125
tcp-half-open <age-interval>	Set the session age in seconds for tcp-half-open sessions.	125
tcp-normal <age-interval>	Set the session age in seconds for tcp-normal sessions.	3605
tcp-timewait <age-interval>	Set the session age in seconds for tcp-timewait sessions.	2
udp <age-interval>	Set the session age in seconds for udp sessions.	185

session-setup

Use this command to set the load balancing method that the FortiController uses to distribute traffic to workers. Also configure how fragmented packets, pinhole sessions, TCP and UDP ingress sessions, and UDP sessions are distributed.

Syntax

```
config load-balance session-setup
   set fragment {disable | hardware}
   set gre-session {disable | enable}
   set ipsec-session {disable | forward-to-master | load-balance}
   set load-distribution-method {round-robin | src-ip | dst-ip |
        src-dst-ip | src-ip-sport | dst-ip-dport |
        src-dst-ip-sport-dport}
   set sctp-session {disable | enable}
   set session-helper {disable | enable}
   set tcp-ingress {disable | enable}
   set udp-ingress {disable | enable}
   set udp-session {local | remote}
end
```

Variables	Description	Default
fragment {disable | hardware}	Disable if you don't want the cluster to load balance fragmented packets. If your cluster receives a significant amount of fragmented packets you can set this option to hardware to have the FortiASIC DP processors load balance sessions containing fragmented packets. Enabling this option could reduce performance. If you set the load balancing distribution method to one that does not use ports (for example, round-robin, src-ip, dst-ip, or src-dst-ip) fragment should be disabled.	disable
gre-session {disable | enable}	Enable or disable GRE load balancing.	disable
ipsec-session {disable | forward-to-master | load-balance}	Control how IPsec sessions are handled. You can forward all IPsec sessions to the primary worker (forward-to-master), load balance IPsec sessions to all workers (load-balance) or disable IPsec traffic.	forward-to-master
load-distribution-method {round-robin | src-ip | dst-ip | src-dst-ip | src-ip-sport | dst-ip-dport | src-dst-ip-sport-dport}	Set the method used by the FortiController to distribute sessions among workers. Usually you would only need to change the method if you had specific requirements or you found that the default method wasn't distributing sessions in the manner that you would prefer.	src-dst-ip-sport-dport
sctp-session {disable | enable}	Enable or disable SCTP load balancing.	disable
session-helper {disable | enable}	Enable or disable load balancing pinhole sessions.	enable

Variables	Description	Default
tcp-ingress {disable | enable}	Disable to have the FortiASIC DP processor only record TCP sessions that are accepted by worker firewall policies. The FortiASIC DP processor does not record denied sessions. This setting uses less load balancing resources but results in round-robin load balancing not being supported. Enable to have the FortiASIC DP processor record all TCP sessions, even sessions denied by worker firewall policies. This setting supports round-robin load balancing but uses more resources and results in the cluster being more vulnerable to DDOS attacks.	disable
udp-ingress {disable | enable}	Disable to have the FortiASIC DP processor only record UDP sessions that are accepted by worker firewall policies. The FortiASIC DP processor does not record denied sessions. This setting uses less load balancing resources but results in round-robin load balancing not being supported. Enable to have the FortiASIC DP processor record all UDP sessions, even sessions denied by worker firewall policies. This setting supports round-robin load balancing but uses more resources and results in the cluster being more vulnerable to DDOS attacks.	disable
udp-session {local | remote}	When set to remote, on egress UDP Packets are transmitted directly from the FortiController fabric backplane interface to the FortiController front panel interface, bypassing the FortiASIC DP processor. The workers update the FortiASIC DP processor UDP session table by sending worker-to-FortiController heartbeats. When set to local, both incoming and outgoing UDP sessions are forwarded by the FortiASIC DP processor; effectively doubling the number of UDP sessions that the FortiASIC DP processor handles. Doubling the session load on the FortiASIC DP processor can create a performance bottleneck. Set to local if you experience errors with UDP traffic.	remote

setting

Use this command to set a wide range of load balancer that control how management and control traffic is communicated as well as other settings.

Syntax

```
config load-balance setting
  set base-ctrl-interface-mode {active-active | active-passive}
    config base-ctrl-interfaces
      edit {b1 | b2}
        set vlanid <vlan-id>
  set base-ctrl-network <ip> <netmask>
  set base-mgmt-allowaccess <access-types>
  set base-mgmt-external-ip <ip> <netmask>
  set base-mgmt-interface-mode {active-active | active-passive}
    config base-mgmt-interfaces
      edit {b1 | b2}
        set vlanid <vlan-id>
  set base-mgmt-internal-fgfm-port <port-number>
  set base-mgmt-internal-http-port <port-number>
  set base-mgmt-internal-https-port <port-number>
  set base-mgmt-internal-mac
  set base-mgmt-internal-network <ip> <netmask>
  set base-mgmt-internal-snmp-port <port-number>
  set base-mgmt-internal-ssh-port <port-number>
  set base-mgmt-internal-telnet-port <port-number>
  set board-init-holddown <delay>
  set forticontroller-proxy {disable | enable}
  set forticontroller-proxy-port <port-number>
  set max-miss-heartbeats <heartbeats>
  set max-miss-mgmt-heartbeats <heartbeats>
  set nat-source-port {chassis-slots | running-slots}
  set session-sync {disable | enable}
    config slots
      edit <slot>
        set weight <weight>
  set standby-override {disable | enable}
    config traffic-interface
      edit <port>
        set port-mac-address <mac-address>
  set weighted-load-balance {disable | enable}
```

```
end
```

Variables	Description	Default
base-ctrl-interface-mode {active-active | active-passive}	Control how the b1 and b2 interfaces are used for base control communication between chassis. Active-passive means that b1 is used and b2 is on standby. If b1 becomes disconnected, management traffic fails over to b2. Active-active means that both b1 and b2 are used at the same time.	active-passive
config base-ctrl-interfaces	Change the VLAN ID used for base control communication between chassis.	
base-ctrl-network <ip> <netmask>	Change the base control IP address and netmask.	10.101.11.0 255.255.255.0
vlanid <vlan-id>	Change the VLAN ID used for base control communication between chassis.	301
base-mgmt-allowaccess <access-types>	Set the types of management access allowed for the external management IP address. Options include: fgfm (FortiManager), http, https, ping, snmp, ssh, and telnet.	
base-mgmt-external-ip <ip> <netmask>	Set the external management IP address and netmask.	192.168.1.101 255.255.255.0
base-mgmt-interface-mode {active-active | active-passive}	Control how the b1 and b2 interfaces are used for base management communication between chassis. Active-passive means that b1 is used and b2 is on standby. If b1 becomes disconnected, management traffic fails over to b2. Active-active means that both b1 and b2 are used at the same time.	active-passive
config base-mgmt-interfaces	Change the VLAN ID used for management communication between chassis.	
vlanid <vlan-id>	Change the VLAN ID used for management communication between chassis.	101
base-mgmt-internal-fgfm-port <port-number>	Set the port number used for FortiManager traffic on the internal management network.	541
base-mgmt-internal-http-port <port-number>	Set the port number used for HTTP traffic on the internal management network.	80
base-mgmt-internal-https-port <port-number>	Set the port number used for HTTPS traffic on the internal management network.	443
base-mgmt-internal-mac	Set the MAC address for internal management communication on the base channel.	00:09:0f:9c:6b:23
base-mgmt-internal-network <ip> <netmask>	Set the subnet used for internal management communication on the base channel.	10.101.10.0 255.255.255.0
base-mgmt-internal-snmp-port <port-number>	Set the port number used for SNMP traffic on the internal management network.	161
base-mgmt-internal-ssh-port <port-number>	Set the port number used for SSH traffic on the internal management network.	22

Variables	Description	Default
base-mgmt-internal-telnet-port <port-number>	Set the port number used for telnet traffic on the internal management network.	23
board-init-holddown <delay>	Set the delay in seconds before assuming a worker is ready for traffic after being added to a cluster. Range is 0 to 1200 seconds.	0
forticontroller-proxy {disable | enable}	Enable the FortiController proxy to support IPsec VPN. To support IPsec VPN, workers send static route information of tunnel interfaces to the FortiController and this communication is handled by the forticontroller-proxy. The forticontroller-proxy also enables automatic failover to other chassis after worker firmware updates are complete.	disable
forticontroller-proxy-port <port-number>	Configure the UDP port used by the FortiController proxy.	11133
max-miss-heartbeats <heartbeats>	Set the number of missed heartbeats before a worker is considering to have failed. If this many heartbeats are not received from a worker, this indicates that the worker is not able to process data traffic and no more traffic will be sent to this worker. The time between heartbeats is 0.2 seconds. Range is 3 to 300. 3 means 0.6 seconds, 10 means 2 seconds, and 300 means 60 seconds.	10
max-miss-mgmt-heartbeats <heartbeats>	Set the number of missed management heartbeats before a worker is considering to have failed. If a management heartbeat fails, there is a communication problem between a worker and other workers. This communication problem means the worker may not be able to synchronize configuration changes, sessions, the kernel routing table, the bridge table and so on with other workers. If a management heartbeat failure occurs, no traffic will be sent to the worker. The time between managment heartbeats is 1 second. Range is 3 to 300 seconds.	20
nat-source-port {chassis-slots | running-slots}	Set how the 64K NAT source port number ranges are distributed. chassis-slots distributes the port numbers evenly among all chassis slots. running-slots distributes the port numbers among the slots that are configured to contain workers (using the config slots command). running-slots provides more port numbers per slot if the chassis is not full. However, if you have selected running-slots traffic may be lost if you install a new worker while the cluster is operating.	chassis-slots
session-sync {disable | enable}	For an SLBC of two chassis, enable to synchronize sessions between workers in the same slots in each chassis. For example, the worker in chassis1 slot3 is synchronized with the worker in chassis2 slot3). After a failover the cluster attempts to maintain existing sessions on the workers in the new chassis.	disable

Variables	Description	Default
config slots	Select the chassis slots that contain workers and set the weights for chassis slots 3 to 14. Edit a slot to add it to the cluster. Optionally change the slot weight to send more traffic to that slot of `weighted-load-balance` is enabled.	
weight <weight>	Set the weight for a chassis slot. Range is 1 to 10. 5 is average, 1 is -80% of average and 10 is +100% of average. The weights take effect if `weighted-load-balance` is enabled.	5
standby-override {disable | enable}	Enable to allow active workers to immediately replace running standby units.	disable
config traffic-interface	Change the MAC address of a FortiController front panel interface. All workers should be using the same MAC address for the same data port. This command sets that MAC address and allows you to change it.	
port-mac-address <mac-address>	Change the MAC address of a FortiController front panel interface. All workers should be using the same MAC address for the same data port. This command sets that MAC address and allows you to change it.	
weighted-load-balance {disable | enable}	Enable weighted load balancing depending on the slot weight. Use the `config slot` command to set the weight for each slot.	disable

log

Configure sending log messages to up to three syslog servers. The following logging commands are available:

{syslogd | syslogd2 | syslogd3} filter

{syslogd | syslogd2 | syslogd3} setting

{syslogd | syslogd2 | syslogd3} filter

Use this command to enable or disable sending event log messages to a syslog server. You can select the event log messages that are sent and the minimum severity of the messages that are sent.

Syntax

```
config log {syslogd | syslogd2 | syslogd3} filter
     set event {disable | enable}
     set severity {alert | critical | debug | emergency | error |
          information | notification | warning}
     set base-switch-config {disable | enable}
     set base-switch-general {disable | enable}
     set base-switch-trunk {disable | enable}
     set fabric-switch-config {disable | enable}
     set fabric-switch-general {disable | enable}
     set fabric-switch-stp {disable | enable}
     set fabric-switch-trunk {disable | enable}
     set system-config {disable | enable}
     set system-general {disable | enable}
   end
```

Variables	Description	Default
event {disable | enable}	Enable or disable sending event log messages to this syslog server. If set to enable you can enable or disable sending individual event log messages.	disable
severity {alert | critical | debug | emergency | error | information | notification | warning}	Set the lowest severity for which to send log messages.	information
base-switch-config {disable | enable}	Send an event log message when the base switch configuration is changed.	disable
base-switch-general {disable | enable}	Send an event log message for base switch events.	disable
base-switch-trunk {disable | enable}	Send an event log message for base switch trunk membership changes.	disable
fabric-switch-config {disable | enable}	Send an event log message for fabric switch configuration changes.	disable
fabric-switch-general {disable | enable}	Send an event log message for general fabric switch events.	disable
fabric-switch-stp {disable | enable}	Send an event log message for fabric switch STP changes.	disable
fabric-switch-trunk {disable | enable}	Send an event log message for fabric switch trunk membership changes.	disable
system-config {disable | enable}	Send an event log message for non-switch configuration changes.	disable
system-general {disable | enable}	Send an event log message for general system changes.	disable

{syslogd | syslogd2 | syslogd3} setting

Use this command to enable logging to up to three syslog servers. If you enable logging to a syslog server you can specify the server address, port number, syslog message format, and set the syslog facility.

Syntax

```
config log {syslogd | syslogd2 | syslogd3} filter
     set status {disable | enable}
     set server <address_ipv4 | fqdn>
     set port <port>
     set csv {disable | enable}
     set facility <type>
   end
```

Variables	Description	Default
status {disable | enable}	Enable or disable sending log messages to this syslog server.	disable
server <address_ipv4 | fqdn>	Enter the IP address of the syslog server that stores the logs.	(null)
port <port>	Enter the port number for communication with the syslog server.	514
csv {disable | enable}	Enable to send log messages in comma separated value (CSV) format.	disable
facility <type>	Enter the facility type. The facility type identifies the source of the log message. You might want to change the facility to distinguish log messages from different FortiControllers. Enter ? to see the available facility types.	local7

route

Configure static routes for management interfaces. The following routing command is available:

static

static

Use this command to add, edit, or delete static routes for management interfaces (for example mgmt or base-mgmt).

Syntax

```
config route static
  edit <sequence_number>
    set device <interface>
    set dst <destination-address_ipv4mask>
    set gateway <gateway-address_ipv4>
  end
```

Variables	Description	Default
edit <sequence_number>	Enter a sequence number to identify the static route.	No default.
device <interface>	The name of the management interface for which to add a static route.	`mgmt`
dst <destination-address_ipv4mask>	Enter the destination IP address and network mask for this route. You can enter `0.0.0.0 0.0.0.0` to create a default route.	0.0.0.0 0.0.0.0
gateway <gateway-address_ipv4>	Enter the IP address of the next-hop router to which traffic is forwarded by this route.	0.0.0.0

switch

Configure base channel and fabric channel switch settings. Many of these commands are available in switch mode only. The following switch commands are available:

base-channel global
base-channel interface
base-channel mirror
base-channel physical-port
base-channel trunk
domain
fabric-channel flow-rule
fabric-channel global
fabric-channel interface
fabric-channel mirror
fabric-channel physical-port
fabric-channel stp instance
fabric-channel stp settings
fabric-channel trunk
port-extension

base-channel global

Use this command to configure global settings for the base-channel switch interfaces. This command is available in switch mode only.

Syntax

```
config switch base-channel global
   set dtag-mode {disabled | enable-external | enable-internal}
   set name <name_string>
end
```

Variables	Description	Default
dtag-mode {disabled | enable-external | enable-internal}	Enable and set default double-tagging support on the base channel switch ports. enable-external all base channel ports default to customer (UNI) ports. enable-internal all base channel ports default to service provider (NNI) ports. If you enable global default double-tagging you can override double-tagging for individual base channel interfaces.	disabled
mac-aging-interval <time>	Set the MAC address aging interval for the base channel interfaces. The range is 1 to 1000000 seconds. 0 to disable.	0
name <name_string>	Enter a name for the base channel switch.	No default.

base-channel interface

Use this command to configure settings for individual base-channel switch interfaces. This command is available in switch mode only.

Syntax

```
config switch base-channel interface
  edit <interface_name>
    set allowed-vlans <id_numbers>
    set dtag-mode {external | internal}
    set native-vlan <id_number>
  end
```

Variables	Description	Default
allowed-vlans <id_numbers>	Specify the IEEE 802.1Q VLAN IDs that can be added to VLAN-tagged packets that this interface can receive and transmit. Packets tagged with other VLAN IDs are dropped by the interface. Untagged packets are not affected. You can enter any combination of single VLAN IDs and ranges of VLAN IDs. Use a hyphen to specify ranges. Separate each single ID or range with a comma. Do not include spaces. For example: `1,3-4,6,7,9-100`.	No default.
dtag-mode {external | internal}	Set the double-tagging mode for this interface. external for customer (UNI) port. internal for service provider (NNI) port. This command is available if global double-tagging has been enabled using the config switch base-channel global command.	internal
native-vlan <id_number>	Change the IEEE 802.1Q native VLAN ID for this interface. Packets tagged with the native VLAN ID are not modified when sent or received by the interface. If an untagged packet is received by the interface, the packet is tagged with the native VLAN ID.	1

base-channel mirror

Use this command to configure a base channel mirror interface. When you add a destination interface, traffic on all switch base channel interfaces is mirrored to that interface and the destination interface can no longer be used as a switch interface. You can use the other parameters of this command to limit the traffic mirrored to the destination interface, enable using the mirror interface as a switch interface, and activate or deactivate mirroring on the destination interface. This command is available in switch mode only.

Syntax

```
config switch base-channel mirror
  set dst <interface_name>
  set src-egress <interface_name>
  set src-ingress <interface_name>
  set status {active | inactive}
  set switching-packet {enable | disable}
end
```

Variables	Description	Default
dst <interface_name>	Select the mirror interface. All base channel traffic will be mirrored to this interface.	No default.
src-egress <interface_name>	Specify switch interfaces for which you only want to mirror base channel egress traffic. Separate interface names with a space.	No default.
src-ingress <interface_name>	Specify switch interfaces for which you only want to mirror base channel ingress traffic. Separate interface names with a space.	No default.
status {active | inactive}	Set the mirror interface to be active or inactive.	inactive
switching-packet {enable | disable}	Enable or disable being able to use the mirror interface as a switch interface when mirroring.	disable

base-channel physical-port

Use this command to change the maximum frame size, speed and status (up or down) of a base channel interface.

Syntax

```
config switch base-channel physical-port
  edit <interface_name>
    set description <description_str>
    set max-frame-size <integer>
    set status {up | down}
    set speed <speed>
  end
```

Variables	Description	Default
description <description_str>	Optionally, enter a description.	
max-frame-size <integer>	Set the maximum frame size. Range depends on the hardware.	hardware dependant
status {up | down}	Set the port as active (up) or disabled (down).	up
speed <speed>	Set the speed of the base channel interface. Not available for all interfaces. The options available and the default depends on the hardware but can include, 10000full, 1000auto, and 1000full.	hardware dependant

base-channel trunk

Use this command to configure trunks. This command is available in switch mode only.

Syntax

```
config switch base-channel trunk
  edit <trunk_name>
    set description <description_str>
    set members <interface_names>
    set port-selection-criteria {dst-ip | src-dst-ip | src-ip}
  end
```

Variables	Description	Default
edit <trunk_name>	Enter the name of a trunk to add or edit. This trunk name appears in base channel interface list.	
description <description_str>	Optionally, enter a description.	
members <interface_names>	Enter the names of the base channel interfaces that are part of this trunk. Separate names with spaces.	No default.
port-selection-criteria {dst-ip | src-dst-ip | src-ip}	Set the algorithm for aggregate port selection. You can choose dst-ip, src-dst-ip, or src-ip.	src-dst-ip

domain

Use this command to configure a switch domain. The default domain is named root.

A switch domain is similar to a virtual switch, but is not a true virtual switch because the MAC table is shared globally. This command is available in switch mode only.

Syntax

```
config switch domain
  edit <domain_name>
    set ha-block {blade-ports misc-ports monitor-ports}
    set ha-L2-clear-on-role-change {blade-ports misc-ports
        monitor-ports}
    set inter-front-panel-traffic {enable | disable}
    set priority <priority_int>
    set vcluster-id <id_int>
  end
```

Variables	Description	Default
edit <domain_name>	Enter the domain name.	
ha-block {blade-ports misc-ports monitor-ports}	Select port types to be blocked if domain becomes an HA slave: • blade-ports — block blade ports • misc-ports — block ports that aren't monitor or blade ports • monitor-ports — block monitor ports	blade-ports misc-ports monitor-ports
ha-L2-clear-on-role-change {blade-ports misc-ports monitor-ports}	Select port types that have their L2 tables cleared when changing HA roles: • blade-ports — block blade ports • misc-ports — block ports that aren't monitor or blade ports • monitor-ports — block monitor ports	None selected.
inter-front-panel-traffic {enable | disable}	Enable or disable front panel port to front panel port traffic.	enable
priority <priority_int>	Set the priority (0-255). This is used to decide the FortiController's HA role if HA is enabled.	128
vcluster-id <id_int>	Enter the HA virtual cluster id (1-255).	0

fabric-channel flow-rule

Use this command to add flow rules that add exceptions to how matched traffic is processed by an SLBC cluster. Specifically you can use these rules to match a type of traffic and control whether the traffic is forwarded or blocked. And if the traffic is forwarded you can specify whether to forward the traffic to a specific worker or to all workers.

One common use of this command is to control how traffic that is not load balanced is handled. For example, use the following command to send all GRE traffic to the worker in slot 8. In this example the GRE traffic is received by FortiController front panel ports F1 nd F5:

```
config switch fabric-channel flow-rule
  edit 0
    set src-interface f1 f5
    set ether-type ip
    set protocol gre
    set action forward
    set forward-slot 8
end
```

Syntax

```
config switch fabric-channel flow-rule
  edit 0
    set src-interface <interface-name>
    set vlan <vlan-id>
    set ether-type {any | arp | ip | ipv4}
    set src-addr-ipv4 <ip-address> <netmask>
    set dst-addr-ipv4 <ip-address> <netmask>
    set protocol {any | icmp | tcp | udp | igmp | sctp | gre | esp |
        ah | ospf | pim | vrrp}
    set action {drop | forward | stats}
    set forward-slot <number>
    set priority <number>
    set comment <text>
end
```

Variables	Description	Default
src-interface <interface-name>	The names of one or more FortiController front panel interfaces accepting the traffic to be subject to the flow rule.	
vlan <vlan-id>	If the traffic matching the rule is VLAN traffic, enter the VLAN ID used by the traffic.	0
ether-type {any | arp | ip | ipv4}	Specify the type of traffic to be matched by the rule. You can match any traffic or just match ARP, IP, or IPv4 traffic.	any
src-addr-ipv4 <ip-address> <netmask>	If `ether-type` is set to `ipv4`, specify the source address of traffic to match the rule. The default matches all traffic.	0.0.0.0 0.0.0.0
dst-addr-ipv4 <ip-address> <netmask>	If `ether-type` is set to `ipv4`, specify the destination address of traffic to match the rule. The default matches all traffic.	0.0.0.0 0.0.0.0

Variables	Description	Default
protocol {any | icmp | tcp | udp | igmp | sctp | gre | esp | ah | ospf | pim | vrrp}	If `ether-type` is set to `ipv4` or `ip` specify the protocol of the IP or IPv4 traffic to match the rule.	any
action {drop | forward | stats}	How to handle matching packets. They can be dropped, forwarded to another destination or you can record statistics about the traffic for later analysis. You can combine two or three settings in one command for example you can set action to both `forward` and `stats` to forward traffic and collect statistics about it.	forward
forward-slot <number>	Specify the slot number of the worker that you want to forward the traffic to in the range 3 to 14. Specify slot 0 to forward traffic to the ELBC master. Specify slot 1 to forward traffic to all workers (slots 3 to 14).	0
priority <number>	Set the priority of the flow rule in the range 1 (highest priority) to 10 (lowest priority). Higher priority rules are matched first. You can use the priority to control which rule is matched first if you have overlapping rules.	5
comment <text>	Optionally add a comment that describes the rule.	

fabric-channel global

Use this command to configure global settings for the fabric-channel switch interfaces. This command is available in switch mode only.

Syntax

```
config switch fabric-channel global
   set src-interface <interface-name>
   set vlan <vlan-id>
   set ether-type {any | arp | ip | ipv4}
end
```

Variables	Description	Default
dtag-mode {disabled | enable-external | enable-internal}	Enable and set default double-tagging support on the fabric channel switch ports. enable-external all fabric channel ports default to customer (UNI) ports. enable-internal all fabric channel ports default to service provider (NNI) ports. If you enable global default double-tagging you can override double-tagging for individual fabric channel interfaces.	disabled
mac-aging-interval <time>	Set the MAC address aging interval for the fabric channel interfaces. The range is 1 to 1000000 seconds. 0 to disable.	0
name <name_string>	Enter a name for the fabric channel switch.	No default.

fabric-channel interface

Use this command to configure the VLANs allowed on fabric channel interfaces. You can also change the native VLAN for each interface and disable or enable MSTP for each interface. This command is available in switch mode only.

Syntax

```
config switch fabric-channel interface
  edit <interface_name>
    set native-vlan <id_number>
    set allowed-vlans <id_numbers>
    set stp-state {disable | enable}
    set edge-port {disable | enable}
  end
```

Variables	Description	Default
edit <interface_name>	Enter the name of the fabric channel interface or trunk to configure. You cannot edit an interface that has been added to a trunk.	
native-vlan <id_number>	Change the IEEE 802.1Q native VLAN ID for this interface. Packets tagged with the native VLAN ID are not modified when sent or received by the interface. If an untagged packet is received by the interface, the packet is tagged with the native VLAN ID.	1
allowed-vlans <id_numbers>	Specify the IEEE 802.1Q VLAN IDs that can be added to VLAN-tagged packets that this interface can receive and transmit. Packets tagged with other VLAN IDs are dropped by the interface. Untagged packets are not affected. You can enter any combination of single VLAN IDs and ranges of VLAN IDs. Use a hyphen to specify ranges. Separate each single ID or range with a comma. Do not include spaces. For example: `1,3-4,6,7,9-100`.	
stp-state {disable | enable}	Enable or disable Multi-Spanning Tree Protocol (MSTP) for this interface. If MSTP is disabled you cannot use this interface in MSTP configurations.	enable
edge-port {disable | enable}	Enable if the port is connected to a LAN segment that does not have any bridge connected to it.	disable

fabric-channel mirror

Use this command to configure a fabric channel mirror interface. When you add a destination interface, traffic on all fabric channel switch interfaces is mirrored to that interface and the destination interface can no longer be used as a switch interface. You can use the other parameters of this command to limit the traffic mirrored to the destination interface, enable using the mirror interface as a switch interface, and activate or deactivate mirroring on the destination interface. This command is available in switch mode only.

Syntax

```
config switch fabric-channel mirror
  set dst <interface_name>
  set src-egress <interface_name>
  set src-ingress <interface_name>
  set status {active | inactive}
  set switching-packet {enable | disable}
end
```

Variables	Description	Default
dst <interface_name>	Select the mirror interface. All fabric channel traffic will be mirrored to this interface.	No default.
src-egress <interface_name>	Specify switch interfaces for which you only want to mirror fabric channel egress traffic. Separate interface names with a space.	No default.
src-ingress <interface_name>	Specify switch interfaces for which you only want to mirror fabric channel ingress traffic. Separate interface names with a space.	No default.
status {active | inactive}	Set the mirror interface to be active or inactive.	inactive
switching-packet {enable | disable}	Enable or disable being able to use the mirror interface as a switch interface when mirroring.	disable

fabric-channel physical-port

Use this command to change the maximum frame size, speed and status (up or down) of a fabric channel interface. This command also displays the link status and port index of each fabric channel interface.

Syntax

```
config switch fabric-channel physical-port
  edit <interface_name>
    set descriptionAAAA <description_str>
    set domain <domain-name>
    set max-frame-size <integer>
    set status {up | down}
    set speed <speed>
  end
```

Variables	Description	Default
descriptionAAAA <description_str>	Optionally, enter a description.	
domain <domain-name>	Add the interface to a domain. You configure domains use the config switch domain command. The default domain is root.	
max-frame-size <integer>	Set the maximum frame size. Range depends on the hardware.	hardware dependant
status {up | down}	Set the port as active (up) or disabled (down).	up
speed <speed>	Set the speed of the fabric channel interface. Not available for all interfaces. The options available and the default depends on the hardware but can include, 40000full, 10000full, 1000auto, and 1000full.	hardware dependant

fabric-channel stp instance

Use this command to add and configure 802.1s Multi-Spanning Tree Protocol (MSTP) spanning tree instances. A spanning tree instance consists of the following:

- An instance ID
- A priority value
- A VLAN range
- A cost and priority value for each FortiSwitch-5003A interface

This command is available in switch mode only.

Syntax

```
config switch fabric-channel stp instance
  edit <instance_id>
    set priority <priority_value>
    set vlan-range <id_numbers>
    config stp-port
      edit <interface_name>
      set cost <cost_int>
      set priority <priority_value>
      end
  end
```

Variables	Description	Default
edit <instance_id>	Enter a numeric spanning tree instance number in the range 0 to 15. All devices participating in an MSTP region must have the same spanning tree instances. The default configuration includes spanning tree instance 0 that has a <priority_value> of 32768 and does not include a vlan-range setting. The stp-port configuration of spanning tree instance 0 sets the cost of all FortiSwitch-5003A interfaces to 0 and the priority of all interfaces to 128.	
priority <priority_value>	The priority value of the spanning tree instance. MSTP regions include multiple devices with the same spanning tree instances. The different priority values of the same instances on different devices determines how spanning tree routes packets to the different devices. The device with the spanning tree instance with the lowest priority value is more likely to be the root device and to process all packets. The <priority_value> range is 0 to 61440 in increments of 4096. Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.	32768

Variables	Description	Default
vlan-range <id_numbers>	Specify the IEEE 802.1Q VLAN IDs that can be added to VLAN-tagged packets that this spanning tree instance can receive and transmit. Only packets with these VLAN IDs are affected by this spanning tree instance. You can enter any combination of single VLAN IDs and ranges of VLAN IDs. Use a hyphen to specify ranges. Separate each single ID or range with a comma. Do not include spaces. For example: `1,3-4,6,7,9-100`. This is not available in instance 0.	No default.
config stp-port variables		
edit <interface_name>	Enter the name of the FortiSwitch-5003A fabric channel interface to configure. You cannot edit an interface that has been added to a trunk. Edit the interface to change its spanning tree cost and priority.	
cost <cost_int>	Enter the cost for the FortiSwitch-5003Ainterface in the range from 1 to 200000000. Spanning tree selects the interface with the lowest cost. Suggested values for different interface speeds: • 10 Mbps: 20000000 • 100 Mbps: 200000 • 1 Gbps: 20000 • 10 Gbps: 2000	0
priority <priority_value>	The priority value of the FortiSwitch-5003A interface in the spanning tree instance. Spanning tree selects the interface with the lowest priority. The `<priority_value>` range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240.	128

fabric-channel stp settings

Use this command to change MSTP spanning tree timers, specify an MSTP region name and use a revision number to track changes to the MSTP configuration. All of these MSTP settings should be the same on all of the devices in an MSTP region. These settings apply to all MSTP instances added to a FortiController. This command is available in switch mode only.

Syntax

```
config switch fabric-channel stp settings
   set forward-time <delay_time_int>
   set hello-time <hello_time_int>
   set max-age <age_time_int>
   set max-hops <hops_int>
   set name <name_str>
   set revision <number_str>
   set status {enable | disable}
   end
```

Variables	Description	Default
forward-time <delay_time_int>	The MSTP forward delay time in seconds. The forward delay time is the number of seconds that spanning tree spends in the listening and learning state. The range is 4 to 30 seconds.	15
hello-time <hello_time_int>	Enter the time between sending bridge protocol data units (BPDUs). The range is 1 to 10 seconds.	2
max-age <age_time_int>	The max age timer controls the maximum length of time in seconds that passes before a device saves its configuration BPDU information. The range is 6 to 40 seconds.	20
max-hops <hops_int>	The maximum number of hops in a MSTP region. The range is 1 to 40. The root bridge sends BPDUs with the hop count set to this maximum value. When a device receives a BPDU, it decrements the remaining hop count by one and includes this lower hop count in its BPDUs. When a device receives a BPDU with a hop count of zero, the device discards the BPDU.	20
name <name_str>	Enter a region name for the spanning tree configuration. The name is optional. All devices in the same MSTP region should have the same name. The region name is added to BPDUs.	
revision <number_str>	Enter a revision number of up to 4 digits. All devices in an MSTP region must have the same revision number. Change the revision number manually whenever you change the MSTP configuration. You can use the revision number to keep track of changes in the MSTP configuration and to help confirm that the MSTP configurations of all of the devices in a region are in sync.	0
status {enable | disable}	Enable or disable spanning tree protocol.	enable

fabric-channel trunk

Use this command to create a trunk and add FortiController interfaces to the trunk. You use trunks to group FortiController interfaces so that you can use 802.3ad static mode layer-2 link aggregation or LACP to distribute sessions to the fabric interfaces of the FortiGates connected to the FortiController interfaces in the trunk.

This command includes the `min-links` option that can be used to determine how many links in the trunk can fail before the trunk itself fails.

You can also use the following command to determine if an entire SLBC cluster should failover if links in an LCAP trunk fail:

```
config system ha
  set link-failure-threshold <number>
end
```

Syntax

```
config switch fabric-channel trunk
  edit <trunk_name>
    set description <string>
    set member-withdrawal-behavior {block | forward}
    set members <interface_names>
    set mode {fortinet-trunk | lacp-active | lacp-passive | static}
    set min-links <number>
    set port-selection-criteria {dst-ip | src-dst-ip | src-ip}
  end
```

Variables	Description	Default
description <string>	Optionally, enter a description.	
member-withdrawal-behavior {block | forward}	Set how an interface behaves after it withdraws because of loss of control packets. You can set the interfaces to block traffic or to continue to forward traffic.	block
members <interface_names>	Enter the names of the fabric channel interfaces that are part of this trunk. Separate names with spaces.	
mode {fortinet-trunk | lacp-active | lacp-passive | static}	Configure the trunk mode: • fortinet-trunk — use heartbeat packets to negotiate Fortinet aggregation • lacp-active — actively use LACP to negotiate 802.3ad aggregation • lacp-passive — passively use LACP to negotiate 802.3ad aggregation • static — use static aggregation, do not send and ignore any control messages	static

Variables	Description	Default
min-links <number>	Specify the minimum number of links in this `lacp-active` or `lacp-passive` trunk that must be up for the trunk to be up. You can use this option to keep a trunk from going down if the trunk can continue to process traffic as required when one or more interfaces in the trunk fails or is disconnected. The `min-links` option is commonly used in an LACP trunk that is being used for redundancy. For example, an LACP trunk could have two physical interfaces and if one interface goes down the remaining interface can still process sufficient traffic. In this case you would set `min-links` to 1. If an LACP trunk with two interfaces is used to improve bandwidth capacity and will normally process more traffic than can be handled by one interface then set min-links to 2 to indicate that the LACP trunk requires a minimum of two interfaces to function as required. The range is 0 to 8. Setting `min-links` to 0 disables this feature and the LACP trunk will be up as long as at least one of the interfaces in it has not failed.	0
port-selection-criteria {dst-ip | src-dst-ip | src-ip}	Set the load balancing algorithm used to distribute traffic to the interfaces in the trunk. You can choose `dst-ip`, `src-dst-ip`, or `src-ip`.	src-dst-ip

port-extension

Set port extension attributes. Use the following command to enable port extension mode:

```
config system global
  set port-extension enable
end
```

This command is available in switch mode only.

Syntax

```
config switch port-extension
  set px-auto-recovery {auto | manual}
  set px-weight-trigger <threshold>
  set remote-port-extension {disable | enable}
  set px-remote-alt-ip <address>
  set px-remote-ip <address>
end
```

Variables	Description	Default
px-auto-recovery {auto | manual}	Set the port extension recovery method.	auto
px-weight-trigger <threshold>	Set the port extension weight trigger threshold. Range is 100 to 1000.	100
remote-port-extension {disable | enable}	Enable remote port extension.	disable
px-remote-alt-ip <address>	Specify an alternate remote port extension IP address.	0.0.0.0
px-remote-ip <address>	Specify a remote port extension IP address.	0.0.0.0

system

Configure system settings. The following system commands are available:

central-management

dns

global

ha

interface

ntp

snmp community

snmp sysinfo

snmp user

central-management

Use this command to configure central management of a FortiController using FortiManager.

Syntax

```
config system cental-management
   set allow-monitor {enable | disable}
   set enc-algorithm {default | high | low}
   set fmg <fmg_ipv4>
   set fmg-source-ip <address>
   set mode {backup | normal}
   set serial-number <sn_string>
   set status {enable | disable}
end
```

Variables	Description	Default
allow-monitor {enable | disable}	Enable or disable remote management.	enable
enc-algorithm {default | high | low}	Set the SSL communication encryption algorithms to use for management communication. Default uses high and medium encryption algorithms, high uses high encryption algorithms and low uses low encryption algorithms.	default
fmg <fmg_ipv4>	Enter the IP address fully-qualified domain name of the FortiManager unit to be used for central management.	No default.
fmg-source-ip <address>	Enter a source address to use with communicating with FortiManager. Used if FortiManager is expecting a specific source address.	0.0.0.0
mode {backup | normal}	Change the backup mode.	normal
serial-number <sn_string>	Enter up to 5 FortiManager unit serial numbers. Only these FortiManagers can managed this FortiController.	No default.
status {enable | disable}	Enable or disable central management.	enable

dns

Use this command to configure the DNS servers used by the FortiController.

Syntax

```
config system dns
   set domain <name_str>
   set primary <ip_address>
   set secondary <ip_address>
end
```

Variables	Description	Default
domain <name_str>	Enter the local domain name	example.com
primary <ip_address>	Enter the primary DNS server IP address.	65.39.139.53
secondary <ip_address>	Enter the secondary DNS server IP address.	65.39.139.63

global

Use this command to configure a collection of global system parameters.

Syntax

```
config system global
   set access-banner {disable | enable}
   set admin-lockout-duration <time>
   set admin-lockout-threshold <threshold>
   set admin-server-cert <certificate_name>
   set admintimeout <timeout_integer>
   set banner-message <message>
   set chassis-type {fortigate-5050 | fortigate-5060 | fortigate-5140
        | fortigate-5144}
   set daylightsavetime {disable | enable}
   set hostname <hostname>
   set load-balance {disable | enable}
   set port-extension {disable | enable}
   set pre-login-banner {disable | enable|
   set pre-login-banner-message <message>
   set service-group-hash-size {normal | expanded}
   set service-group-mode {disable | basic | 2-port-lag | 4-port-lag}
   set service-group-snmp-community <name>
   set strong-crypto {enable | disable}
   set timezone <timezone_number>
end
```

Variables	Description	Default
access-banner {disable | enable}	Enable to display an admin access disclaimer message prior to logging into the CLI. Use the banner-message command to create the message. Administrators must indicate they accept the message before they can log into the CLI.	disable
admin-lockout-duration <time>	Set the administration account's lockout duration in seconds. Repeated failed login attempts will enable the lockout.	60
admin-lockout-threshold <threshold>	Set the threshold, or number of failed attempts, before the account is locked out for the admin-lockout-duration.	3

Variables	Description	Default
admin-server-cert <certificate_name>	Select the server certificate to be used for HTTPS management access to the FortiController. The default Fortinet_Factory certificate key strength is 1024 bits. You can use this option to select a certificate with higher key strength. Before you can select a certificate you must use the `execute user certificate upload` command to install the certificate on the FortiController. For security reasons, certificates are not synchronized between FortiControllers. So you need to upload the certificate to each FortiController in an SLBC cluster.	
admintimeout <timeout_integer>	Set the time-out for system administration sessions. The range is 1-480 minutes (8 hours).	5
banner-message <message>	Enter the admin access disclaimer message that appears before administrators can log into the CLI. Enabled by the access-banner command.	
chassis-type {fortigate-5050 | fortigate-5060 | fortigate-5140 | fortigate-5144}	Select the type of chassis that the FortiController is installed in. Select the type of chassis to make sure the FortiController looks for the correct number of slots and the correct hardware architecture.	fortigate-5140
daylightsavetime {disable | enable}	Enable or disable daylight saving time. If you enable daylight saving time, the FortiController adjusts the system time when the time zone changes to daylight saving time and back to standard time.	enable
hostname <hostname>	Enter a name to identify this FortiController.	serial number
load-balance {disable | enable}	Enable or disable load balance mode. If you disable load balance mode the FortiController operates in switch mode and can provide backplane fabric and base backplane switching.	enable
port-extension {disable | enable}	Enable or disable port extension mode. Use the config switch port-extension command to configure port extension. Available in switch mode only.	disable
pre-login-banner {disable | enable|	Enable to display an admin access disclaimer message prior to logging into the GUI. Use the pre-login-banner-message command to create the message. Administrators must indicate they accept the message before they can log into the GUI.	disable
pre-login-banner-message <message>	Enter the admin access disclaimer message that appears before administrators can log into the GUI. Enabled by the pre-login-banner command.	
service-group-hash-size {normal | expanded}	Select size of hash key for ELBC operation: • normal — 5-bit hash • expanded — 6-bit hash This is not available if service-group-mode is disabled. Available in switch mode only.	normal

Variables	Description	Default
service-group-mode {disable | basic | 2-port-lag | 4-port-lag}	Select service group mode for Enhanced Load Balance Cluster (ELBC) operation: • disable — no ELBC operation • basic — basic ELBC operation • 2-port-lag — ELBC with 2-port aggregation • 4-port-lag — ELBC with 4-port aggregation Available in switch mode only.	disable
service-group-snmp-community <name>	Name of elbc-mgmt SNMP community (workers must be configured with same community on base-mgmt). Available in switch mode only.	elbc-mgmt-comm
strong-crypto {enable | disable}	Enable or disable strong crypto for HTTPS/SSH access.	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 FortiController from the list and enter the correct number. The default is `04 (GMT-8:00)Pacific Time(US&Canada).`	04

ha

Setup HA for an Session-aware Load Balancing Cluster (SLBC). This command is available if load balancing is enabled. Available in load balance mode only.

Syntax

```
config system ha
  set mode {a-p | dual | standalone}
  set password <password_str>
  set group-id <id_integer>
  set override {enable | disable}
  set priority <priority_integer>
  set hb-interval <interval_integer>
  set hb-lost-threshold <threshold_integer>
  set hbdev-vlan-id <id>
  set failover-holdown <holddown>
  set graceful-upgrade {enable | disable}
  set chassis-redundancy {disable | enable}
  set chassis-id {1 | 2}
  set session-sync-port {disable | <interface-name>}
  set board-failover-tolerance <number-of-workers>
  set l3-gateway-failure-failover-interval <seconds>
  set minimize-chassis-failover {disable | enable}
  set hbdev {b1 | b2 | mgmt}
  set ha-eth-type <type_int>
  set ha-mgmt-vmac <mac-address>
  set boot-holdown <delay>
  set link-failure-threshold <number>
end
```

Variables	Description	Default
mode {a-p | dual | standalone}	Set the HA mode. • a-p create an Active-Passive cluster. • dual create a dual mode cluster. • standalone disable HA. All members of a cluster must be set to the same HA mode.	standalone
password <password_str>	Enter a password for the HA cluster. The password must be the same for all FortiController units in the cluster. The maximum password length is 15 characters.	no default
group-id <id_integer>	The HA group ID. The range is from 0 to 255. All members of the cluster must have the same group ID. Changing the Group ID changes the cluster virtual MAC address.	0

Variables	Description	Default
override {enable | disable}	Enable or disable forcing the cluster to renegotiate and select a new primary unit every time a cluster unit leaves or joins a cluster, changes status within a cluster, or every time the HA configuration of a cluster unit changes. This setting is not synchronized by HA.	disable
priority <priority_integer>	Change the device priority of the cluster unit. Each cluster unit can have a different device priority. During HA negotiation, the cluster unit with the highest device priority becomes the primary unit. The device priority range is 0 to 255. This setting is not synchronized by HA.	128
hb-interval <interval_integer>	The heartbeat interval is the time between sending heartbeat packets. The heartbeat interval range is 100 to 1000 milliseconds.	250
hb-lost-threshold <threshold_integer>	The lost heartbeat threshold is the number of consecutive heartbeat packets that are not received from another cluster unit before assuming that the cluster unit has failed. The range is 2 to 255 packets.	5
hbdev-vlan-id <id>	The VLAN to use for HA heartbeat traffic. The range is 1 to 4094.	999
failover-holdown <holddown>	The HA switch hold down interval. The range is 0 to 5000 milliseconds.	500
graceful-upgrade {enable | disable}	Enable to reduce service interruptions during a firmware upgrade. If enabled, the cluster upgrades the primary unit after first upgrading the other units in the cluster.	enable
chassis-redundancy {disable | enable}	Enable chassis redundancy for a SLBC that includes two chassis.	disable
chassis-id {1 | 2}	If chassis-redundancy is enabled, set the chassis number that the FortiController is installed in.	1
session-sync-port {disable | <interface-name>}	Set the name of the FortiController front panel interface to be used for session sync communication between FortiControllers in different chassis.	disable
board-failover-tolerance <number-of-workers>	The number of worker failures that will cause a multi-chassis cluster to switch processing to the backup chassis. Range 0 to 12.	0

Variables	Description	Default

l3-gateway-failure-failover-interval <seconds>	If the primary worker detects a link failure, an SLBC failover occurs after the time specified by this option. The time is relatively long to keep the SLBC cluster from failing over if the remote link is temporarily down. The range is 300 to 3600 seconds.
	To enable SLBC link monitoring, use the following command to add a link health monitor to the primary worker. The following example monitors the FortiController F1 front panel interface by pinging 8.8.8.8 through a remote gatway with IP address 50.50.50.1.
	`config system link-monitor`
	`edit link-mon-name`
	`set scrintf fctrl/f1`
	`set server 8.8.8.8`
	`set gateway-ip 50.50.50.1`
	`set update-cascade-interface disable`
	`end`
	If the link health monitor detects a failure it could be because the F1 interface of the currently active FortiController has failed or become disconnected. After a failover a different FortiController should become the primary FortiController.
		600

minimize-chassis-failover {disable | enable}	Enable in a multi-chassis configuration, so that after the primary FortiController fails, select the new primary FortiController from the same chassis as long as both chassis have the same number of operating FortiControllers.	disable
hbdev {b1 | b2 | mgmt}	Select the FortiController interfaces to be heartbeat interfaces.	
ha-eth-type <type_int>	Set the Ethertype used by heartbeat packets. <type_int> is a 4-digit hex number.	9890
ha-mgmt-vmac <mac-address>	Set the HA master management interface virtual MAC address.	00:00:00:00:00:00

Variables	Description	Default
boot-holdown <delay>	The delay in seconds before a FortiController becomes the primary unit if no other primary unit is found. The range is 3 to 65000 seconds.	40
link-failure-threshold <number>	You can use the `link-failure-threshold` to determine if an SLBC failover occurs when individual interfaces in any configured `lacp-active`, `lacp-passive`, or `static` trunk fails. These trunks are set up using the `config switch fabric-channel trunk` command. The `link-failure-threshold` is a global parameter that applies to any trunk in an SLBC cluster. If `link-failure-threshold` is set to 0 (the default), any the failure of any link in a trunk triggers an SLBC failover. You can set the threshold higher to require more links to fail before an SLBC failover occurs. A failover occurs if a number of links greater than the `link-failure-threshold` fail. For example, if you set `link-failure-threshold` to 3, then at least 4 links in one trunk must fail before an SLBC failover occurs. The FortiController-5103B `<number>` range is 0 to 8. The FortiController-5903C range is 0-16. The FortiController-5913C range is 0-20. To disable this feature, set `link-failure-threshold` to the maximum value for your hardware.	0

interface

Use this command to change the IP address and management access setting of the mgmt and base-mgmt interfaces and to bring the interfaces up or down.

Syntax

```
config system interface
  edit {mgmt | base-mgmt}
    set status {down | up}
    set ip <interface_ipv4mask>
    set allowaccess {http | https | ping | snmp | ssh | telnet}
    set mtu <bytes_integer>
    set mtu-override {enable | disable}
    set speed {1000full | 1000half | 100full |100half | 10full
        |10half | auto}
    set alias <string>
    set description <string>
    set mode {dhcp | static}
end
```

Variables	Description	Default
status {down | up}	Bring the mgmt interface up or down (start or stop the interface). If the interface is down, it does not accept or send packets.	up
ip <interface_ipv4mask>	Enter the mgmt interface IP address and netmask.	192.168.1.99 255.255.255.0
allowaccess {http | https | ping | snmp | ssh | telnet}	Enter the types of management access permitted on the mgmt interface. Valid types are: `ping ssh telnet`. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	None selected.
mtu <bytes_integer>	Set a custom maximum transmission unit (MTU) size in bytes. Ideally, you should set the MTU to the size of the smallest MTU of all the networks between this FortiController and the packet destination. This is available if mtu-override is enabled.	1500
mtu-override {enable | disable}	Enable to define a custom maximum transmission unit (MTU) size using the mtu variable.	disable
speed {1000full | 1000half | 100full |100half | 10full |10half | auto}	Set the speed of the network interface: 1000full — 1000M full-duplex 100full — 100M full-duplex 100half — 100M half-duplex 10full — 10M full-duplex 10half — 10M half-duplex auto — auto adjust speed	auto

Variables	Description	Default
alias <string>	Optionally, enter an alias name (maximum 25 characters) for the interface. The alias is displayed along with the interface name.	No default.
description <string>	Optionally, enter a description for this interface.	No default.
mode {dhcp | static}	Set the interface to have a static IP address or to get its IP address from DHCP.	static

ntp

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

Syntax

```
config system ntp
   set ntpsync {enable | disable}
   set syncinterval <interval_int>
   set type {fortiguard | custom}
   config ntpserver
      edit <serverid_int>
         set authentication {enable | disable}
         set key <password_str>
         set key-id <int>
         set ntpv3 {enable | disable}
         set server <ipv4_addr>[/<hostname_str>]
      end
end
```

Variable	Description	Default
ntpsync {enable | disable}	Enable to synchronize FortiGate unit's system time with the ntp server.	disable
server-mode {enable | disable}	Enable of disable FortiGate unit 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
type {fortiguard | custom}	Select FortiGuard or custom NTP server.	fortiguard
config ntpserver fields	Configures custom NTP time source.	
edit <serverid_int>	Enter the number for this NTP server	
authentication {enable | disable}	Enable or disable MD5 authentication.	disable
key <password_str>	Enter the password for MD5 authentication.	null
key-id <int>	Enter the Key-ID value for MD5 authentication.	0
ntpv3 {enable | disable}	Use NTPv3 protocol instead of NTPv4.	disable
server <ipv4_addr>[/<hostname_str>]	Enter the IPv4 address and hostname (optional) for this NTP server.	

snmp community

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

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

Syntax

```
config system snmp community
   edit <index_integer>
      set events {cpu-high | mem-low | ha-switch | ha-hb-member-up |
           ha-member-down | hbfail | hbrcv | tkmem-down | tkmem-up}
      set name <name_string>
      set query-v1-port <port_number>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_number>
      set query-v2c-status <port_number>
      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}
   end
```

Variables	Description	Default
edit <index_integer>	Enter the index number of the community in the SNMP communities table. Use 0 to assign the index number automatically.	No default.
events {cpu-high | mem-low | ha-switch | ha-hb-member-up | ha-member-down | hbfail | hbrcv | tkmem-down | tkmem-up}	Select one or more events for which to send SNMP traps. Separate the events with spaces. • cpu-high, cpu usage too high • mem-low, available memory too low • ha-switch, cluster status change • ha-hb-member-up, cluster member up • ha-member-down, cluster member down, • hbfail, heartbeat • hbrcv, heartbeat received • tkmem-down, trunk member down • tkmem-up, trunk member up	No default.
name <name_string>	Enter a name for the SNMP community.	No default.
query-v1-port <port_number>	Enter the SNMP v1 query port number used for SNMP manager queries.	161

Variables	Description	Default
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 <port_number>	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

snmp sysinfo

Use this command to enable the SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiController to identify it.

Syntax

```
config system snmp sysinfo
   set contact-info <string>
   set description <string>
   set location <string>
   set status {enable | disable}
   set trap-high-cpu-treshold <percentage>
   set trap-lowmemory-treshold <percentage>
end
```

Variables	Description	Default
contact-info <string>	Enter the contact information for the person responsible for this FortiController. The contact information can be up to 35 characters long.	
description <string>	Optionally enter a description of this FortiController.	
location <string>	Enter the physical location of the FortiController, up to 35 characters long.	
status {enable | disable}	Enable or disable the FortiController SNMP agent.	disable
trap-high-cpu-treshold <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
trap-lowmemory-treshold <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.

FortiOS 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.

Syntax

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

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

Variable	Description	Default
events <event_string>	Select which SNMP notifications to send. Select each event that will generate a notification, and add to string. Separate multiple events by a space. Available events include: **cpu-high** — cpu usage too high **ha-hb-failure** — HA heartbeat interface failure **ha-member-down** — HA cluster member down **ha-member-up** — HA cluster member up **ha-switch** — HA cluster status change **mem-low** — available memory is low **tkmem-down** — trunk member down **tkmem-up** — trunk member up ***Note***: On the `events` field, the `unset` command clears all options.	cpu-high mem-low ha-switch ha-hb-failure ha-member-down ha-member-up hbfail hbrcv tkmem-down tkmem-up
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.
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.	disable
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

execute

The following execute commands are available:

- backup
- base-channel
- bootimage
- date
- fabric-channel
- factory-reset
- load-balance
- ping
- reboot
- restore
- shutdown
- time
- top
- traceroute
- user certificate

backup

Use this command to back up the FortiController configuration and certificates to a TFTP server.

Syntax

```
execute backup all-config <backup_filename> <tftp_ipv4> [<password>]
execute backup config <backup_filename> <tftp_ipv4> [<password>]
```

Keywords and variables	Description
all-config	Back up the system configuration and certificates.
config	Back up the system configuration.
<backup_filename>	Enter a name for the backup file.
<tftp_ipv4>	Enter the IP address of the TFTP server.
<password>	Optionally, enter a password to protect the backup file with encryption.

base-channel

Clear virtual MAC address entries on a base channel interface. Clear virtual MAC addresses that match the following:

- a specific MAC address
- a VLAN tag
- a VLAN tag on a specific interface
- a VLAN tag and a specific MAC address

Syntax

```
execute base-channel mac clear by-interface <base-channel-interface-
  name>
execute base-channel mac clear by-mac-address <mac-address>
execute base-channel mac clear by-vlan <vlan>
execute base-channel mac clear by-vlan-and-interface <vlan>
  <interface>
execute base-channel mac clear by-vlan-and-mac-address <vlan> <mac-
  address>
```

bootimage

Use this command to change the firmware image used to start the FortiController by switching between the primary or secondary firmware image. To use this command you must install a primary and a secondary firmware image by using the system startup options available when you reboot the FortiController from a console connection.

Syntax

```
execute bootimage {primary | secondary}
```

date

Display or set the system date.

Syntax

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

date_str has the form mm/dd/yyyy, where

- mm is the month and can be 1 to 12
- dd is the day of the month and can be 1 to 31
- yyyy is the year and can be from 2001 to 2037

If you do not specify a date, the command returns the current system date. Shortened values for the year, such as ‘10’ instead of ‘2010’ are not valid.

fabric-channel

Clear virtual MAC address entries on a fabric channel interface. Clear virtual MAC add res es that match the following:

- a specific MAC address
- a VLAN tag
- a VLAN tag on a specific interface
- a VLAN tag and a specific MAC address

Syntax

```
execute fabric-channel mac clear by-interface <base-channel-
  interface-name>

execute fabric-channel mac clear by-mac-address <mac-address>

execute fabric-channel mac clear by-vlan <vlan>

execute fabric-channel mac clear by-vlan-and-interface <vlan>
  <interface>

execute fabric-channel mac clear by-vlan-and-mac-address <vlan> <mac-
  address>
```

factory-reset

Reset the FortiController configuration to factory default settings. This command deletes all changes that you have made to the FortiController configuration and reverts the system to its original configuration, including resetting the mgmt interface IP address.

Syntax

```
execute factory-reset
```

load-balance

Restore the MAC address of FortiController load-balance interfaces and other interfaces to their factory default MAC addresses. Available in load balance mode only.

Syntax

```
execute load-balance restore-factory-mac
```

ping

Send an ICMP echo request (ping) to test a network connection. You need a valid DNS server to ping a hostname.

Syntax

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

<host-name_str> should be a fully qualified domain name, for example: `www.fortinet.com`.

reboot

Restart the FortiController. While the FortiController is rebooting it cannot forward traffic.

Syntax

```
execute reboot
```

restore

Use this command to restore the FortiSwitch-5003A configuration from a file on a TFTP server or change the FortiSwitch-5003A firmware.

Syntax

```
execute restore all-config <filename> <tftp_ipv4> [<password>]
execute restore config <filename> <tftp_ipv4> [<password>]
execute restore image tftp <filename> <tftp_ipv4>
execute restore secondary-image tftp <filename> <tftp_ipv4>
```

Keywords and variables	Description
all-config	Restore the system configuration and certificates. The new configuration and certificates replace the existing ones.
config	Restore the system configuration. The new configuration replaces the existing configuration.
<filename>	Enter the name of the backup file or firmware image.
image	Restore (install) the primary firmware image. The system reboots, loading the new firmware.
secondary-image	Restore (install) the secondary firmware image.
<tftp_ipv4>	Enter the IP address of the TFTP server.
<password>	Enter the password for the backup file, if the file is password-protected.

shutdown

Shut down the FortiController now. You will be prompted to confirm the shutdown.

Syntax

```
execute shutdown
```

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 and can be `00` to `23`
- `mm` is the minutes and can be `00` to `59`
- `ss` is the seconds and can be `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.

top

Display a list of processes running on the FortiController. The command also displays information about each process. Press Ctrl-C to exit.

traceroute

Test the connection between the FortiController and an address or hostname and display information about the network hops. You need a valid DNS server to enter a hostname.

Syntax

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

Example

This example shows how to test the connection with 172.20.120.178. In this example the traceroute command times out after the first hop indicating a possible problem.

```
execute traceroute 172.16.100.149
traceroute to 172.16.100.149 (172.16.100.149), 30 hops max, 38 byte
    packets
 1  * * *
 2  * * *
```

user certificate

Use this command to upload certificates to the FortiController. You can also use this command to list and delete the certificates that you have uploaded.

For security reasons, certificates are not synchronized between FortiControllers. So you need to upload the certificate to each FortiController in an SLBC cluster.

Syntax

```
execute user certificate delete <filename>
execute user certificate list
execute user certificate upload tftp <file.crt> <file.key>
  <tftp_ipv4>
```

`<file.crt>` is the certificate file on the tftp server and `<file.key>` is the key file on the tftp server.

get

`Get` commands provide information about the operation of your FortiController.

The following `get` commands are available:

- get load-balance status
- get system csum
- get system mgmt-csum
- get system performance
- get system status

load-balance status

Use this command to view status information about the FortiController load balance operation

Syntax

```
get load-balance status
   ELBC Master Blade: slot-5
   Confsync Master Blade: slot-5
   Blades:
      Working:  2 [  2 Active  0 Standby]
      Ready:    0 [  0 Active  0 Standby]
      Dead:     0 [  0 Active  0 Standby]
     Total:     2 [  2 Active  0 Standby]

      Slot  5: Status:Working   Function:Active
        Link:      Base: Up          Fabric: Up
        Heartbeat: Management: Good   Data: Good
        Status Message:"Running"
      Slot  6: Status:Working   Function:Active
        Link:      Base: Up          Fabric: Up
        Heartbeat: Management: Good   Data: Good
        Status Message:"Running"
```

system csum

Use this command to view system checksum values.

Syntax

```
get system csum
```

Example

```
get system csum

debugzone checksum
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
checksum
4f 72 8c 28 8f 41 0e 19 7d b0 e6 39 a1 03 9f 89
```

system mgmt-csum

This command displays system checksum values. It is intended for use by a FortiManager central management unit.

Syntax

```
get system mgmt-csum
```

Example

```
get system mgmt-csum
debugzone
global: 6c 38 d5 7a 67 99 b2 fc e6 48 8a 5a 10 ac 42 41
all: 6c 38 d5 7a 67 99 b2 fc e6 48 8a 5a 10 ac 42 41
checksum
global: 6c 38 d5 7a 67 99 b2 fc e6 48 8a 5a 10 ac 42 41
all: 6c 38 d5 7a 67 99 b2 fc e6 48 8a 5a 10 ac 42 41
```

system performance

Use this command to display CPU usage, memory usage, and USB disk usage.

Syntax

```
get system performance
```

Example

The output looks like this (for an idle system):

```
# get system performance
CPU:
        Used:   2.9%
Memory:
        Total:  506,864 KB
        Used:   25,228 KB       5.0%
USB Disk:
        Total:  27,265 KB
        Used:   9,733 KB        35.7%
```

system status

Use this command to display FortiController system 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

```
Version: FortiSwitch-5003B v5.0,build0028,141027 (Patch 5)
Branch Point: 0028
Serial-Number: FS503B3E11700083
BIOS version: 04000004
Hostname: slot2-5003B
Current HA mode: standalone
System time: Fri Jan 16 22:08:16 2015
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
Version: FortiController-5103B v5.0,build0128,141202 (MR2)
Branch Point: 0128
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: slot-1-5103b
Current HA mode: standalone
System time: Fri Jan 16 14:40:23 2015
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

diagnose

This section describes some of the available FortiController diagnose commands.

You can use diagnose commands for debugging the operation of the FortiController and to set parameters for displaying different levels of diagnostic information.

Diagnose commands are intended for advanced users only. Contact Fortinet technical support before using these commands.

This section describes:

Monitoring the status of trunk members

You can monitor the status changes of trunk members. To do this, enable debugging for trunk. The console will then display `port effective` or `port ineffective` according to the status of the trunk member.

Syntax

```
diagnose debug trunk enable
diagnose switch fabric-channel trunk
```

Example output

```
Switch Trunk Information, Fabric-Channel
Trunk Name: slot_8_12
Port Selection Algorithm: src-dst-ip
Port       Serial Number        Update Time
__________ ____________________ ____________________
slot-8     FG5A253E06500030     19:45:31 May-05-2011
slot-6     FG5A253E06500032     19:45:32 May-05-2011

set switch port effective, port(slot-8)
set switch port ineffective, port(slot-8)
set switch port effective, port(slot-8)
set switch port ineffective, port(slot-8)
set switch port effective, port(slot-8)
set switch port ineffective, port(slot-8)
```

spanning-tree instance fabric-channel

Display the configuration of a spanning tree instance for an interface. For example, to display the configuration of spanning tree instance 5 for the FortiSwitch-5003A F5 interface enter:

Syntax

```
diagnose spanning-tree instance fabric-channel <instance_integer>
     [<interface_name>]
```

Variables	Description
<instance_integer>	The number of a spanning tree instance added to the FortiController in the range 0 to 15. Enter a number greater than 15 to display all instances.
[<interface_name>]	Enter the name of a FortiController interface to display how the spanning tree instance affects this interface. If you don't include an interface name the command displays the status of the spanning tree instance for all interfaces.

Example output

```
diagnose spanning-tree instance fabric-channel 5 f5

MST Instance Information, Fabric-Channel:


Instance ID : 5
Mapped VLANs : 101
Switch Priority : 4096
Regional Root MAC Address :   003064058f87
Regional Root Priority:       4096
Regional Root Path Cost:      0
Regional Root Port:           slot-2/1
Remaining Hops:               20

Port        Speed   Cost     Priority  Role       State
__________  ______  ________ _________ __________ __________

f5          10G     2000     128       DESIGNATED FORWARDING
```

spanning-tree mst-config fabric-channel

Display the FortiSwitch-5003A fabric channel MSTP configuration.

Syntax

```
diagnose spanning-tree mst-config fabric-channel
```

Example output

```
MST Configuration Identification Information

Unit: Fabric
MST Configuration Name: tree_1
MST Configuration Revision: 1
MST Configuration Digest: d397441fd8666b0abb8f5fab64b9d18a

Instance ID      Mapped VLANs
_____________________________________________________________
3                100
5                101
```

switch fabric-channel mac-address filter

Filter the FortiSwitch-5003A MAC addresses.

Syntax

```
diagnose switch fabric-channel mac-address filter <filter>
```

Where `<filter>` can be:

- clear — clear filter
- flags — flag pattern to match and mask of important bits
- port-id-map — list of port-ids to display
- show — show filter
- trunk-id-map — list of trunk-ids to display
- vlan-map — list of vlans to display

switch fabric-channel mac-address list

Verify the FortiController MAC address table.

Syntax

```
diagnose switch fabric-channel mac-address list
```

Example output

```
MAC: 00:09:0f:09:37:02 VLAN: 904 Trunk: slot_8_12(trunk-id 0)
Flags: 0x00000c80 [ trunk ]
MAC: 00:09:0f:71:00:61 VLAN: 902 Trunk: slot_8_12(trunk-id 0)
Flags: 0x00000c80 [ trunk ]
MAC: 00:09:0f:09:33:01 VLAN: 1 Port: slot-3(port-id 1)
Flags: 0x00000c00 [ ]
MAC: 00:09:0f:91:01:4f VLAN: 1 Port: slot-5(port-id 3)
Flags: 0x00000c00 [ ]
MAC: 00:09:0f:09:37:02 VLAN: 906 Trunk: slot_8_12(trunk-id 0)
Flags: 0x00000c80 [ trunk ]
MAC: 00:09:0f:71:03:1d VLAN: 1 Trunk: slot_8_12(trunk-id 0)
Flags: 0x00000c80 [ trunk ]
```