



# FortiSwitch 5000 series CLI Reference

for FortiOS 4.0 MR2



## **FortiSwitch 5000 series**

### **CLI Reference**

30 November 2010

01-420-135099-20101130

for FortiOS 4.0 MR2

© Copyright 2010 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

### **Trademarks**

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Contents

---

<b>Introduction</b>	<b>5</b>
How this guide is organized . . . . .	5
Typographical conventions . . . . .	5
CLI command syntax conventions . . . . .	6
Connecting to the CLI . . . . .	7
Connecting to the FortiSwitch-5003A console . . . . .	7
Setting administrative access on the mgmt interface . . . . .	8
Connecting to the FortiSwitch-5003A CLI using SSH . . . . .	9
Entering configuration data . . . . .	9
Entering text strings (names). . . . .	9
Entering numeric values . . . . .	10
Selecting options from a list . . . . .	10
Enabling or disabling options. . . . .	10
Support . . . . .	11
Fortinet products End User License Agreement . . . . .	11
Training. . . . .	11
Documentation . . . . .	11
Customer service and technical support . . . . .	11

---

<b>config</b>	<b>13</b>
admin radius-server . . . . .	14
admin user . . . . .	15
route static . . . . .	16
switch base-channel global. . . . .	17
switch base-channel interface . . . . .	18
switch base-channel mirror. . . . .	19
switch base-channel physical-port . . . . .	20
switch base-channel trunk . . . . .	21
switch domain . . . . .	22
switch fabric-channel global . . . . .	23
switch fabric-channel ha . . . . .	24
switch fabric-channel interface . . . . .	25
switch fabric-channel mirror . . . . .	27
switch fabric-channel physical-port . . . . .	28
switch fabric-channel stp instance . . . . .	29

switch fabric-channel stp settings . . . . .	31
switch fabric-channel trunk . . . . .	33
system central-management . . . . .	35
system dns . . . . .	36
system global . . . . .	37
system interface . . . . .	38
system snmp community . . . . .	40
system snmp sysinfo . . . . .	42

---

**execute 43**

backup . . . . .	44
bootimage . . . . .	45
date . . . . .	46
factory-reset . . . . .	47
ping . . . . .	48
reboot . . . . .	49
restore . . . . .	50
shutdown . . . . .	51
time . . . . .	52
top . . . . .	53
traceroute . . . . .	54

---

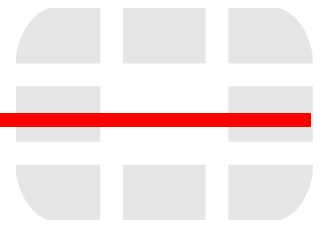
**get 55**

system csum . . . . .	56
system mgmt-csum . . . . .	57
system performance . . . . .	58
system status . . . . .	59

---

**diagnose 61**

Monitoring the status of trunk members . . . . .	62
spanning-tree instance fabric-channel . . . . .	63
spanning-tree mst-config fabric-channel . . . . .	64
switch fabric-channel mac-address filter . . . . .	65
switch fabric-channel mac-address list . . . . .	66



# Introduction

This manual describes the CLI commands for FortiSwitch-5000 series products such as the FortiSwitch-5003A board. Working with the FortiSwitch-5003A CLI is the same as working with the FortiOS CLI.

This chapter describes:

- [How this guide is organized](#)
- [Typographical conventions](#)
- [CLI command syntax conventions](#)
- [Connecting to the CLI](#)
- [Entering configuration data](#)
- [Support](#)

## 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:

- “[Introduction](#)” (this chapter) describes document conventions, how to access the CLI, and product support.
- “[config](#)” describes config commands.
- “[execute](#)” describes execute commands.
- “[get](#)” describes get commands.
- “[diagnose](#)” describes some useful troubleshooting commands.

## Typographical conventions

Fortinet documentation uses the following typographical conventions:

**Table 1: Typographical conventions in Fortinet technical documentation**

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns   set primary &lt;address_ipv4&gt; end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments          : (null) opmode            : nat</pre>
Emphasis	HTTP connections are <b>not</b> secure and can be intercepted by a third party.

**Table 1: Typographical conventions in Fortinet technical documentation**

<b>File content</b>	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><H4>You must authenticate to use this service.</H4>
<b>Hyperlink</b>	Visit the Fortinet Technical Support web site, <a href="https://support.fortinet.com">https://support.fortinet.com</a> .
<b>Keyboard entry</b>	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
<b>Navigation</b>	Go to <code>VPN &gt; IPSEC &gt; Auto Key (IKE)</code> .
<b>Publication</b>	For details, see the <a href="#">FortiOS Handbook</a> .

## CLI command syntax conventions

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

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

**Table 2: Command syntax notation**

Convention	Description
<b>Square brackets</b> [ ]	A non-required word or series of words. For example: [verbose {1   2   3}] indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: <code>verbose 3</code>
<b>Curly braces</b> { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
<b>Options delimited by vertical bars</b>	Mutually exclusive options. For example: {enable   disable} indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
<b>Options delimited by spaces</b>	Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: <code>ping https ssh</code> <b>Note:</b> To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type: <code>ping https snmp ssh</code> If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Table 2: Command syntax notation (Continued)

Convention	Description
<b>Angle brackets &lt; &gt;</b>	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore ( _ ) and suffix that indicates the valid data type. For example:</p> <pre>&lt;retries_int&gt;</pre> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> <li>• <b>&lt;xxx_name&gt;</b>: A name referring to another part of the configuration, such as <code>policy_A</code>.</li> <li>• <b>&lt;xxx_index&gt;</b>: An index number referring to another part of the configuration, such as 0 for the first static route.</li> <li>• <b>&lt;xxx_pattern&gt;</b>: A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all email addresses ending in <code>@example.com</code>.</li> <li>• <b>&lt;xxx_fqdn&gt;</b>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>.</li> <li>• <b>&lt;xxx_email&gt;</b>: An email address, such as <code>admin@mail.example.com</code>.</li> <li>• <b>&lt;xxx_url&gt;</b>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet./com/</code>.</li> <li>• <b>&lt;xxx_ipv4&gt;</b>: An IPv4 address, such as <code>192.168.1.99</code>.</li> <li>• <b>&lt;xxx_v4mask&gt;</b>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>.</li> <li>• <b>&lt;xxx_ipv4mask&gt;</b>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>.</li> <li>• <b>&lt;xxx_ipv4/mask&gt;</b>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>.</li> <li>• <b>&lt;xxx_ipv6&gt;</b>: A colon ( : )-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>.</li> <li>• <b>&lt;xxx_v6mask&gt;</b>: An IPv6 netmask, such as <code>/96</code>.</li> <li>• <b>&lt;xxx_ipv6mask&gt;</b>: An IPv6 address and netmask separated by a space.</li> <li>• <b>&lt;xxx_str&gt;</b>: A string of characters that is <i>not</i> another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.</li> <li>• <b>&lt;xxx_int&gt;</b>: An integer number that is <i>not</i> another data type, such as 15 for the number of minutes.</li> </ul>

## Connecting to the CLI

You can use a direct console connection, SSH, Telnet or the web-based manager to connect to the FortiSwitch-5003A CLI. Using SSH or Telnet you connect to the CLI through the mgmt interface.

- [Connecting to the FortiSwitch-5003A console](#)
- [Setting administrative access on the mgmt interface](#)
- [Connecting to the FortiSwitch-5003A CLI using SSH](#)

### Connecting to the FortiSwitch-5003A console

Connect to the FortiSwitch-5003A console using the FortiSwitch-5003A front panel COM port. You need:

- a computer with an available communications port
- a null modem cable, with an RJ-45 connector as provided with your FortiSwitch-5003A board
- terminal emulation software such as HyperTerminal for Windows



**Note:** The following procedure describes how to connect to the FortiSwitch-5003A CLI using Windows HyperTerminal software. You can use any terminal emulation program.

### To connect to the CLI

- 1 Connect the FortiSwitch-5003A RJ-45 COM port to the available communications port on your computer.
- 2 Make sure the FortiSwitch-5003A board is powered on.
- 3 Start HyperTerminal, enter a name for the connection, and select OK.
- 4 Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the FortiSwitch-5003A COM port.
- 5 Select OK.
- 6 Select the following port settings and select OK.

<b>Bits per second</b>	9600
<b>Data bits</b>	8
<b>Parity</b>	None
<b>Stop bits</b>	1
<b>Flow control</b>	None

- 7 Press Enter to connect to the FortiSwitch-5003A CLI.

A prompt similar to the following appears.

```
FS5A033E08000111 login:
```

The prompt includes the FortiSwitch-5003A host name. The default host name is the FortiSwitch-5003A serial number.

- 8 Type a valid administrator name and press Enter.

The default administrator name is `admin`.

- 9 Type the password for this administrator and press Enter.

The default is no password.

A prompt similar to the following appears:

```
FS5A033E080001~#
```

## Setting administrative access on the mgmt interface

To perform administrative functions through a the FortiSwitch-5003A mgmt network interface, you must enable the required types of administrative access. Access to the CLI requires SSH or Telnet access.

### To use the CLI to configure SSH or Telnet access

- 1 Connect and log into the FortiSwitch-5003A console.
- 2 Use the following command to configure the mgmt interface to accept SSH connections:

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

- 3 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
```

## Connecting to the FortiSwitch-5003A CLI using SSH

Secure Shell (SSH) provides strong secure authentication and secure communications to the FortiSwitch-5003A CLI from your internal network or the internet. Once the FortiSwitch-5003A board is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiSwitch-5003A CLI.

### To connect to the CLI using SSH

- 1 Install and start an SSH client.
- 2 Connect to the FortiSwitch-5003A mgmt interface.
- 3 Type a valid administrator name and press Enter.
- 4 Type the password for this administrator and press Enter.

A prompt similar to the following appears:

```
FS5A033E080001~#
```

You have connected to the FortiSwitch-5003A CLI, and you can enter CLI commands.

## Entering configuration data

The configuration of a FortiGate unit or a FortiSwitch-5003A board is stored as a series of configuration settings in the FortiOS configuration database. To change the configuration you can use the web-based manager or CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

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

### Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, text strings in FortiGate configuration names cannot include the following characters:

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

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

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

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

## Entering numeric values

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

Most web-based manager numeric value configuration fields limit the number of numeric digits that you can add or contain extra information to make it easier to add the acceptable number of digits and to add numbers in the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

## Selecting options from a list

If a configuration field can only contain one of a number of selected options, the web-based manager and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI you must spell the selection name correctly.

## Enabling or disabling options

If a configuration field can only be on or off (enabled or disabled) the web-based manager presents a check box or other control that can only be enabled or disabled. From the CLI you can set the option to enable or disable.

# Support

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article [Registration Frequently Asked Questions](#).

## Fortinet products End User License Agreement

See the [Fortinet products End User License Agreement](#).

## Training

Fortinet Training Services provides courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at <http://campus.training.fortinet.com>, or email [training@fortinet.com](mailto:training@fortinet.com).

## Documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

## Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

## Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

## Comments on Fortinet technical documentation

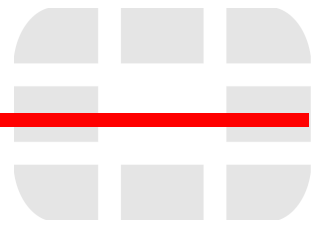
Please send information about any errors or omissions in this or any Fortinet technical document to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article [FortiGate Troubleshooting Guide - Technical Support Requirements](#).



# config

The following config commands are available:

- `admin radius-server`
- `admin user`
- `route static`
- `switch base-channel global`
- `switch base-channel interface`
- `switch base-channel mirror`
- `switch base-channel physical-port`
- `switch base-channel trunk`
- `switch domain`
- `switch fabric-channel global`
- `switch fabric-channel ha`
- `switch fabric-channel interface`
- `switch fabric-channel mirror`
- `switch fabric-channel physical-port`
- `switch fabric-channel stp instance`
- `switch fabric-channel stp settings`
- `switch fabric-channel trunksystem dns`
- `system central-management`
- `system dns`
- `system global`
- `system interface`
- `system snmp community`
- `system snmp sysinfo`

## admin radius-server

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

### Syntax

```
config admin radius-server
  edit <server_name>
    set port <port_integer>
    set secret <password>
    set server <ip_address>
  end
```

Variables	Description	Default
edit <server_name>	Enter a name to identify the RADIUS server.	No default.
port <port_integer>	Enter the RADIUS port for this server. Range is 0..65535.	1812
secret <password>	Enter the RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length.	No default.
server <ip_address>	Enter the RADIUS server domain name or IP address.	No default.

## admin user

Use this command to add and configure FortiSwitch-5003A administrator accounts. You cannot set different access levels for FortiSwitch-5003A administrators.

### Syntax

```
config admin user
  edit <administrator_name>
    set description <description_str>
    set password <admin_password>
    set radius-server <server_str>
    set user-type {local | radius}
end
```

Variables	Description	Default
edit <administrator_name>	Enter a new administrator name to add or enter the name of an administrator to edit. The <administrator_name> can be up to 35 characters.	No default.
description <description_str>	Describe the administrator account. The description can be up to 128 characters.	No default.
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.	No default.
radius-server <server_str>	Enter the name of the RADIUS server with which the user must authenticate. You can only select a RADIUS server that has been added to the list of RADIUS servers. See <a href="#">“config admin radius-server” on page 14</a> . This is available if user-type is radius.	No default.
user-type {local   radius}	Specify how this user’s password is verified: <ul style="list-style-type: none"> <li>local — the FortiSwitch-5003A board verifies the password</li> <li>radius — the RADIUS server specified in radius-server verifies the password.</li> </ul>	local

### Example

This example shows how to add a new administrator called new\_admin.

```
config admin user
  edit new_admin
    set description "A new administrator"
    set password 123456
end
```

## route static

Use this command to add, edit, or delete static routes for the mgmt interface.

### Syntax

```
config route static
  edit <sequence_number>
    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.
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

### Example

This example shows how to add a default route for the mgmt interface that points to 192.168.22.44.

```
config route static
  edit 0
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.22.44
  end
```

### Related topics

- [config system interface](#)
- [execute traceroute](#)

## switch base-channel global

Use this command to set base-channel global options.

### Syntax

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

Variables	Description	Default
edit <interface_name>		
dtag-mode {disabled   enable-external   enable-internal}	Select double-tagging support on this switch: <ul style="list-style-type: none"> <li>disabled — no double tagging support</li> <li>enable-external — all ports default to customer (UNI) ports</li> <li>enable-internal — all ports default to service provider (NNI) ports</li> </ul> Note: To change from enable-external to enable-internal or vice-versa, you must first select disabled.	disabled
name <name_string>	Enter a name for this switch channel.	No default.

## switch base-channel interface

Use this command to configure a base-channel switch interface.

### Syntax

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

Variables	Description	Default
edit <interface_name>	Enter the name of the interface to configure.	No 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 dtag-mode {external   internal}	Set the double-tagging mode for this interface: external — customer (UNI) port internal — service provider (NNI) port This is available if the dtag-mode in switch base-channel global is not disabled.	internal
native-vlan <id_number>	Select the native (untagged) VLAN for this interface.	1
type	This is a read-only variable.	physical

## switch base-channel mirror

Use this command to configure a mirror port.

### Syntax

```

config switch base-channel mirror
  set dst <port_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 <port_name>	Set destination port.	No default.
src-egress <interface_name>	Enter the egress port.	No default.
src-ingress <interface_name>	Enter the ingress port.	No default.
status {active   inactive}	Set mirror port active or inactive.	inactive
switching-packet {enable   disable}	Enable or disable switching functionality when mirroring.	disable

## switch base-channel physical-port

Use this command to configure physical port settings.

### Syntax

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

Variables	Description	Default
edit <port_name>	Enter the name of the port to configure.	
description <description_str>	Optionally, enter a description.	
max-frame-size <integer>	Set the maximum frame size. Range 68 to 16379.	16379
status {up   down}	Set the port as active (up) or disabled (down).	up

## switch base-channel trunk

Use this command to configure trunks.

### 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 the trunk.	
description <description_str>	Optionally, enter a description.	
members <interface_names>	Enter the names of the interfaces that are part of this trunk. Separate names with spaces.	No default.
port-selection-criteria {dst-ip   src-dst-ip  src-ip}	dst-ip — destination IP address src-dst-ip — source and destination IP address src-ip — source IP address	src-dst-ip

## switch domain

Use this command to configure a switch domain.

A switch domain is similar to a virtual switch, but is not a true virtual switch because the MAC table is shared globally.

### 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>
```

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: <ul style="list-style-type: none"> <li>• <b>blade-ports</b> — block blade ports</li> <li>• <b>misc-ports</b> — block ports that aren't monitor or blade ports</li> <li>• <b>monitor-ports</b> — block monitor ports</li> </ul>	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: <ul style="list-style-type: none"> <li>• <b>blade-ports</b> — block blade ports</li> <li>• <b>misc-ports</b> — block ports that aren't monitor or blade ports</li> <li>• <b>monitor-ports</b> — block monitor ports</li> </ul>	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 FortiSwitch-5003A board's HA role if HA is enabled.	128
vcluster-id <id_int>	Enter the HA virtual cluster id (1-255).	0

## switch fabric-channel global

Use this command to configure fabric-channel global options.

### Syntax

```
config switch fabric-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}	Select the double-tagging mode: disabled — no double tagging support enable-external — all ports default to customer (UNI) ports enable-internal — all ports default to service provider (NNI) ports	disabled
name <name_string>	Enter a name for this switch.	

## switch fabric-channel ha

Use this command to configure HA options for fabric channels.

### Syntax

```
config switch fabric-channel ha
  set mode {a-p | standalone}
  set hb-interval <interval_int>
  set hb-lost-threshold <interval_int>
  set hbdev-vlan-id <vlan_int>
  set monitor <interface_str>
end
```

Variables	Description	Default
mode {a-p   standalone}	Select whether HA is enabled in A-P mode or disabled (standalone operation). To set a-p mode, stp status must be disabled.	standalone
hb-interval <interval_int>	Enter the 5003A-to-5003A HA heartbeat interval (100ms-1000ms)	200
hb-lost-threshold <interval_int>	Enter the number of HA heartbeats lost before a device is considered dead (2-255)	5
hbdev-vlan-id <vlan_int>	VLAN to use for 5003A-to-5003A HA heartbeats on MGMTport(1-4094)	999
monitor <interface_str>	Enter the interface to monitor for HA heartbeat.	

## switch fabric-channel interface

Use this command to configure the VLANs allowed on FortiSwitch-5003A fabric channel interfaces. You can also change the native VLAN for each interface and disable or enable MSTP for each interface.

### 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 FortiSwitch-5003A fabric channel interface or trunk to configure. The interfaces added to a trunk do not appear in this list. 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

### Example

This example shows how to allow VLAN tags 201 to 210 on slots 6, 8, and 10 and the F1 front panel interface.

```
config switch fabric-channel interface
  edit "slot-6"
    set allowed-vlans 1,201-210
  next
  edit "slot-8"
    set allowed-vlans 1,201-210
  next
  edit "slot-10"
    set allowed-vlans 1,201-210
  next
  edit "f1"
    set allowed-vlans 1,201-210
  end
```

## Related topics

- [config switch fabric-channel physical-port](#)
- [config switch fabric-channel stp instance](#)
- [config switch fabric-channel stp settings](#)
- [config switch fabric-channel trunk](#)

## switch fabric-channel mirror

Use this command to configure a mirror port.

### Syntax

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

Variables	Description	Default
dst <port_str>	Enter the destination port.	
src-egress <interface_name>	Enter the egress port.	No default.
src-ingress <interface_name>	Enter the ingress port.	No default.
status {active   inactive}	Set mirror port active or inactive.	inactive
switching-packet {enable   disable}	Enable or disable switching functionality when mirroring.	disable

## switch fabric-channel physical-port

Use this command to change the administrative status of FortiSwitch-5003A fabric channel interfaces (bring each interface up or down) and configure each fabric channel interface to receive heartbeat packets from FortiGate-5001A or 5005FA2 fabric channel interfaces.

### Syntax

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

Variables	Description	Default
edit <interface_name>	Enter the name of the FortiSwitch-5003A fabric channel interface to configure. You cannot configure physical port settings for a trunk. You can configure physical port settings for interfaces that have been added to a trunk.	
status {down   up}	Bring the interface up or down.	up
description <description_str>	Optionally, enter a description.	
domain <domain_name>	Select the domain to which the port belongs.	root
max-frame-size <integer>	Set the maximum frame size. Range 68 to 16379.	16379

### Example

This example shows how to bring down the slot-2/1 FortiSwitch-5003A interface. You may need to bring this interface down to disable communication between fabric channel 1 and fabric channel 2.

```
config switch fabric-channel physical-port
  edit slot-2/1
    set status down
  end
```

### Related topics

- [config switch fabric-channel interface](#)
- [config switch fabric-channel stp instance](#)
- [config switch fabric-channel stp settings](#)
- [config switch fabric-channel trunk](#)

## switch 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

### 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
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 FortiSwitch-5003A 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
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.

Variables	Description	Default
<b>config stp-port variables</b>		
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-5003A interface 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

## Example

This example shows how to add spanning tree instance 10 with priority 4096 and with a VLAN ID range that includes 1, 200-210, and 23, 54, and 68. This instance also changes the cost and priority of interface slot-13.

```

config switch fabric-channel stp instance
  edit 10
    set priority 4096
    config stp-port
      edit slot-13
        set cost 2000
        set priority 16
      end
    end
  end
end

```

## Related topics

- [config switch fabric-channel interface](#)
- [config switch fabric-channel physical-port](#)
- [config switch fabric-channel stp settings](#)
- [config switch fabric-channel trunk](#)

## switch 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 FortiSwitch-5003A board.

### 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

### Example

This example shows how to set the name of an MSTP region to "MSTP\_test", set the revision to 1 and change the max-hops value to 4.

```
config switch fabric-channel stp instance
  set name "MSTP_test"
  set revision 1
  set max-hops 4
end
```

## Related topics

- [config switch fabric-channel interface](#)
- [config switch fabric-channel physical-port](#)
- [config switch fabric-channel stp instance](#)
- [config switch fabric-channel trunk](#)

## switch fabric-channel trunk

Use this command to create a trunk and add FortiSwitch-5003A interfaces to the trunk. You use trunks to group FortiSwitch-5003A interfaces so that you can use 802.3ad static mode layer-2 link aggregation to distribute sessions to the fabric interfaces of the FortiGate-5001A and 5005FA2 boards connected to the FortiSwitch-5003A interfaces in the trunk.

For information about FortiSwitch-5003A link aggregation for the FortiGate-5140 or FortiGate-5050 chassis, see “Fabric channel layer-2 link aggregation” in the *FortiSwitch-5003A and 5003 Fabric and Base Backplane Communications Guide*. Refer to the “FortiGate-5140 fabric backplane communication” or “FortiGate-5050 fabric backplane communication” chapter as appropriate.

### Syntax

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

Variables	Description	Default
edit <trunk_name>	Enter the name of a trunk to add or edit. This trunk name appears in fabric channel interface lists.	
members <interface_names>	Enter the names of the FortiSwitch-5003A fabric channel interfaces to add to the trunk. An interface can be added to only one trunk. Separate each interface name with a space. You can enter the interface names in any order. To add or remove an interface from a trunk, retype the complete list as required.	
port-selection-criteria {dst-ip   src-dst-ip   src-ip}	dst-ip destination IP address src-dst-ip source and destination IP address src-ip source IP address	src-dst-ip
description <string>	Optionally, enter a description.	
mode {fortinet-trunk   lacp-active   lacp-passive   static }	Configure the trunk mode: <ul style="list-style-type: none"> <li>fortinet-trunk — use heartbeat packets to negotiate Fortinet aggregation</li> <li>lacp-active — actively use LACP to negotiate 802.3ad aggregation</li> <li>lacp-passive — passively use LACP to negotiate 802.3ad aggregation</li> <li>static — use static aggregation, do not send and ignore any control messages</li> </ul>	static

### Example

This example shows how to add slot-6, slot-7, and slot-8 to a trunk named trunk\_678. This trunk can distribute sessions to FortiGate-5001A or 5005FA2 boards in chassis slots 6, 7, and 8.

```
config switch fabric-channel trunk
  edit trunk_678
    set members slot-6 slot-8 slot-7
  end
```

## Related topics

- [config switch fabric-channel interface](#)
- [config switch fabric-channel physical-port](#)
- [config switch fabric-channel stp instance](#)
- [config switch fabric-channel stp settings](#)

## system central-management

Use this command to configure central management.

### Syntax

```
config system cental-management
  set allow-monitor {enable | disable}
  set authorized-manager-only {enable | disable}
  set fmg <fmg_ipv4>
  set serial-number <sn_string>
  set status {enable | disable}
```

Variables	Description	Default
allow-monitor {enable   disable}	Enable or disable remote management.	enable
authorized-manager-only {enable   disable}	Enable or disable restricting access to the authorized manager only.	enable
fmg <fmg_ipv4>	Enter the IP address of the FortiManager unit.	No default.
serial-number <sn_string>	Enter the serial number of the FortiManager unit. This is available if authorized-manager-only is enabled.	No default.
status {enable   disable}	Enable or disable central management.	enable

## system dns

Use this command to configure DNS server settings.

### Syntax

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

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

## system global

Use this command to enable daylight saving time and configure the hostname and time zone for a FortiSwitch-5003A board.

### Syntax

```
config system global
  set admintimeout <timeout_integer>
  set chasis-id <chassis-id_integer>
  set daylightsavetime {enable | disable}
  set hostname <board_hostname>
  set strong-crypto {enable | disable}
  set timezone <timezone_number>
end
```

Variables	Description	Default
admintimeout <timeout_integer>	Set the idle time-out for system administration The idle timeout range is 1-480 minutes(8 hours).	5
chasis-id <chassis-id_integer>	Chassis-id (1 or 2)	1
daylightsavetime {enable   disable}	Enable or disable daylight saving time. If you enable daylight saving time, the FortiSwitch-5003A board adjusts the system time when the time zone changes to daylight saving time and back to standard time.	enable
hostname <board_hostname>	Enter a name to identify this FortiSwitch-5003A board. The hostname can be up to 36 characters and can include letters, numbers, hyphens, and underlines. Spaces and the following characters are not allowed: \ " > < ( ) ' & `   ; #.	serial number
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 FortiSwitch-5003A board from the list and enter the correct number. The default is 04 (GMT-8:00) Pacific Time (US&Canada).	04

### Example

This example shows how to set the time zone to 19 (GMT-3:00) Buenos Aires, Georgetown and how to change the host name to 5003A\_slot2.

```
config system global
  set timezone 04 (GMT-8:00) Pacific Time (US&Canada)
  set hostname 5003A_slot2
end
```

### Related topics

- [execute date](#)
- [execute time](#)

## system interface

Use this command to change the IP address and management access setting of the FortiSwitch-5003A mgmt (management) interface and to bring the mgmt interface up or down.

### Syntax

```
config system interface
  edit 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>
  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 FortiSwitch board 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 1000half — 1000M half-duplex 100full — 100M full-duplex 100half — 100M half-duplex 10full — 10M full-duplex 10half — 10M half-duplex auto — auto adjust speed	auto
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.

### Example

This example shows how to set the mgmt interface IP address and netmask and to configure the mgmt interface to allow ping, ssh, and telnet administrative access.

```
config system interface
  set ip 172.20.120.178/24
  set allowaccess ping ssh telnet
end
```

## Related topics

- [config route static](#)

## system snmp community

Use this command to configure SNMP communities on your FortiSwitch board. You add SNMP communities so that SNMP managers can connect to the FortiSwitch board 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 FortiSwitch board for a different set of events. You can also the 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, 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, hbfail, hbrcv, tkmem-down, tkmem-up}	cpu-high — cpu usage too high mem-low — available memory too low hbfail — heartbeat lost 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
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

Variables	Description	Default
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

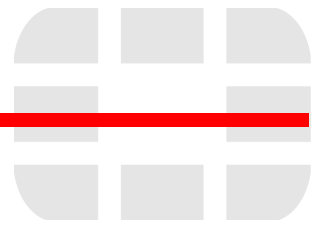
## system snmp sysinfo

Use this command to enable the SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiSwitch board to identify it. When your SNMP manager receives traps from the FortiSwitch board, you will know which board sent the information.

### 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 FortiSwitch board. The contact information can be up to 35 characters long.	
description <string>	Optionally enter a description of this board.	
location <string>	Enter the physical location of the FortiSwitch board, up to 35 characters long.	
status {enable   disable}	Enable or disable the FortiSwitch 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



# execute

The following execute commands are available:

- [backup](#)
- [bootimage](#)
- [date](#)
- [factory-reset](#)
- [ping](#)
- [reboot](#)
- [restore](#)
- [shutdown](#)
- [time](#)
- [top](#)
- [traceroute](#)

## backup

Use this command to back up the FortiSwitch-5003A 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.

### Example

This example shows how to backup the FortiSwitch-5003A configuration to a file named 5003A\_new.cfg on a TFTP server at IP address 192.168.1.23.

```
execute backup config 5003A_new.cfg 192.168.1.23
```

### Related topics

- [execute restore](#)

## bootimage

Use this command to change the firmware image used to start the FortiSwitch-5003A board 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 FortiSwitch-5003A from a console connection to the FortiSwitch-5003A COM port.

### 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.

### Examples

This example sets the date to 17 December 2010:

```
execute date 12/17/2010
```

### Related topics

- [config system global](#)
- [execute time](#)

## factory-reset

Reset the FortiSwitch-5003A configuration to factory default settings.

### Syntax

```
execute factory-reset
```



**Caution:** This command deletes all changes that you have made to the FortiSwitch-5003A configuration and reverts the system to its original configuration, including resetting the mgmt interface IP address.

## ping

Send an ICMP echo request (ping) to test the network connection between the FortiSwitch-5003A mgmt interface and another network device. You must add a DNS server to the FortiSwitch-5003A configuration 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`.

### Example

This example shows how to ping a host with the IP address 172.20.120.11.

```
execute ping 172.20.120.11
```

```
PING 172.20.120.11 (172.20.120.11): 56 data bytes
64 bytes from 172.20.120.11: seq=0 ttl=128 time=0.454 ms
64 bytes from 172.20.120.11: seq=1 ttl=128 time=0.399 ms
64 bytes from 172.20.120.11: seq=2 ttl=128 time=0.402 ms
64 bytes from 172.20.120.11: seq=3 ttl=128 time=0.431 ms

--- 172.20.120.11 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.399/0.421/0.454 ms
```

### Related topics

- [execute traceroute](#)

## reboot

Restart the FortiSwitch-5003A board. While the FortiSwitch-5003A board 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.

### Example

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

```
execute restore config backupconfig 192.168.1.23
```

### Related topics

- [execute backup](#)

## shutdown

Shut down the FortiSwitch-5003A board 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.

### Example

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

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

### Related topics

- [execute date](#)
- [config system global](#)

## top

Display a list of processes running on the FortiSwitch-5003A board. The command also displays information about each process. Press **Ctrl-C** to exit.

```
Mem: 100168K used, 406696K free, 0K shrd, 344K buff, 75092K cached
CPU:  0% usr  0% sys  0% nice 100% idle  0% io  0% irq  0% softirq
Load average: 0.00 0.00 0.00
  PID  PPID  USER      STAT   VSZ  %MEM  %CPU  COMMAND
   79   49  root      S      4276  1%    0%  -newcli admin --userfrom=telnet(172.2
   46    1  root      S      4220  1%    0%  /bin/cmdbsvr
   50    1  root      S      3720  1%    0%  /bin/sshd
   51    1  root      S      3572  1%    0%  /bin/switchd
   49    1  root      S      1884  0%    0%  /usr/sbin/telnetd -F
   52    1  root      S      1880  0%    0%  /sbin/getty 38400 /dev/vc/1
   53    1  root      S      1880  0%    0%  /sbin/getty -L /dev/usb/tts/0 9600 vt
   80   79  root      S      1876  0%    0%  sh -c top
   81   80  root      R      1876  0%    0%  top
    1    0  root      S      1380  0%    0%  init
   28    2  root     SW<         0  0%    0%  [bcm-shell]
   48    2  root     SWN         0  0%    0%  [bcmRX]
   43    2  root     SW<         0  0%    0%  [bcmLINK.1]
   19    1  root     SW          0  0%    0%  [usb-storage-0]
    2    1  root     SW          0  0%    0%  [keventd]
    3    1  root     SWN         0  0%    0%  [ksoftirqd_CPU0]
    4    1  root     SW          0  0%    0%  [kswapd]
    5    1  root     SW          0  0%    0%  [bdflush]
    6    1  root     SW          0  0%    0%  [kupdated]
    8    1  root     SW          0  0%    0%  [scsi_ah_0]
```

## traceroute

Test the connection between the FortiSwitch-5003A board and an address or hostname and display information about the network hops between the address and the FortiSwitch-5003A board. You must add a DNS server to the FortiSwitch-5003A configuration to trace the route to a hostname.

### Syntax

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

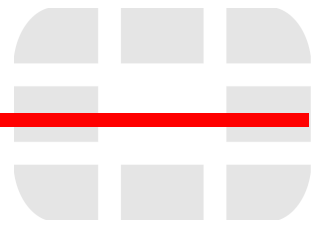
### Example

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  * * *
```

### Related topics

- [execute ping](#)



# get

`get` commands provide information about the operation of your FortiSwitch board.

The following `get` commands are available:

- `get system csum`
- `get system mgmt-csum`
- `get system performance`
- `get system status`

## 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. Use [get system csum](#) instead.

### Syntax

```
get system mgmt-csum
```

### Example

```
# get system mgmt-csum

debugzone checksum
cd 4b 90 41 de 62 a3 e0 c1 74 d2 64 a1 06 72 50
checksum
cd 4b 90 41 de 62 a3 e0 c1 74 d2 64 a1 06 72 50
```

## system performance

Use this command to display FortiSwitch-5003A 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 FortiSwitch-5003A system status information including:

- firmware version, build number and branch point
- serial number
- host name
- system time and date and related settings

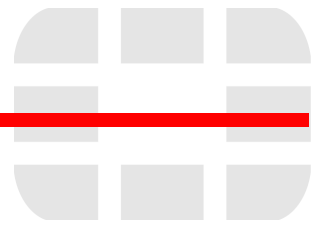
### Syntax

```
get system status
```

### Example output

```
Version: FortiSwitch-5003A 3.00,build0026,080911  
Serial-Number: FS5A033E08000111  
Hostname: FS5A033E08000111  
System time: Fri Sep 18 05:02:45 2009  
Daylight Time Saving: Yes  
Time Zone: (GMT-8:00)Pacific Time (US&Canada)
```





# diagnose

This section describes some of the available FortiSwitch-5003A diagnose commands.

You can use diagnose commands for debugging the operation of the FortiSwitch-5003A board and to set parameters for displaying different levels of diagnostic information.



**Caution:** 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](#)
- [spanning-tree instance fabric-channel](#)
- [spanning-tree mst-config fabric-channel](#)
- [switch fabric-channel mac-address filter](#)
- [switch fabric-channel mac-address list](#)

## 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 FortiSwitch-5003A board in the range 0 to 15. Enter a number greater than 15 to display all instances.
[<interface_name>]	Enter the name of a FortiSwitch-5003A 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 FortiSwitch-5003A 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 ]
```