



FortiCore CLI Reference

Version 1.1

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



Thursday, December 10, 2015

FortiCore CLI Reference Version 1.1

TABLE OF CONTENTS

Change Log	6
Introduction	7
FortiCore models	7
How this guide is organized	7
Conventions	7
IP Addresses	7
Cautions, tips and notes	8
Typographical conventions	8
Command syntax	9
Indentation	9
Notation	9
Subcommands	11
Entering configuration data	12
Entering text strings (names)	12
Entering numeric values	13
User Permissions	13
log	14
log setting local	14
log setting remote	15
router	18
router static	18
system	20
accprofile	20
admin	20
certificate ca	22
certificate local	23
global	25
interface	26
network-function-group	28
open-flow-channel	28
password-policy	29
service-group	30
session-aging	30
snmp community	31

snmp sysinfo.....	33
snmp threshold.....	34
snmp user.....	35
time manual.....	36
time ntp.....	37
user.....	38
radius.....	38
execute.....	39
backup.....	39
caching.....	39
certificate ca.....	40
certificate config verify.....	40
certificate crt.....	40
certificate local.....	41
certificate remote.....	41
date.....	41
factoryreset.....	42
formatlogdisk.....	42
log delete-file.....	43
log delete-type.....	43
log list-type.....	43
log rebuild-db.....	44
log tftp.....	44
nslookup.....	44
ping/ping6.....	44
ping-option, ping6-option.....	45
reboot.....	46
reload.....	47
restore.....	47
shutdown.....	48
tcpdump/tcpdump6.....	48
tcpdump-file.....	48
traceroute.....	49
get.....	50
log setting.....	50
open-flow channel.....	50
open-flow error-message.....	51
open-flow flow.....	52
open-flow protocol.....	52
open-flow table.....	53
port counters.....	54
port status.....	54

router static.....	55
service-group info.....	55
session port counters.....	55
system.....	56
user.....	56
show.....	58

Change Log

Date	Change Description
2015-11-03	FortiCore Release 1.0.0
2015-12-03	FortiCore Release 1.1.0
2015-12-08	Add command outputs for Release 1.1.0

Introduction

This guide provides information about configuring the FortiCore product, and detailed information about the FortiCore CLI commands.

FortiCore models

This guide is applicable to all FortiCore models: 6200A, 6240A, 6300A

How this guide is organized

This document contains the following content:

- the following chapters describe the configuration commands:
 - **log** - set the logging type, the logging severity level and the logging location.
 - **router** - Static routing commands
 - **system** - global parameters, system interfaces, NTP, and SNMP.
 - **user** - create users and user groups and control authentication.
- **execute** - commands that perform immediate operations.
- **get** - commands that display FortiCore provisioned values.
- **show** - commands that display FortiCore provisioned values.

Conventions

This section describes the conventions that this document uses.

IP Addresses

To avoid IP conflicts that would occur if you used examples in this document with public IP addresses that belong to a real organization, the IP addresses used in this document are fictional. They belong to the private IP address ranges defined by these RFCs.

- RFC 1918: Address Allocation for Private Internet
<http://ietf.org/rfc/rfc1918.txt?number-1918>
- RFC 5737: IPv4 Address Blocks Reserved for Documentation
<http://tools.ietf.org/html/rfc5737>
- RFC 3849: IPv6 Address Prefix Reserved for Documentation
<http://tools.ietf.org/html/rfc3849>

For example, even though a real network's Internet-facing IP address would be routable on the public Internet, in this document's examples, the IP address would be shown as a non-Internet-routable IP such as 10.0.0.1, 192.168.0.1, or 172.16.0.1.

Cautions, tips and notes

This document uses the following styles for cautions, tips, and notes.

Cautions:



Warns you about procedures or feature behaviors that could have unexpected or undesirable results including loss of data or damage to equipment.

Tips:



Highlights important, possibly unexpected but non-destructive, details about a feature's behavior.

Notes



Presents best practices, troubleshooting, performance tips, or alternative methods.

Typographical conventions

The following table describes the typographical conventions used in this document.

Convention	Example
CLI input	<code>config system global set language english end</code>
CLI output	<code>FortiCORE-6200A # get system global operation-mode : transect</code>
Emphasis	HTTP connections are not secure and can be intercepted by a third party.

Convention	Example
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
Hyperlink	Visit the Fortinet Technical Support web site: https://support.fortinet.com
Keyboard entry	To display the DNS server addresses, enter <code>get system dns</code> .
Publication	For additional information, see the FortiOS Handbook .

Command syntax

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

Indentation

Indentation indicates levels of nested commands, which indicate what other subcommands are available from within the scope.

For example, the **edit** subcommand is available only within a command that affects tables, and the next subcommand is available only from within the edit subcommand:

```
config system interface
  edit port1
    set status up
  next
end
```

Notation

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.

The following table describes the command notation.

Convention	Description
Square brackets []	A non-required word or series of words. For example: <code>[verbose {1 2 3}]</code> indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: <code>verbose 3</code>

Convention	Description
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [].
Options delimited by vertical bars	Mutually exclusive options. For example: {enable disable} indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
Options delimited by spaces	<p>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></p> <p>Note: 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:</p> <pre>ping https snmp ssh</pre> <p>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.</p>
Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: <code><retries_int></code> indicates that you should enter a number of retries, such as 5.
Data types include:	
<code><xxx_name></code>	A name referring to another part of the configuration, such as <code>policy_A</code> .
<code><xxx_index></code>	An index number referring to another part of the configuration, such as 0 for the first static route.
<code><xxx_pattern></code>	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> .
<code><xxx_fqdn></code>	A fully qualified domain name (FQDN), such as <code>mail.example.com</code> .
<code><xxx_email></code>	An email address, such as <code>admin@mail.example.com</code> .
<code><xxx_url></code>	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> .
<code><xxx_ipv4></code>	An IPv4 address, such as <code>192.168.1.99</code> .

Convention	Description
<xxx_v4mask>	A dotted decimal IPv4 netmask, such as 255.255.255.0.
<xxx_ipv4mask>	A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.
<xxx_ipv4/mask>	A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as 192.168.1.99/24.
<xxx_ipv6>	A colon(:)-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234.
<xxx_v6mask>	An IPv6 netmask, such as /96
<xxx_ipv6mask>	An IPv6 address and netmask separated by a space.
<xxx_str>	A string of characters that is not another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.
<xxx_int>	An integer number that is not another data type, such as 15 for the number of minutes.

Indentation indicates levels of nested commands, which indicate what other subcommands are available from within the scope.

For example, the edit subcommand is available only within a command that affects tables, and the next subcommand is available only from within the edit subcommand:

```
config system interface
    edit port1
        set status up
    next
end
```

Subcommands

Once you connect to the CLI, you can enter commands.

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects, for example:

```
get system admin
```

Subcommands are available from within the scope of some commands. When you enter a subcommand level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin) #
```

Applicable subcommands are available to you until you exit the scope of the command, or until you descend an additional level into another subcommand.

For example, the `edit` subcommand is available only within some configuration commands; the next subcommand (**set**, in the following example) is available only from within the `edit` subcommand:

```
config system interface
  edit port1
    set status up
  next
end
```

Available subcommands vary by command.

Entering configuration data

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

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

Entering text strings (names)

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

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

You can determine the limit to the number of characters that are allowed in a text string by determining how many characters the CLI allows for a given name field. From the CLI, you can also use the `tree` command to view the number of characters that are allowed.

For example, static route weight is an integer in the range 0-255. From the CLI you can do the following to confirm this:

```
# config router static
(static) # tree
-- [static] --*seq-num (0,0)
|- dst
|- gateway
|- distance (0,0)
|- weight (0,255)
|- priority (0,0)
|- device (36)
|- comment (64 xss)
|- blackhole
+- dynamic-gateway
```

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 (such as MAC addresses) require hexadecimal numbers.

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

User Permissions

Depending on the account that you use to log in to the FortiCore, you may not have complete access to all of the CLI commands.

Access profiles control which commands and areas an administrator account can access. Access profiles assign either:

- Read (view configuration)
- Write (change configuration)
- Both read and write
- No access

The administrator account named **admin** exists by default and cannot be deleted. The **admin** administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all configuration options, including viewing and changing all other administrator accounts. Its name and permissions cannot be changed. Only the administrator account can reset another administrator's password without being required to enter that administrator's existing password.

For complete access to all commands, log in with the **admin** administrator account.

log

Use the log commands to configure local or remote logging for the system.

log setting local

Use this command to configure basic log settings.

The local log is a datastore hosted on the FortiCore system.

Typically, you use the local log to capture information about system health and system administration activities. We recommend that you use local logging during evaluation and verification of your initial deployment, and then configure remote logging to send logs to a log management repository where they can be stored long term and analyzed using preferred analytic tools.

Local log disk settings are configurable. You can select a subset of system events, traffic, and security logs.

Syntax

```
config log settings local
    set disk-full {overwrite | nolog}
    set event-log-cached-lines {0|100|500|800|1000|2000|5000|10000}
    set event-log-category {admin app configuration system user}
    set event-log-status {enable|disable}
    set loglevel {alert | critical | debug | emergency | error | information | notification
    |
    warning}
    set rate_limit <integer>

    set rotation-size <integer>
    set status {enable|disable}
end
```

Variable	Description	Default
disk-full	Specify log behavior when the maximum disk space for local logs (30% of total disk space) is reached: overwrite — Continue logging. Overwrite the earliest logs. nolog — Stop logging	overwrite
event-log-category	Specify the types of events to collect in the local log: Configuration —Configuration changes. Admin —Administrator actions. Application —Health check results. System —System operations, warnings, and errors. User —Authentication results.	configuration admin app system

Variable	Description	Default
event-log-status	Enable/disable logging.	enable
loglevel	<p>Specify the lowest severity for which alerts are sent:</p> <ul style="list-style-type: none"> Emergency—The system has become unstable. Alert—Immediate action is required. Critical—Functionality is affected. Error—An error condition exists and functionality could be affected. Warning—Functionality might be affected. Notification—Information about normal events. Information—General information about system operations. Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior. <p>For example, if you select error, the system sends alerts with level Error, Critical, Alert, and Emergency. If you select alert, the system sends alerts with level Alert and Emergency.</p>	information
rate_limit	Rate limit logging (logs/second). The default is 0 (no limit).	0
rotation-size	Maximum size for a local log file. The default is 200 MB. When the current log file reaches this size, a new file is created.	200
status	Enable/disable local logging.	enable

example

log setting remote

Use this command to configure logging to a remote syslog server.

A remote syslog server is a system provisioned specifically to collect logs for long-term storage and analysis with preferred analytic tools.

Syntax

```

config log setting remote
edit <name>
    set comma-separated-value {enable|disable}
    set event-log-status {enable|disable}
    set event-log-category {admin app configuration system user}
    set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kern |
    local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, news,

```

```

    ntp}
    set loglevel {alert | critical | debug | emerge | error | information | notification
    | warning}
    set port <integer>
    set server <string>
    set status {enable|disable}
next
end

```

Variable	Description	Default
comma-separated-value	Send logs in CSV format.	disable
event-log-status	Enable/disable logging for system events.	disable
event-log-category	Specify the types of events to send to the syslog server: <ul style="list-style-type: none"> • Admin—Administrator actions. • Application—Health check results. • Configuration—Configuration changes. • System—System operations, warnings, and errors. • User—Authentication results. 	n/a
facility	Identifier that is not used by any other device on your network when sending logs to FortiAnalyzer/syslog.	kern
loglevel	Specify the lowest severity for which alerts are sent: <ul style="list-style-type: none"> • Emergency—The system has become unstable. • Alert—Immediate action is required. • Critical—Functionality is affected. • Error—An error condition exists and functionality could be affected. • Warning—Functionality might be affected. • Notification—Information about normal events. • Information—General information about system operations. • Debug—Detailed information about the system that can be used to troubleshoot unexpected behavior. For example, if you select error , the system sends alerts with level Error, Critical, Alert, and Emergency. If you select alert , the system sends alerts with level Alert and Emergency.	information
port	Listening port number of the syslog server. Usually this is UDP port 514.	514

Variable	Description	Default
server	IP address of the syslog server.	n/a
status	Enable/disable the syslog server.	disable

router

Use the router command to configure static routing.

router static

Use this command to configure static routes. Static routes are based on destination IP addresses.

The static route table must include a “default route” to be used when no more specific route has been determined.

Static routes specify the IP address of a next-hop router that is reachable from that network interface. Routers are aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets’ ultimate destinations.

You must configure at least one static route that points to a router, often a router that is the gateway to the Internet. You might need to configure multiple static routes if you have multiple gateway routers, redundant ISP links, or other special routing cases.

Syntax

```
config router static
edit <number>
    set destination <ip&netmask>
    set distance <integer>
    set gateway <class_ip>
next
end
```

Variable	Description	Default
destination	Address/mask notation to match the destination IP in the packet header. Specify 0.0.0.0/0 or ::/0 to set a default route for all packets.	No default
distance	The default administrative distance is 10, which makes it preferred to OSPF routes that have a default of 110. We recommend you do not change these settings unless your deployment has exceptional requirements.	No default
gateway	Specify the IP address of the gateway router that can route packets to the destination IP address that you have specified.	No default

Note about Default Routes

It is a best practice to include a default route. If there is no other, more specific static route defined for a packet’s destination IP address, a default route will match the packet, and pass it to a gateway router so that any packet

can reach its destination.

If you do not define a default route, and if there is a gap in your routes where no route matches a packet's destination IP address, packets passing through the FortiCore towards those IP addresses will, in effect, be null routed. While this can help to ensure that unintentional traffic cannot leave your FortiCore and therefore can be a type of security measure, the result is that you must modify your routes every time that a new valid destination is added to your network. Otherwise, it will be unreachable. A default route ensures that this kind of locally-caused "destination unreachable" problem does not occur.

system

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

accprofile

Use this command to manage access profiles. Access profiles associate permissions with the roles. The following permissions can be assigned:

- Read (view access)
- Read-Write (view, change, and execute access)
- No access

In larger companies where multiple administrators divide the share of work, access profiles often reflect the specific job that each administrator does ("role"), such as account creation or log auditing. Access profiles can limit each administrator account to their assigned role. This is sometimes called role-based access control (RBAC).

If you provision read access, the role can issue a CLI **get** command. If you provision read-write access, the role can issue a CLI **set** command.

Syntax

```
config system accprofile
  edit <profile-name>
    set log {none | read | read-write}
    set router {none | read | read-write}
    set system {none | read | read-write}
  end
```

Variable	Description	Default
<profile-name>	Enter the name for the profile.	No default
log {none read read-write}	Set the access permission for Log commands.	none
router {none read read-write}	Set the access permission for Router commands.	none
system {none read read-write}	Set the access permission for System commands.	none

admin

Use this command to manage administrator accounts.

We recommend that only network administrators—and if possible, only a single person—use the admin account. You can configure accounts that provision different scopes of access. For example, you can create an account for a security auditor who must only be able to view the configuration and logs, but not change them.

You can authenticate administrators using a password stored on the FortiCore or you can use a RADIUS server to perform authentication.

If you want to use RADIUS authentication, you must have already have created the RADIUS server configuration.

Syntax

```
config system admin
  edit <admin_name>
    set access-profile <profile-name>
    set access-token <string>
    set auth-strategy {local | ldap | radius}
    set is-system-admin {no|yes}
    set password <passwd>
    set privilege-map <string>
    set role-list <string>
    set trusted-hosts <ip&netmask>
    set vdom <datasource>
  end
```

Variable	Description	Default
<admin_name>	Enter the name for the admin account.	No default
access-profile <profile-name>	Specify a user-defined or predefined profile. The predefined profile named super_admin_prof is a special access profile used by the admin account. However, specifying this access profile will not confer all permissions of the admin account. For example, the new administrator would not be able to reset lost administrator passwords. Note: This option does not appear for the admin administrator account, which by definition always uses the super_admin_prof access profile.	No default
access-token <string>	Reserved for future use.	
auth-strategy {local ldap radius}	Enter the authentication strategy	local
is-system-admin { no yes }	Whether this user a system administrator.	no
password	Set a strong password for all administrator accounts. The password should be at least eight characters long, be sufficiently complex, and be changed regularly. To check the strength of your password, you can use a utility such as Microsoft's password strength meter.	*

Variable	Description	Default
privilege-map	Not used	n/a
role-list	Not used	n/a
trusted-hosts	Source IP address and netmask from which the administrator is allowed to log in. For multiple addresses, separate each entry with a space. You can specify up to three trusted areas. They can be single hosts, subnets, or a mixture of both.	0.0.0.0/0 ::/0
vdom	If you have enabled the virtual domain feature, specify the virtual domain that this administrator can view and manage.	root

Trusted hosts

Configuring trusted hosts hardens the security of the system. In addition to knowing the password, an administrator must connect only from the computer or subnets you specify.

Trusted host definitions apply to the CLI when accessed through Telnet, SSH, or the CLI console widget. Local console access is not affected by trusted hosts.

If ping is enabled, the address you specify here is also a source IP address to which the system will respond when it receives a ping or traceroute signal.

To allow logins only from one computer, enter only its IP address and 32- or 128-bit netmask:

```
192.0.2.2/32
```

```
2001:0db8:85a3::8a2e:0370:7334/128
```

To allow login attempts from any IP address (not recommended), enter:

```
0.0.0.0/0.
```

Caution: If you restrict trusted hosts, do so for all administrator accounts.

Tip: For improved security, restrict all trusted host addresses to single IP addresses of computer(s) from which only this administrator will log in.

certificate ca

Use this command to configure CA certificates. This command is an alternative to **execute certificate ca**.

Reserved entry "Fortinet_CA". Users cannot modify this entry.

Syntax

```
config system certificate ca
  edit <name>
    set certificate <certificate>
  next
end
```

Variable	Description	Default
certificate	Paste the contents of a CA certificate file between quotation marks as shown in the example.	n/a

example

```
FortiCore-VM # config system certificate ca
FortiCore-VM (ca) # get
== [ Fortinet_CA ]
== [ OracleSSLCA ]
== [ ca ]
FortiCore-VM # config system certificate ca
FortiCore-VM (ca) # edit ca-new
FortiCore-VM (ca-new) # set certificate "-----BEGIN CERTIFICATE-----
> MIID0TCCArmGAWIBAgIJAKr1/WtE48FeMA0GCSqGSIb3DQEBCwUAMGgxZARBgoJ
> kiaJk/IsZAEZFgNvcmcxZfzAVBgoJkiaJk/IsZAEZFgdjaWxvZ29uMQswCQYDVQQG
> EwJVUzEQMA4GA1UEChMHQ01Mb2dvbjEZMBcGA1UEAxMQQ01Mb2dvbiBPU0cgQ0Eg
> MTAeFw0xNDA0MzAxNDE4MDhaFw0zNDA0MzAxNDE4MDhaMGgxZARBgoJkiaJk/Is
> ZAEZFgNvcmcxZfzAVBgoJkiaJk/IsZAEZFgdjaWxvZ29uMQswCQYDVQQGEwJVUzEQ
> MA4GA1UEChMHQ01Mb2dvbjEZMBcGA1UEAxMQQ01Mb2dvbiBPU0cgQ0EgMTCCASIw
> DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMQQzsB9Uc37VuIyt5xJxcYYkc6K
> XpYihHgskTQp6YYB4XHVimouHafMYyoFsnenrcgf2NGFDvi9l9x9mnL77920JqGr
> LijieMiFEyPlnhGW8C6nJjkSsXLbgZNh9u6U+0oAbspsFRwdHDZOI7gIHSJ2zuiY
> CkMAVjw9TN44Q4IFCvSIf7mfzZgBH7AW1sbgznqnAJsWQhQGTPxZAxubItesyduD
> vj8tz9eb5u8JO3iQ/LYhMspNnxcptFdaLn2v82NAFTtCrZdCd7aLj1DM0DPEX7Nw
> V/rt/l+tlscglYyEoUnlPYuSQN0Q6Aj5i1GcKPvnFS0Oy9lGY11T1vZJ4F0CAwEA
> Aan+MHwwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYE
> FP7bnvI4TIqtrM+KGgCvedJiQpuHMB8GA1UdIwQYMBaAFP7bnvI4TIqtrM+KGgCv
> FP7bnvI4TIqtrM+KGgCvedJiQpuHMB8GA1UdIwQYMBaAFP7bnvI4TIqtrM+KGgCv
> edJiQpuHMBkGA1UdEQQSMBCBDMNhQGNpbG9nb24ub3JnMA0GCSqGSIb3DQEBCwUA
> A4IBAQCq5KUHQNq51uh1pxKMXQ98ADj2bNzQbswdAFs1Pow8tTZIBMwhdrq02ZHC
> XPyp2IHxfv+G+pMV1JFtdR0fy8ivilMNYjObEGh1Ss3kvvU7d1z3XwPxqpNcwDqs
> 1K6RRg4zpNWCFFcliAkPDsDbaN1B6A6zJXqOpGgzwoC3dZbPe5sYLgkWZO2/8MI
> eAEk7zoU1ZPSZiu5HghPafKuE1HYshvsak090tRgC6VLvaSLonZlwR0GuFVGdewH
> 4jR1HpENH7QiLCB1NGCoJgDi3qiFosw3M2+0ExevE1afj2Usm4oZir+Uty0rvR8D
> 03RHH8yYbZ9rw0kuwTkJEo3bYDxH
> -----END CERTIFICATE-----"
FortiCore-VM (ca-new) # end
```

certificate local

Use this command to manage local certificates. Reserved entry "Factory". Users cannot modify this entry.

Syntax

```
config system certificate local
edit <name>
    set certificate <certificate>
    set comments <string>
    set csr <csr>
    set password <passwd>
```

```

        set private-key <key>
    next
end

```

Variable	Description	Default
name	Name of the certificate	
certificate	Paste the contents of a certificate file between quotation marks as shown in the example.	
comments	Optional administrator note.	
csr	Paste the contents of a Certificate Signing Request (CSR) file between quotation marks as shown in the example.	
password	Password that was used to encrypt the file. The FortiCore system uses the password to decrypt and install the certificate.	
private-key	Paste the contents of a key file between quotation marks as shown in the example.	

example

```

FortiCore-VM # config system certificate local
FortiCore-VM (local) # get
== [ Factory ]
== [ csr_name_test ]

FortiCore-VM (local) # show
config system certificate local
    edit "csr_name_test"
t7e4fiX6Sd6T5426Gg/HQXRH41mBwGmjKdBShUbvVUZTka2FtD1oLMWE2mTq1c9GMUz0DokP-
foqXkjkmja5mWv4/w
A5XdQ00lQmTeMZK/X5OSFmSS
    set private-key "-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBNjBAbGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5/vf1VQB/28CAggA
MBQGCCqGSIb3DQMHBAGZorM0zlnPNASCAViZk4wTZYYMP10e7NwyxqvLND3LxUaV
UG1XpUSPfnUP4YgrV2d0Uijclj5M7MS341cMVKZ7G1pS/6jvxUr0NamQv4j7JsJ0
t3G7LMkzcTiep26GUCy55Qt+iob7lh0iiKa+4uPOq/Mzy+84AWnRNLfIhevHPsYb
rk4UbwNOFb0ZD9i06+UrFLsRGmtp/vlDyBgAoBojKxB/4j0G299QamnzPz4qneBc
HtPqTMPELyqtT6w4cmnwp6Ti200Ar9c44mKdyyAVZKie+Iu/4pSVBNSfuC+jjtmC
k8OrCrG14NwrhbtY9zEnGxBRR1NMTEBBTqAQNYWtjUEQVjmY1GAJA3/oBQe7l8C/
G/IUVvc/aaqMvsKSNfDpgZaudTDe1Wxi1792ADGh7zsl1s+ykH9nmqh7BPfm30Nv
f801hXgq01Lvo4v1xdC0w5oAeCyG1bTY5ZnXJFm0HCp0kA==
-----END ENCRYPTED PRIVATE KEY-----
"

    set csr "-----BEGIN CERTIFICATE REQUEST-----
MIIBNzCB4gIBADBqMQswCQYDVQQIEwJjYTESMBAGA1UEBxMJc3Vubnl2YWxlMREw

```

```

DwYDVQQKEwhmb3J0aW5ldDENMAsgA1UECxmEZmFkYzEQMA4GA1UEAxMHZXhhbXBs
ZTETMBEGCSqGSib3DQEJARYEcm9vdDBcMA0GCSqGSib3DQEBAQUAA0sAMEgCQQDK
XH/MC1KTkkZJiQDFb6IXHLYsSVbJzF0K30s3CVmKZvJQSBnmV8aq3fJjN281rrFT
iUovVdBzwCF5jKbxsrPLAgMBAAGgEzARBgNVHRMxChMIQ0E6RkFMU0UwDQYJKoZI
hvcNAQEFBQADQQB96NU+xjds83/6VRSzsyxeVxAGVD7F9Npuji8r/MpxPiMT0PQM
G8Wg//26ZqpwjupQ2V1+7QU4MDk3B5VUJSEF
-----END CERTIFICATE REQUEST-----
"
    next
end

```

global

Use this command to manage system settings.

Note: When you change the operation mode (from transect to conditional-forwarding or vice-versa), the system requires a reboot. The system prompts you to confirm the reboot when you change the mode.

Syntax

```

config system global
    set admin-idle-timeout <integer>
    set default-certificate <certname>
    set hostname <string>
    set language english
    set operation-mode {transect | conditional-forwarding}
    set port-http <integer>
    set port-https <integer>
    set port-ssh <integer>
    set port-telnet <integer>
end

```

Variable	Description	Default
admin-idle-timeout	Log out an idle administrator session. The default is 30 minutes.	30
default-certificate	The default is Factory.	Factory

Variable	Description	Default
hostname	<p>You can configure a hostname to facilitate system management. If you use SNMP, for example, the SNMP system name is derived from the configured hostname.</p> <p>The hostname can be up to 35 characters in length. It can include US-ASCII letters, numbers, hyphens, and underscores, but not spaces and special characters.</p> <p>The System Information widget and the get system status CLI command display the full hostname. If the hostname is longer than 16 characters, the name is truncated and ends with a tilde (~) to indicate that additional characters exist, but are not displayed.</p>	n/a
language	Currently, only English is supported	English
operation-mode	<p>Set the mode to transect or conditional-forwarding:</p> <p>transect - no TCP-session awareness. Forwards all traffic to the Network Security Function.</p> <p>conditional-forwarding - TCP-session awareness. Forwards only active session traffic to the Network Security Function.</p> <p>Note: the system requires a reboot to change the operation mode. The system prompts you to confirm.</p>	transect
port-http	Specify the port for the HTTP service. Usually, HTTP uses port 80.	80
port-https	Specify the port for the HTTPS service. Usually, HTTPS uses port 443.	443
port-ssh	Specify the port for the SSH service. Usually, SSH uses port 22.	22
port-telnet	Specify the port for the Telnet service. Usually, Telnet uses port 25.	25

interface

Use this command to configure network interfaces.

Syntax

```
config system interface
edit <name>
set allowaccess {http https ping snmp ssh telnet}
set direction {eastbound | northbound | southbound | westbound}
set ip <ip&netmask>
```

```

set mac-addr <mac address>
set mode static
set redundant-master
set speed {1Gfull | 1Ghalf | 10Gfull | 10Ghalf | 100Gfull | 100Ghalf | 1000Gfull |
1000Ghalf | auto}
set status {down | up}
set type {vlan | aggregate | physical}

```

Variable	Description	Default
edit <interface_name>	Edit an existing interface or create a new VLAN interface.	None.
allowaccess <access_types>	Enter the types of management access permitted on this interface or secondary IP address. Valid types are: http https ping snmp ssh telnet. Separate each type with a space. To add or remove an option from the list, retype the complete list.	Varies for each interface.
direction	Values: eastbound, northbound, southbound, westbound Flow Processing: the direction assigned to the interface determines which processing unit will process the interface's ingress traffic. Flows received from the SDN controller will be populated onto the unit associated with the incoming port value of the flow. If the flow has no incoming port value, the flow is programmed on all four processing units.	northbound
ip <ip&netmask>	Specify the IP address and CIDR-formatted subnet mask, separated by a forward slash (/), such as 192.0.2.5/24. Dotted quad formatted subnet masks are not accepted. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet (i.e. overlapping subnets).	0.0.0.0/0
mode	static — the IP address is assigned statically.	.
speed	The interface speed. Speed options vary for different models and interfaces. Port speeds must be configured as follows: - Management port must be set to auto, 1Gfull or 1Ghalf (on all models) - Ports 1-32 must be set to 1Gfull or 10Gfull (on all models) - Ports 33-36 must be set to 40Gfull on 6240A - Ports 33-34 must be set to 100Gfull on 6300A	auto
status	The interface status. The status is down or up .	up

Variable	Description	Default
type {aggregate physical vlan}	<p>Enter the type of interface. Note: Some types are read only, and are set automatically by hardware.</p> <p>aggregate — Aggregate links use the 802.3ad standard to group up to 8 interfaces together.</p> <p>physical — a physical interface.</p> <p>vlan — a virtual LAN interface.</p>	physical

network-function-group

Use this command to configure the East and West port pairing for each network security device. This is required only for Conditional Forwarding operation mode.

Syntax

```
config system network-function-group
edit <number>
    set east-port <port>
    set west-port <port>
```

Example

In the following example, the network security device is connected to port 3 and port 7:

```
config system network-function-group
edit 1
    set east-port 3
    set west-port 7
next
end
```

open-flow-channel

Use this command to configure the Open Flow channel between the FortiCore and the SDN controller.

Syntax

```
config system open-flow-channel
set cacert <name>
set cert <name>
set ip <ipv4_addr>
set max-backoff <interval_int>
set port <integer>
set probe-interval <integer>
set transport ( tcp | tls )
end
```

Variable	Description	Default
cacert	CA certificate name	n/a
cert	certificate name	n/a
ip	open flow controller ip address	0.0.0.0
max-backof	Maximum interval in seconds to wait before retrying a connection to the controller	8
port	open flow controller port number	6633
probe-interval	Interval in seconds at which idle controller is probed	5
transport	transport type. Select TCP or TLS.	tcp

password-policy

Use this command to configure the password policy for admin and other users.

Syntax

```

config system password-policy
    set status {enable | disable}
    apply-to admin-user
    minimum-length <integer>
    must-contain {lower-case-letter non-alphanumeric number upper-case-letter}
end

```

Variable	Description	Default
status	Enable/disable password requirements.	enable.
apply-to	Apply the policy to all admin users.	admin-user
minimum-length	Specify a minimum length. The default is 8.	8
must-contain	Specify character requirements. lower-case-letter - password must contain lower case letter non-alphanumeric - password must contain non-alphanumeric characters number - password must contain number upper-case-letter - password must contain upper case letter	n/a

service-group

Use this command to configure a service group.

Forticore expects all incoming traffic to be tagged with a single VLAN. If traffic on a North or South port is double VLAN-tagged or untagged, the default action is for Forticore to drop the packets. You can configure a North and South port pair using the **service-group** command. All double-tagged and untagged traffic entering the North port exits on the South port and vice-versa.

Syntax

```
config system service-group
  edit <service group>
    set north-port <num_int>
    set south-port <num_int>
end
```

Variable	Description	Default
edit <service group>	Edit or create a service group.	None.
north-port <num_int>	Set the northbound port number	0
south-port <num_int>	Set the southbound port number	0

session-aging

Use this command to configure the TCP session aging timers for conditional-forwarding operation mode. The values that you configure in the FortiCore must match the equivalent values in the Network Security Function (such as the **firewall service custom** configuration on FortiGate).

Syntax

```
config system session-aging
  set tcp-halfclose-timer <32 - 4080 seconds>
  set tcp-halfopen-timer <32 - 4080 seconds>
  set tcp-normal-timer <32 - 4080 seconds>
  set tcp-timewait-timer <32 - 4080 seconds>
```

Variable	Description	Default
tcp-halfclose-timer	The number of seconds that the system will wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is 32 - 4080 seconds. The recommended value is 128.	128
tcp-halfopen-timer	The number of seconds that the system will wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is 32 - 4080 seconds. The recommended value is 32.	32
tcp-normal-timer	The number of seconds that the system will wait to close an established session in which the system has not received any data packets. The valid range is 32 - 4080 seconds. The recommended value is 512.	512
tcp-timewait-timer	The number of seconds that the system will wait after sending the connection termination request. This timer is to ensure the remote TCP received the acknowledgment of its connection termination request. The valid range is 32 - 4080 seconds. The recommended value is 32.	32

snmp community

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

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



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

Syntax

```
config system snmp community
edit <index_number>
```

```

set name <community_name>
set queryportv1 <port_number>
set queryportv2c <port_number>
set queryv1-status {enable | disable}
set queryv2c-status {enable | disable}
set status {enable | disable}
set trapportv1-local <port_number>
set trapportv1-remote <port_number>
set trapportv2c-local <port_number>
set trapportv2c-remote <port_number>
set trapv1-status {enable | disable}
set trapv2c-status {enable | disable}
config hosts
    edit <host_number>
        set ip <address_ipv4>
    end
end

```

Variable	Description	Default
edit <index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.	No default
events <events_list>	Enable the events for which the system should send traps to the SNMP managers in this community.	All events enabled.
name <community_name>	Enter the name of the SNMP community to which the FortiCore system and at least one SNMP manager belongs. You must configure the FortiCore system to belong to at least one SNMP community so that community's SNMP managers can query system information and receive SNMP traps.	No default
query-v1-port <port_number>	Enter the SNMP v1 query port number used for SNMP manager queries.	161
query-v1-status {enable disable}	Enable or disable SNMP v1 queries for this SNMP community.	enable
query-v2c-port <port_number>	Enter the SNMP v2c query port number used for SNMP manager queries.	161
query-v2c-status {enable disable}	Enable or disable SNMP v2c queries for this SNMP community.	enable
status {enable disable}	Enable or disable the SNMP community.	enable
trap-v1-lport <port_number>	Enter the SNMP v1 local port number used for sending traps to the SNMP managers.	162

Variable	Description	Default
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
host variables		
edit <host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.	No Default
ip <address_ipv4>	Enter the IPv4 IP address of the SNMP manager (for hosts).	0.0.0.0

snmp sysinfo

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

Syntax

```
config system snmp sysinfo
    set contact <info_str>
    set description <description>
    set location <location>
    set status {enable | disable}
end
```

Variable	Description	Default
contact-info <info_str>	Add the contact information for the person responsible for this FortiCore. The contact information can be up to 35 characters long.	No default

Variable	Description	Default
description <description>	Add a name or description of the system. The description can be up to 35 characters long.	No default
location <location>	Describe the physical location of the system. The system location description can be up to 35 characters long.	No default
status {enable disable}	Enable or disable the FortiCore SNMP agent.	disable

snmp threshold

Set the threshold values for triggering SNMP events.

Syntax

```
config system snmp threshold
set cpu <trigger> 1-100 <threshold> 1-960 <total sample period> 30-28800 <sample frequency> 30-100
set logdisk <trigger> 1-100 <threshold> 1-8 <total sample period> 3600-28800 <sample frequency> 3600-7200
set mem <trigger> 1-100 <threshold> 1-960 <total sample period> 30-28800<sample frequency> 30-100
```

Use the **set cpu** command to set the parameters for CPU Overusage trap

Use the **set logdisk** to set the parameters for Low log disk space trap

Use the **set mem** to set the parameters for Memory Low trap

Each of the above set commands takes 4 values:

- Trigger — Utilization level that triggers the event. Enter a Percentage value
- Threshold — The event is reported when the condition has been triggered this many times during the total sample period.
- Total Sample Period — Duration of time (in seconds) in which threshold events can accumulate to report the event.
- Sample Frequency — How often (in seconds) that the utilization level is sampled

The following table displays the default values for each of the commands:

Command	Trigger	Threshold	Total Sample Period	Sample Frequency
cpu	80	3	600	30
logdisk	90	1	7200	3600
mem	80	3	600	30

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.

Syntax

```
config system snmp user
  edit <username>
    set query-status {enable|disable}
    set queryport <integer>
    set security-level {authnopriv | authpriv | noauthnopriv}
    set auth-proto {md5 | sha}
    set auth-pwd <password>
    set priv-proto {aes | des}
    set priv-pwd <password>
    set status {enable|disable}
    set trap-status {enable|disable}
    set trapevent {cpu ha ip-change logdisk mem raid remote-storage system}
    set trapport-local <integer>
    set trapport-remote <integer>
  end
```

Variable	Description	Default
edit <username>	Edit or add selected user.	No default
auth-proto {md5 sha}	Select authentication protocol: <ul style="list-style-type: none"> md5 — use HMAC-MD5-96 authentication protocol. sha — use HMAC-SHA-96 authentication protocol. This field is only available if <code>security-level</code> is <code>auth-priv</code> or <code>auth-no-priv</code> .	sha
auth-pwd <password>	Enter the SNMP user authentication password. Maximum 32 characters. This is only available if <code>security-level</code> is <code>auth-priv</code> or <code>auth-no-priv</code> .	No default
priv-proto {aes des}	Select privacy (encryption) protocol: <ul style="list-style-type: none"> aes — use CFB128-AES-128 symmetric encryption. des — use CBC-DES symmetric encryption. This is available if <code>security-level</code> is <code>auth-priv</code> .	aes

Variable	Description	Default
priv-pwd <password>	Enter the SNMP user private password. This is available if security-level is auth-priv.	No default
query-status {enable disable}	Enable or disable SNMP queries for this user.	enable
queryport <port_int>	Enter the number of the port used for SNMP queries. If multiple versions of SNMP are being supported, each version should listen on a different port.	161
security-level <slevel>	Set security level to one of: <ul style="list-style-type: none"> noauthnopriv — no authentication or privacy authnopriv — authentication but no privacy authpriv — authentication and privacy 	no-auth-no-priv
status	Enable or disable the user	enable
trap-status	Enable or disable SNMP traps.	disable
trapevent	cpu ha ip-change logdisk mem raid remote-storage system	cpu mem logdisk system raid ha remote-storage
trapport-local	set local trap port value	162
trapport-remote	set remote trap port value	162

time manual

Use this command to manage the system time.

```

config system time manual
    set daylight-saving-time {enable|disable}
    set zone <0-71>
end

```

Variable	Description	Default
daylight-saving-time	Enable if you want the system to adjust its own clock when its time zone changes between daylight saving time (DST) and standard time.	No default
zone	Specify the code number for the time zone where the appliance is located.	No default

time ntp

Use this command to synchronize the system time using NTP.

syntax

```
config system time ntp
  set ntpsync {enable|disable}
  set ntpserver <string>
  set syncinterval <integer>
end
```

Variable	Description	Default
ntpsync	Enable if you want the system to use NTP.	disable
ntpserver	Specify the IP address or domain name of an NTP server or pool, such as pool.ntp.org. To find an NTP server, go to http://www.ntp.org .	pool.ntp.org
syncinterval	Specify the synchronization time interval in minutes. The range is 1-1440.	60

user

The user commands configure the authentication framework for administrator accounts and user accounts.

radius

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

Syntax

```
config user radius
  edit <server_name>
    set auth-type {chap | ms_chap | ms_chap_v2 | pap}
    set port <port_num>
    set secret <server_password>
    set server <domain>
    set vdom <datasource>
  end
```

Variable	Description	Default
edit <server_name>	Enter a name to identify the RADIUS server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	No default
auth-type { chap ms_chap ms_chap_v2 pap}	Select the authentication method for this RADIUS server. pap chap ms_chap ms_chap_v2	pap
radius-port <radius_port_num>	Change the default RADIUS port for this server. The default port for RADIUS traffic is 1812. Range is 0..65535	1812
secret <server_password>	Enter the RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length.	No default
server <domain>	Enter the RADIUS server domain name or IP address.	No default
vdom <datasource>	Administrative domain for this user	n/a

execute

Use the **execute** commands perform operations on the FortiCore.

backup

Use this command to back up the FortiCore configuration files to a TFTP server.

Syntax

```
execute backup config tftp <filename_str> <TFTP_server_ipv4> [<password>]
```

Variable	Description
<filename_str>	Name of a file on a TFTP server.
<ipaddress>[:port]	TFTP server IP address and optional port.
[<password>]	You can optionally specify a password to protect the contents of the backup file.

Example

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

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

caching

Use this command to show information about a virtual server cache or to clear the cache.

Syntax

```
execute caching {show| clean } <vsname>
```

Variable	Description
show	Show cache statistics
clean	Clear the cache
<vsname>	Name of the virtual server

certificate ca

Use this command to import or export a certificate file. This command is an alternative to **config system certificate ca**.

Syntax

```
execute certificate ca import tftp <filename> <ip>
execute certificate ca export tftp <cert> <filename> <ip>
```

Variable	Description
<cert>	Local (FortiCore) certificate name.
<filename>	Name of the certificate file.
<ip>	IP address of the TFTP server.

certificate config verify

Use this command to verify the certificate file is a supported type.

Syntax

```
execute certificate config verify
```

certificate crl

Use this command to import a certificate file. This command is an alternative to **config system certificate crl**.

Syntax

```
execute certificate crl import tftp <filename> <ip>
```

Variable	Description
<filename>	Name of the certificate file.
<ip>	IP address of the TFTP server.

certificate local

Use this command to import/export a certificate file or to generate/regenerate a certificate file. This command is an alternative to **config system certificate local**.

Syntax

```
execute certificate local import tftp <filename> <ip>
execute certificate local export tftp <cert> <filename> <ip>
execute certificate local generate <cert_name> <keysize> <subject> <country> <state> <org>
    <unit> <email>
execute certificate local regenerate
```

Variable	Description
<cert>	Local (FortiCore) certificate name.
<filename>	Name of the certificate file.
<ip>	IP address of the TFTP server.

certificate remote

Use this command to import or export a remote certificate file. This command is an alternative to **config system certificate remote**.

Syntax

```
execute certificate remote import tftp <filename> <ip>
execute certificate remote export tftp <cert> <filename> <ip>
```

Variable	Description
<cert>	Local (FortiCore) certificate name.
<filename>	Name of the certificate file.
<ip>	IP address of the TFTP server.

date

Use this command to display or set the system date and time.

Syntax

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

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

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

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

Example

This example sets the date to 17 September 2015:

```
execute date 2015-09-17
```

factoryreset

Use this command to reset the system to its default configuration settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings.

Syntax

```
execute factoryreset
```



Back up your configuration first. This command resets all changes that you have made to the configuration file and reverts the system to the default values for the firmware version. Depending on the firmware version, this could include factory default settings for the IP addresses of network interfaces.

formatlogdisk

Use this command to clear the logs from the hard disk and reformat the disk.

Syntax

```
execute formatlogdisk
```



This operation deletes all locally stored log files.

log delete-file

Use this command to delete a log file. Specify the filename of the file you want to delete.

Syntax

```
execute log delete-file <filename>
```

log delete-type

Use this command to delete all log files for a specified log type.

Syntax

```
execute log delete-type {elog|tlog|alog|all}
```

Variable	Description
elog	Delete event logs.
tlog	Delete traffic logs.
alog	Delete security logs.
all	Delete logs for all types.

log list-type

Use this command to list log files for a specified log type.

Syntax

```
execute log list-type {elog|tlog|alog|all}
```

Variable	Description
elog	List event logs.
tlog	List traffic logs.
alog	List security logs.
all	List logs for all types.

log rebuild-db

Use this command to rebuild the log database.

Syntax

```
execute log rebuild-db
```

log tftp

Use this command to download all log files as a single file to the specified TFTP server. The log files are compressed into a tar ball.

Syntax

```
execute log tftp <tftp-ipv4-addr>
```

nslookup

Use this command to perform nslookup queries.

Syntax

```
execute nslookup name {<fqdn>|<ip>}
```

Variable	Description
<fqdn>	Lookup the FQDN for the specified IP address.
<ip>	Lookup the IP address for the specified host.

ping/ping6

Use these commands to perform an ICMP ECHO request (also called a ping) to a host by specifying its fully qualified domain name (FQDN) or IPv4 address, using the options configured by the **execute ping-option/ping6-option** command.

Pings are often used to test IP-layer connectivity during troubleshooting.

Syntax

```
execute {ping|ping6} {<hostname> | <ipaddress>}
```

Example

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

```
#execute ping 172.20.120.16

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

--- 172.20.120.16 ping statistics ---

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

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

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

ping-option, ping6-option

Use these commands to configure the behavior of the execute ping/ping6 command.

Syntax

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

Variable	Description	Default
data-size <bytes>	Specify the datagram size in bytes.	56
df-bit {yes no}	Applicable to ping-option only: set df-bit to yes to prevent the ICMP packet from being fragmented. Set df-bit to no to allow the ICMP packet to be fragmented.	no

Variable	Description	Default
pattern <2-byte_hex>	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the <code>data_size</code> parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default
repeat-count <repeats>	Specify how many times to repeat the ping.	5
source {auto <source-intf_ip>}	Specify the FortiCore interface from which to send the ping. If you specify <code>auto</code> , the system selects the source address and interface based on the route to the <host-name_str> or <host_ip>. Specifying the IP address of a FortiCore interface tests connections to different network segments from the specified interface.	auto
timeout <seconds>	Specify, in seconds, how long to wait until ping times out.	2
tos <service_type>	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted. <ul style="list-style-type: none"> • lowdelay — minimize delay • throughput — maximize throughput • reliability — maximize reliability • lowcost — minimize cost 	0
ttl <hops>	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
validate-reply {yes no}	Select <code>yes</code> to validate reply data.	no
view-settings	Display the current ping-option settings.	No default

Example

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

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

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

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

reboot

Use this command to restart the system.



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

Syntax

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

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

Example

This example shows the reboot command with a message included.

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

reload

Use this command to reload the system.

Syntax

```
execute reload
```

restore

Use the following commands to manually import system files from an FTP/TFTP server as indicated:

- **execute restore config**—Imports a backup of the configuration text file. It is imported from a TFTP server.
- **execute restore config-file**—Imports a tar file that includes the configuration text file, error page files, script files, and ISP address book files. It is imported from a TFTP server.
- **execute restore image**—Imports a firmware image. It is imported from an FTP or TFTP server.

Syntax

```
execute restore config tftp <filename> <ip>  
execute restore image tftp <filename> <ip>
```

Variable	Description
<filename>	File name of a file on the FTP /TFTP server.
<ftp tftp tftp-ha-sync>	FTP or TFTP server.
<ip>	IP address of the FTP/TFTP server.

Example

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

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

shutdown

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



Abruptly powering off your system may corrupt its configuration. Use the reboot and shutdown options in the CLI to ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute shutdown
```

Example

This example shows the shutdown command:

```
execute shutdown
```

An event log message similar to the following is recorded:

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

tcpdump/tcpdump6

You use these commands to capture packets using tcpdump.

```
execute tcpdump <interface> ["Expression"] [<count>] [pcap|text] [<filename>]
```

tcpdump-file

You use this command to manage tcpdump files.

```
execute tcpdump-file {cat <filename> | delete <filename> |list |upload tftp <filename>  
<ip>}
```

traceroute

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

Use this command to use ICMP to test the connection between the FortiCore and another network device, and display information about the time required for network hops between the device and the FortiCore.

Syntax

```
execute traceroute {<hostname> | <ipaddress>}
```

Variable	Description
<hostname>	Fully qualified domain name (FQDN) of the other network device.
<ip>	IP address of the network device

Example

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

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

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

get

Use **get** commands to display configuration settings and values. You must have read permission for the configuration object you want to display.

The **show** commands display user-configured settings but not default settings; the **get** commands display all settings, including both user-configured settings and defaults.

For example, you might get the current DNS settings:

```
get system dns
  primary : 8.8.8.8
  secondary : 0.0.0.0
```

Notice that the command displays the setting for the secondary DNS server, even though it has not been configured, or has reverted to its default value.

Also unlike show, unless used from within an object or table, get requires that you specify the object or table whose settings you want to display.

log setting

Use this command to get information about log settings.

Syntax

```
get log setting {local | remote}
```

Example output

```
# get log setting local
FortiCORE-6200A # get log setting local
status                : enable
rotation-size         : 200
disk-full              : overwrite
loglevel               : information
event-log-status      : enable
event-log-category     : configuration admin app system
traffic-log-status     : disable
attack-log-status      : disable
rate_limit             : 0
```

open-flow channel

Use this command to get information about open-flow channels/

Syntax

```
get open-flow channel status
```

Example output

```
FortiCORE-6200A # get open-flow channel status
channel-type           : tcp
openflow-controller ip : 0.0.0.0
openflow-controller port : 6633
connection-status      : not-configured
connection-uptime      : 0s
openflow-version-negotiated : 3
probe interval         : 5
maximum backoff interval : 8
certificate-name        :
ca-certificate-name     :
datapath-id            : 9187185533130
```

open-flow error-message

Use this command to get information about open-flow error-message counters

Syntax

```
get open-flow error-message counters
```

Example output

```
# get open-flow error-message counters

Flow Message Error Counters-----
flow_mod_fail__unknown           :0
flow_mod_fail__table_full        :0
flow_mod_fail__bad_table_id      :0
flow_mod_fail__overlap           :0
flow_mod_fail__eperm             :0
flow_mod_fail__bad_timeout       :0
flow_mod_fail__bad_command       :0
flow_mod_fail__bad_flags         :0
bad_request__bad_version         :0
bad_request__bad_table_id        :0
bad_action__bad_type             :0
bad_action__bad_len              :0
bad_action__bad_out_port         :0
bad_action__bad_argument         :0
bad_action__too_many             :0
bad_instruction__unknown_inst    :0
bad_instruction__unsup_inst      :0
bad_match__bad_type              :0
bad_match__bad_len               :0
bad_match__bad_dl_addr_mask      :0
bad_match__bad_nw_addr_mask      :0
bad_match__bad_wildcards         :0
bad_match__bad_field             :0
```

```

bad_match__bad_value      :0
bad_match__bad_mask       :0
bad_match__bad_prereq     :0
bad_match__dup_field      :0

```

open-flow flow

Use this command to get information about open-flow flows

Syntax

```

get open-flow flow counters {eastbound | northbound | southbound | westbound}
get open-flow flow detail {eastbound | northbound | southbound | westbound}

```

Example output

```

# get open-flow flow counters eastbound

MatchFields
I:in port V:vlan id S4:source ip v4 D4:destination ip v4 P:protocol type
ST:source port tcp DT:dest port tcp SU:source port udp DU:dest port udp
SS:source port sctp DS:dest port sctp
D:dscp E:ecn S6:source ip v6 D6:destination ip v6
Num flow entries: 1500
Seq      Cookie(in hex)      Prior Actions      MatchFields      Type      Pkt-cts
-----
13501    10000000000000000000      0      Out      IS4PSTDT      IPV4      0
13502    10000000000000000000      0      Out      IS4PSTDT      IPV4      0
13503    10000000000000000000      0      Out      IS4PSTDT      IPV4      0
...

```

open-flow protocol

Use this command to get information about open-flow protocol counters

Syntax

```

get open-flow protocol counters
get open-flow protocol error-counters
get open-flow protocol flow-mod-counters

```

Example output

```

# get open-flow protocol counters

hello-rx      : 10
hello-tx      : 93
echo-request-rx : 4570
echo-request-tx : 9091
echo-reply-rx  : 9088

```

```

echo-reply-tx           : 4570
features-request-rx      : 10
features-reply-tx        : 10
flow-mod-rx              : 60000
port-status-tx           : 0
total-rx                  : 94699
total-tx                  : 13774
error-rx                  : 7
error-tx                  : 0

```

open-flow table

Use this command to get information about open-flow table counters

Syntax

```
get open-flow table counters
```

Example output

```

# get open-flow table counters

num-tables:           : 1
table-id               : 177

total-flow-entries     : 6000
total-ipv4-flow-entries : 6000
total-ipv6-flow-entries : 0
total-l2-flow-entries  : 0

total-flow-entries-NB  : 1500
total-flow-entries-SB  : 1500
total-flow-entries-EB  : 1500
total-flow-entries-WB  : 1500

total-ipv4-flow-entries-NB : 1500
total-ipv4-flow-entries-SB : 1500
total-ipv4-flow-entries-EB : 1500
total-ipv4-flow-entries-WB : 1500

total-ipv6-flow-entries-NB : 0
total-ipv6-flow-entries-SB : 0
total-ipv6-flow-entries-EB : 0
total-ipv6-flow-entries-WB : 0

total-l2-flow-entries-NB : 0
total-l2-flow-entries-SB : 0
total-l2-flow-entries-EB : 0
total-l2-flow-entries-WB : 0

```

port counters

Use this command to get port counters.

Syntax

```
get port counters
get port counters-clear
```

Example output

```
FortiCORE-6200A # get port counters
Port 1
    rx_pkts:                36801
    rx_bytes:                3337274
    tx_pkts:                 733300
    tx_bytes:                1094932800
    rx_dropped:              0
    tx_dropped:              0
    rx_errs:                 0
    tx_errs:                 0
    rx_frame_err:            0
    rx_crc_err:              0
    rx_over_err:             0
    collision_err:           0

    Duration_up_sec:         67844

Port 2
...
```

port status

Use this command to get port status.

Syntax

```
get port status <num>
```

Example output

```
FortiCORE-6200A # get port status 1
Port 1
    Port Direction:         EastBound
    Port Speed:              10G
    Port Duplex:             Yes
    Port State:              Up
```

```
Port Link State:      Up
SFP is present
SFP Vendor Name:  AVAGO
SFP Vendor Part Number:  AFBR-709ASMZ
SFP Trans Com Code:  10G_Base_SR
```

router static

Use this command to get information about static routes

Syntax

```
get router static <No.>
```

Example output

```
# get router static 1
destination      : 0.0.0.0/0
gateway          : 10.160.14.1
distance         : 10
```

service-group info

Use this command to get information about service-groups

Syntax

```
get service-group info
```

Example output

```
# get service-group info

Number of Service Groups Configured:1
Service Group ID:1  Northbound port:1  Southbound port:2
```

session port counters

Use this command to get a count of active TCP sessions on each port. This command is applicable to Conditional Forwarding mode.

Syntax

```
get session port counters
```

Example output

```
FortiCORE-6200A # get session port counters
```

Port	Active Sessions
-----	-----
1	5178
2	39008

system

Use this command to get information about the system

Syntax

```
get system{
  accprofile |
  admin |
  certificate |
  global |
  interface |
  mailserver |
  network-function-group |
  open-flow-channel |
  password-policy |
  performance |
  service-group |
  session-aging |
  snmp |
  status |
  time
}
```

Example output

```
FortiCORE-6200A # get system global
operation-mode      : transect
default-certificate : Factory
hostname            : FortiCORE-6200A
admin-idle-timeout  : 30
port-http           : 80
port-https          : 443
port-ssh            : 22
port-telnet         : 23
language            : english
```

user

Use this command to get information about users

Syntax

```
get user radius <name>
```

Example output

```
FortiCORE-6200A # get user radius test1
server           : 10.10.1.1
port             : 1812
secret           : *
auth-type        : pap
vdom             : root
```

show

Use **show** commands to display configuration settings and values. You must have read permission for the configuration object you want to display.

Show commands display user-configured settings but not default settings; get commands display all settings, including both user-configured settings and defaults.

For example, you might show the current DNS settings:

```
# show system dns
config system dns
    set primary : 8.8.8.8
end
```

Notice that the command does not display the setting for the secondary DNS server. This indicates that it has not been configured, or has reverted to its default value.



High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.