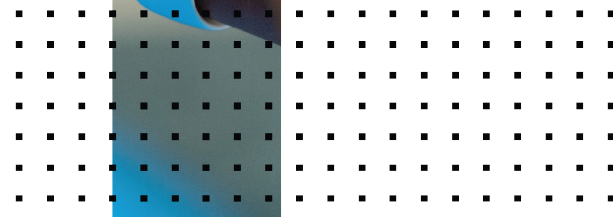


CLI Reference

FortiManager 7.0.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



December 14, 2022

FortiManager 7.0.1 CLI Reference

02-701-686029-20221214

TABLE OF CONTENTS

Change Log	12
Introduction	13
FortiManager documentation	13
What's New in FortiManager 7.0	14
FortiManager 7.0.1	14
FortiManager 7.0.0	16
Using the Command Line Interface	19
CLI command syntax	19
Connecting to the CLI	20
Connecting to the FortiManager console	20
Setting administrative access on an interface	21
Connecting to the FortiManager CLI using SSH	21
Connecting to the FortiManager CLI using the GUI	22
CLI objects	22
CLI command branches	22
config branch	22
get branch	24
show branch	26
execute branch	27
diagnose branch	27
Example command sequences	28
CLI basics	28
Command help	28
Command tree	29
Command completion	29
Recalling commands	29
Editing commands	29
Line continuation	30
Command abbreviation	30
Environment variables	30
Encrypted password support	30
Entering spaces in strings	31
Entering quotation marks in strings	31
Entering a question mark (?) in a string	31
International characters	31
Special characters	31
IPv4 address formats	31
Changing the baud rate	32
Debug log levels	32
Administrative Domains	33
ADOMs overview	33
Configuring ADOMs	34
Concurrent ADOM Access	35

system	37
admin	37
admin group	37
admin ldap	38
admin profile	40
admin radius	47
admin setting	48
admin tacacs	52
admin user	53
alert-console	60
alertemail	61
auto-delete	62
backup all-settings	63
certificate	64
certificate ca	64
certificate crl	65
certificate local	65
certificate oftp	66
certificate remote	67
certificate ssh	67
connector	68
dm	68
dns	70
docker	71
fips	72
fortiview	73
fortiview setting	73
fortiview autocache	73
global	74
Time zones	79
ha	81
General FortiManager HA configuration steps	83
ha-scheduled-check	84
interface	84
locallog	86
locallog setting	86
locallog disk setting	87
locallog filter	89
locallog fortianalyzer (fortianalyzer2, fortianalyzer3) setting	91
locallog memory setting	92
locallog syslogd (syslogd2, syslogd3) setting	93
log	94
log alert	94
log device-disable	95
log interface-stats	95
log ioc	96
log mail-domain	96

log ratelimit	97
log settings	98
log-fetch	101
log-fetch client-profile	101
log-fetch server-setting	103
mail	103
metadata	104
ntp	105
password-policy	105
report	106
report auto-cache	106
report est-browse-time	107
report group	107
report setting	108
route	109
route6	109
saml	110
sniffer	112
snmp	113
snmp community	113
snmp sysinfo	116
snmp user	117
soc-fabric	118
sql	119
syslog	123
workflow approval-matrix	123
fmupdate	125
analyzer virusreport	125
av-ips	126
av-ips advanced-log	126
av-ips web-proxy	126
custom-url-list	127
disk-quota	128
fct-services	128
fds-setting	129
fds-setting push-override	130
fds-setting push-override-to-client	131
fds-setting server-override	132
fds-setting update-schedule	132
fwm-setting	133
multilayer	134
publicnetwork	134
server-access-priorities	135
server-override-status	136
service	136
web-spam	137

web-spam fgd-setting	137
web-spam web-proxy	141
execute	142
add-on-license	142
add-vm-license	143
backup	143
bootimage	145
certificate	145
certificate ca	145
certificate crt	146
certificate local	146
certificate remote	148
chassis	148
console baudrate	149
date	149
device	150
dmserver	150
dmserver delrev	151
dmserver revlist	151
dmserver showconfig	151
dmserver showdev	152
dmserver showrev	152
erasedisk	152
factory-license	153
fgfm reclaim-dev-tunnel	153
fmpolicy	153
fmpolicy check-upgrade-object	153
fmgpolicy clone-adom-object	154
fmpolicy copy-adom-object	154
fmpolicy install-config	155
fmpolicy print-adom-database	155
fmpolicy print-adom-object	155
fmpolicy print-adom-package	156
fmpolicy print-adom-package-assignment	156
fmpolicy print-adom-policyblock	157
fmpolicy print-device-database	157
fmpolicy print-device-object	158
fmpolicy promote-adom-object	158
fmpolicy upload-print-log	158
fmprofile	159
fmprofile copy-to-device	159
fmprofile delete-profile	159
fmprofile export-profile	160
fmprofile import-from-device	160
fmprofile import-profile	160
fmprofile list-profiles	161
fmscript	161

fmscript clean-sched	161
fmscript copy	161
fmscript delete	162
fmscript import	162
fmscript list	163
fmscript run	163
fmscript showlog	164
fmupdate	165
format	166
iotop	166
iotps	167
log	167
log adom disk_quota	168
log device disk_quota	168
log device permissions	168
log device vdom	169
log dlp-files clear	169
log import	170
log ips-pkt clear	170
log quarantine-files clear	170
log storage-warning	171
log-fetch	171
log-fetch client	171
log-fetch server	171
log-integrity	172
lvm	172
max-dev-licence	173
migrate	173
ping	174
ping6	174
raid	175
reboot	175
remove	175
reset	176
reset-sqllog-transfer	176
restore	177
sdns	178
sensor	179
shutdown	179
sql-local	180
sql-query-dataset	180
sql-query-generic	181
sql-report	181
ssh	184
ssh-known-hosts	184
tac	185

time	185
top	186
traceroute	187
traceroute6	187
diagnose	188
auto-delete	188
cdb	189
debug	190
debug application	190
debug backup-oldformat-script-logs	194
debug cdbchk	194
debug cli	195
debug console	195
debug coredump	195
debug crashlog	196
debug disable	196
debug dpm	196
debug enable	197
debug gui	197
debug info	197
debug klog	197
debug reset	198
debug service	198
debug sysinfo	198
debug sysinfo-log	199
debug sysinfo-log-backup	199
debug sysinfo-log-list	199
debug timestamp	199
debug vmd	200
debug vminfo	200
dlp-archives	200
docker	201
dvm	202
dvm adom	202
dvm capability	202
dvm chassis	203
dvm check-integrity	203
dvm csf	203
dvm dbstatus	203
dvm debug	204
dvm device	204
dvm device-tree-update	206
dvm extender	206
dvm fap	207
dvm fsw	207
dvm group	207
dvm lock	207
dvm proc	208

dvm remove	208
dvm supported-platforms	208
dvm task	208
dvm taskline	209
dvm transaction-flag	209
dvm workflow	209
faz-cdb	210
faz-cdb fix	210
faz-cdb reset	210
faz-cdb upgrade	210
fgfm	211
fmnetwork	212
fmnetwork arp	212
fmnetwork interface	212
fmnetwork netstat	212
fmupdate	213
fortilogd	216
fwmanager	217
ha	218
hardware	219
incident	219
license	220
log device	220
pm2	220
report	221
sniffer	221
sql	225
svctools	229
system	230
system admin-session	230
system disk	231
system export	232
system flash	233
system fsck	233
system geoup	233
system geoup-city	234
system interface	234
system mapserver	235
system ntp	235
system print	235
system process	236
system raid	237
system route	237
system route6	237
system server	238
test	238
test application	238

test connection	248
test deploymanager	248
test policy-check	248
test search	249
test sftp	249
upload	249
upload clear	250
upload status	250
vpn	250
get	251
fmupdate analyzer	252
fmupdate av-ips	252
fmupdate custom-url-list	252
fmupdate disk-quota	253
fmupdate fct-services	253
fmupdate fds-setting	253
fmupdate fwm-setting	254
fmupdate multilayer	254
fmupdate publicnetwork	255
fmupdate server-access-priorities	255
fmupdate server-override-status	255
fmupdate service	256
fmupdate web-spam	256
system admin	256
system alert-console	258
system alertemail	258
system auto-delete	258
system backup	259
system certificate	259
system connector	260
system dm	260
system dns	261
system docker	261
system fips	262
system fortiview	262
system global	262
system ha	264
system ha-scheduled-check	264
Syntax	264
system ha-status	264
system interface	265
system locallog	266
system log	267
system log fetch	268
system loglimits	268

system mail	269
system metadata	269
system ntp	269
system password-policy	270
system performance	270
system report	271
system route	271
system route6	272
system saml	272
system sniffer	273
system snmp	273
system soc-fabric	273
system sql	274
system status	275
system syslog	276
system workflow	276
show	277
Appendix A - CLI Error Codes	278

Change Log

Date	Change Description
2021-07-15	Initial release.
2021-07-21	Updated interface on page 84 and system interface on page 265 .
2021-08-12	Updated migrate on page 173 and FortiManager 7.0.1 on page 14 .
2022-02-08	Removed command <code>system alert-event</code> .
2022-03-10	Updated Connecting to the FortiManager CLI using the GUI on page 22 .
2022-06-03	Updated test on page 238 .
2022-12-14	Updated fmupdate on page 165 .

Introduction

FortiManager Centralized Security Management provides a single-pane-of-glass for visibility across the entire Fortinet Security Fabric, as well as to manage Fortinet's security and networking devices to speed the identification of, and response to, security incidents. It allows easy control of the deployment of security policies, FortiGuard content security updates, firmware revisions, and individual configurations for thousands of Fortinet devices.

FortiManager includes:

- Enterprise-class centralized management with single pane-of-glass
- Full control of your network with the Fortinet security fabric
- Common security baseline enforcement for multi-tenancy environments
- Multi-tier management for administrative and virtual domain policy management
- Scalable centralized device & policy management

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager Administration Guide*
This document describes how to set up the FortiManager system and use it to manage supported Fortinet units. It includes information on how to configure multiple Fortinet units, configuring and managing the FortiGate VPN policies, monitoring the status of the managed devices, viewing and analyzing the FortiGate logs, updating the virus and attack signatures, providing web filtering and email filter service to the licensed FortiGate units as a local FDS, firmware revision control and updating the firmware images of the managed units.
- *FortiManager device QuickStart Guides*
These documents are included with your FortiManager system package. Use this document to install and begin working with the FortiManager system and FortiManager GUI.
- *FortiManager Online Help*
You can get online help from the FortiManager GUI. FortiManager online help contains detailed procedures for using the FortiManager GUI to configure and manage FortiGate units.
- *FortiManager CLI Reference*
This document describes how to use the FortiManager Command Line Interface (CLI) and contains references for all FortiManager CLI commands.
- *FortiManager Release Notes*
This document describes new features and enhancements in the FortiManager system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiManager VM Install Guide*
This document describes installing FortiManager VM in your virtual environment.

What's New in FortiManager 7.0

The following tables list the commands and variables that have changed in the CLI.

FortiManager 7.0.1

The table below lists commands which have changed in version 7.0.1.

Command	Change
<code>config fmupdate fds-setting</code>	Variables added: <ul style="list-style-type: none">• system-support-fdc• system-support-fts Variable removed: <ul style="list-style-type: none">• system-support-fsw
<code>config fmupdate fwm-setting</code>	Variable added: <ul style="list-style-type: none">• log
<code>config fmupdate service</code>	Variable added: <ul style="list-style-type: none">• query-iot
<code>config fmupdate web-spam fgd-setting</code>	Variables added: <ul style="list-style-type: none">• iot-cache• iot-log• iot-preload• restrict-iots-dbver
<code>config system admin profile</code>	Variables added: <ul style="list-style-type: none">• ips-baseline-cfg• ips-baseline-ovrd
<code>config system admin setting</code>	Variable added: <ul style="list-style-type: none">• central-ftgd-local-cat-id
<code>config system docker</code>	Variables added: <ul style="list-style-type: none">• fortiaips• fsmcollector• universalconnector
<code>config system ha-scheduled-check</code>	Command added
<code>config system locallog {syslogd syslogd2 syslogd3} setting</code>	Variables added: <ul style="list-style-type: none">• cert• reliable

Command	Change
	<ul style="list-style-type: none"> secure-connection
<code>config system saml</code>	Variable added: <ul style="list-style-type: none"> user-auto-create
<code>diagnose docker</code>	Command added: <ul style="list-style-type: none"> reset Command updated: <ul style="list-style-type: none"> upgrade
<code>diagnose faz-cdb fix</code>	Command added
<code>diagnose fmupdate</code>	Commands added: <ul style="list-style-type: none"> crdb priority-download
<code>diagnose fortilogd lograte-device</code>	Command updated
<code>diagnose ha</code>	Command renamed: <ul style="list-style-type: none"> dbhash to check-data Command renamed and updated: <ul style="list-style-type: none"> dbhash-report to data-check-report
<code>diagnose system disk</code>	Command added: <ul style="list-style-type: none"> usage
<code>diagnose system print</code>	Command updated: <ul style="list-style-type: none"> df
<code>execute certificate</code>	Command added: <ul style="list-style-type: none"> crl
<code>execute certificate ca</code>	Command updated: <ul style="list-style-type: none"> import
<code>execute certificate local</code>	Command updated: <ul style="list-style-type: none"> import
<code>execute fmpolicy</code>	Command added: <ul style="list-style-type: none"> print-adom-package-assignment
<code>execute fmupdate</code>	Command added: <ul style="list-style-type: none"> fgd-db-merge
<code>execute restore image {scp sftp}</code>	Command added
<code>get system ha-status</code>	Command updated

FortiManager 7.0.0

The table below lists commands which have changed in version 7.0.0.

Command	Change
<code>config system admin profile</code>	Variables added: <ul style="list-style-type: none"> • fabric-viewer • run-report • script-access • triage-events • update-incidents
<code>config system admin setting</code>	Variables added: <ul style="list-style-type: none"> • auth-addr • auth-port • idle_timeout_api • idle_timeout_gui
<code>config system admin user</code>	Variables added: <ul style="list-style-type: none"> • login-max • use-global-theme • user-theme
<code>config system docker</code>	Variables added: <ul style="list-style-type: none"> • docker-user-login-max • fortisoar
<code>config system global</code>	Variables added: <ul style="list-style-type: none"> • object-revision-db-max • object-revision-mandatory-note • object-revision-object-max • object-revision-status
<code>config system log</code>	Command added: <ul style="list-style-type: none"> • ratelimit
<code>config system mail</code>	Variables added: <ul style="list-style-type: none"> • auth-type • local-cert
<code>config system saml</code>	Variable added: <ul style="list-style-type: none"> • forticloud-sso
<code>config system soc-fabric</code>	Command added
<code>diagnose debug application</code>	Command added: <ul style="list-style-type: none"> • fabricsyncd
<code>diagnose docker upgrade</code>	Command updated

Command	Change
<code>diagnose dvm debug</code>	Command added: <ul style="list-style-type: none"> • trace
<code>diagnose dvm extender</code>	Command removed: <ul style="list-style-type: none"> • import-dataplan-to-adom Commands renamed and updated: <ul style="list-style-type: none"> • import-sim-profile-to-adom to import-template • set-sim-profile to set-template
<code>diagnose fmupdate check-disk-quota</code>	Command updated
<code>diagnose fwmanager</code>	Command added: <ul style="list-style-type: none"> • image-delete Commands removed: <ul style="list-style-type: none"> • delete-all • delete-imported-images • delete-official-images • delete-serverlist • imported-imagelist • reset-schedule-database • serverlist Command renamed: <ul style="list-style-type: none"> • download-image to image-download Command renamed and updated: <ul style="list-style-type: none"> • official-imagelist to image-list Command updated: <ul style="list-style-type: none"> • fwm-log
<code>diagnose ha</code>	Commands added: <ul style="list-style-type: none"> • dbhash action • dbhash-report
<code>diagnose sql debug hcache-aggr</code>	Command updated: <ul style="list-style-type: none"> • show
<code>diagnose sql debug logview</code>	Command added
<code>diagnose sql debug sqlqry</code>	Command updated: <ul style="list-style-type: none"> • show
<code>diagnose system export</code>	Commands updated: <ul style="list-style-type: none"> • crashlog • dminstallog • upgradelog

Command	Change
	<ul style="list-style-type: none"> • vartmp
diagnose test application	Command added: <ul style="list-style-type: none"> • fabricsyncd
execute tac	Command updated: <ul style="list-style-type: none"> • report Command added: <ul style="list-style-type: none"> • upload
get system ha-status	Command added

Using the Command Line Interface

This chapter explains how to connect to the CLI and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

This chapter describes:

- [CLI command syntax](#)
- [Connecting to the CLI](#)
- [CLI objects](#)
- [CLI command branches](#)
- [CLI basics](#)

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets < > indicate variables.
- Vertical bar and curly brackets { | } separate alternative, mutually exclusive required keywords.

For example:

```
set protocol {ftp | sftp}
```

You can enter `set protocol ftp` or `set protocol sftp`.

- Square brackets [] indicate that a variable is optional.

For example:

```
show system interface [<name_str>]
```

To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the Port1 interface, you can enter `show system interface port1`.

- A space separates options that can be entered in any combination and must be separated by spaces.

For example:

```
set allowaccess {https ping}
```

You can enter any of the following:

```
set allowaccess ping
```

```
set allowaccess https ping
```

```
set allowaccess http https ping snmp soc-fabric ssh webservice
```

In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.

- Special characters:
 - The \ is supported to escape spaces or as a line continuation character.
 - The single quotation mark ' and the double quotation mark " are supported, but must be used in pairs.
 - If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Connecting to the CLI

You can use a direct console connection, SSH, or the CLI console widget in the GUI to connect to the FortiManager CLI. For more information, see the [FortiManager Administration Guide](#) and your device's [QuickStart Guide](#).

- [Connecting to the FortiManager console](#)
- [Setting administrative access on an interface](#)
- [Connecting to the FortiManager CLI using SSH](#)
- [Connecting to the FortiManager CLI using the GUI](#)

Connecting to the FortiManager console

To connect to the FortiManager console, you need:

- a computer with an available communications port
- a console cable, provided with your FortiManager unit, to connect the FortiManager console port and a communications port on your computer
- terminal emulation software, such as HyperTerminal for Windows.



The following procedure describes how to connect to the FortiManager CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI:

1. Connect the FortiManager console port to the available communications port on your computer.
2. Make sure that the FortiManager unit is powered on.
3. Start a terminal emulation program on the management computer, select the COM port, and use the following settings:

COM port	COM1
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

4. Press `Enter` to connect to the FortiManager CLI.
5. In the log in prompt, enter the username and password.
The default log in is username: `admin`, and no password.
You have connected to the FortiManager CLI, and you can enter CLI commands.

Setting administrative access on an interface

To perform administrative functions through a FortiManager network interface, you must enable the required types of administrative access on the interface to which your management computer connects. Access to the CLI requires Secure Shell (SSH) access. If you want to use the GUI, you need HTTPS access.

To use the GUI to configure FortiManager interfaces for SSH access, see the [FortiManager Administration Guide](#).

To use the CLI to configure SSH access:

1. Connect and log into the CLI using the FortiManager console port and your terminal emulation software.
2. Use the following command to configure an interface to accept SSH connections:

```
config system interface
  edit <interface_name>
    set allowaccess <access_types>
  end
```

Where `<interface_name>` is the name of the FortiManager interface to be configured to allow administrative access, and `<access_types>` is a whitespace-separated list of access types to enable.

For example, to configure port1 to accept HTTPS and SSH connections, enter:

```
config system interface
  edit port1
    set allowaccess https ssh
  end
```



Remember to press `Enter` at the end of each line in the command example. Also, type `end` and press `Enter` to commit the changes to the FortiManager configuration.

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

```
get system interface <interface_name>
```

The CLI displays the settings, including the management access settings, for the named interface.

Connecting to the FortiManager CLI using SSH

SSH provides strong secure authentication and secure communications to the FortiManager CLI from your internal network or the internet. Once the FortiManager unit is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiManager CLI.

To connect to the CLI using SSH:

1. Install and start an SSH client.
2. Connect to a FortiManager interface that is configured for SSH connections.
3. Enter a valid administrator name and press `Enter`.
4. Enter the password for this administrator and press `Enter`.
The FortiManager model name followed by a # is displayed.
You have connected to the FortiManager CLI, and you can enter CLI commands.

Connecting to the FortiManager CLI using the GUI

The GUI also provides a CLI console widget.

To connect to the CLI using the GUI:

1. Connect to the GUI and log in.
For information about how to do this, see the [FortiManager Administration Guide](#).
2. From the *Tools* dropdown in the banner, click *>_ CLI Console*.
The *CLI Console* widget opens.

CLI objects

The FortiManager CLI is based on configurable objects. The top-level objects are the basic components of FortiManager functionality. Each has its own chapter in this guide.

fmupdate	Configures settings related to FortiGuard service updates and the FortiManager unit's built-in FDS. See fmupdate on page 125 .
system	Configures options related to the overall operation of the FortiManager unit, such as interfaces, virtual domains, and administrators. See system on page 37 .

There is a chapter in this manual for each of these top-level objects. Each of these objects contains more specific lower level objects. For example, the system object contains objects for administrators, dns, interfaces, and so on.

CLI command branches

The FortiManager CLI consists of the following command branches:

config branch	execute branch
get branch	diagnose branch
show branch	

Examples showing how to enter command sequences within each branch are provided in the following sections.

config branch

The `config` commands configure objects of FortiManager functionality. Top-level objects are not configurable, they are containers for more specific lower level objects. For example, the system object contains administrators, DNS addresses, interfaces, routes, and so on. When these objects have multiple sub-objects, such as administrators or routes, they are organized in the form of a table. You can add, delete, or edit the entries in the table. Table entries each consist of keywords that you can set to particular values. Simpler objects, such as system DNS, are a single set of keywords.

To configure an object, you use the `config` command to navigate to the object's command "shell". For example, to configure administrators, you enter the command

```
config system admin user
```

The command prompt changes to show that you are in the admin shell.

```
(user) #
```

This is a table shell. You can use any of the following commands:

delete	Remove an entry from the FortiManager configuration. For example in the <code>config system admin shell</code> , type <code>delete newadmin</code> and press <code>Enter</code> to delete the administrator account named <code>newadmin</code> .
edit	Add an entry to the FortiManager configuration or edit an existing entry. For example in the <code>config system admin shell</code> : <ul style="list-style-type: none"> • type <code>edit admin</code> and press <code>Enter</code> to edit the settings for the default admin administrator account. • type <code>edit newadmin</code> and press <code>Enter</code> to create a new administrator account with the name <code>newadmin</code> and to edit the default settings for the new administrator account.
end	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. You return to the root FortiManager CLI prompt. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.
get	List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the keywords and their values.
purge	Remove all entries configured in the current shell. For example in the <code>config user local shell</code> : <ul style="list-style-type: none"> • type <code>get</code> to see the list of user names added to the FortiManager configuration, • type <code>purge</code> and then <code>y</code> to confirm that you want to purge all the user names, • type <code>get</code> again to confirm that no user names are displayed.
show	Show changes to the default configuration as configuration commands.

If you enter the `get` command, you see a list of the entries in the table of administrators. To add a new administrator, you enter the `edit` command with a new administrator name:

```
edit admin_1
```

The FortiManager unit acknowledges the new table entry and changes the command prompt to show that you are now editing the new entry:

```
new entry 'admin_1' added
(admin_1) #
```

From this prompt, you can use any of the following commands:

abort	Exit an edit shell without saving the configuration.
--------------	--

config	In a few cases, there are subcommands that you access using a second config command while editing a table entry. An example of this is the command to add host definitions to an SNMP community.
end	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.
get	List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the keywords and their values.
next	Save the changes you have made in the current shell and continue working in the shell. For example if you want to add several new admin user accounts enter the <code>config system admin user shell</code> . <ol style="list-style-type: none"> 1. Enter <code>edit User1</code> and press <code>Enter</code>. 2. Use the <code>set</code> commands to configure the values for the new admin account. 3. Enter <code>next</code> to save the configuration for User1 without leaving the <code>config system admin user shell</code>. 4. Continue using the <code>edit</code>, <code>set</code>, and <code>next</code> commands to continue adding admin user accounts. 5. Type <code>end</code> then press <code>Enter</code> to save the last configuration and leave the shell.
set	Assign values. For example from the <code>edit admin</code> command shell, typing <code>set passwd newpass</code> changes the password of the admin administrator account to <code>newpass</code> . Note: When using a <code>set</code> command to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
show	Show changes to the default configuration in the form of configuration commands.
unset	Reset values to defaults. For example from the <code>edit admin</code> command shell, typing <code>unset passwd</code> resets the password of the admin administrator account to the default of no password.

The `config` branch is organized into configuration shells. You can complete and save the configuration within each shell for that shell, or you can leave the shell without saving the configuration. You can only use the configuration commands for the shell that you are working in. To use the configuration commands for another shell you must leave the shell you are working in and enter the other shell.

The root prompt is the FortiManager host or model name followed by a `#`.

get branch

Use `get` to display settings. You can use `get` within a `config` shell to display the settings for that shell, or you can use `get` with a full path to display the settings for the specified shell.

To use `get` from the root prompt, you must include a path to a shell.

Example

When you type `get` in the `config system admin user shell`, the list of administrators is displayed.

At the `(user) #` prompt, type:

```
get
```

The screen displays:

```
== [ admin ]
userid: admin
== [ admin2 ]
userid: admin2
== [ admin3 ]
userid: admin3
```

Example

When you type `get` in the `admin` user shell, the configuration values for the `admin` administrator account are displayed.

```
edit admin
```

At the `(admin) #` prompt, type:

```
get
```

The screen displays:

```
userid : admin
password : *
trusthost1 : 0.0.0.0 0.0.0.0
trusthost2 : 0.0.0.0 0.0.0.0
trusthost3 : 0.0.0.0 0.0.0.0
trusthost4 : 0.0.0.0 0.0.0.0
trusthost5 : 0.0.0.0 0.0.0.0
trusthost6 : 0.0.0.0 0.0.0.0
trusthost7 : 0.0.0.0 0.0.0.0
trusthost8 : 0.0.0.0 0.0.0.0
trusthost9 : 0.0.0.0 0.0.0.0
trusthost10 : 127.0.0.1 255.255.255.255
ipv6_trusthost1 : ::/0
ipv6_trusthost2 : ::/0
ipv6_trusthost3 : ::/0
ipv6_trusthost4 : ::/0
ipv6_trusthost5 : ::/0
ipv6_trusthost6 : ::/0
ipv6_trusthost7 : ::/0
ipv6_trusthost8 : ::/0
ipv6_trusthost9 : ::/0
ipv6_trusthost10 : ::1/128
profileid : Super_User
adom:
  == [ all_adoms ]
  adom-name: all_adoms
policy-package:
  == [ all_policy_packages ]
  policy-package-name: all_policy_packages
restrict-access : disable
restrict-dev-vdom:
description : (null)
user_type : local
ssh-public-key1 :
ssh-public-key2 :
ssh-public-key3 :
meta-data:
last-name : (null)
```

```
first-name : (null)
email-address : (null)
phone-number : (null)
mobile-number : (null)
pager-number : (null)
hidden : 0
dashboard-tabs:
dashboard:
  == [ 6 ]
  moduleid: 6
  == [ 1 ]
  moduleid: 1
  == [ 2 ]
  moduleid: 2
  == [ 3 ]
  moduleid: 3
  == [ 4 ]
  moduleid: 4
  == [ 5 ]
  moduleid: 5
```

Example

You want to confirm the IPv4 address and netmask of the port1 interface from the root prompt.

At the # prompt, type:

```
get system interface port1
```

The screen displays:

```
name : port1
status : up
ip : 10.2.115.5 255.255.0.0
allowaccess : ping https ssh snmp soc-fabric http webservice
serviceaccess : fgtupdates webfilter-antispam webfilter antispam
speed : auto
description : (null)
alias : (null)
ipv6:
  ip6-address: ::/0 ip6-allowaccess:
```

show branch

Use `show` to display the FortiManager unit configuration. Only changes to the default configuration are displayed. You can use `show` within a `config` shell to display the configuration of that shell, or you can use `show` with a full path to display the configuration of the specified shell.

To display the configuration of all `config` shells, you can use `show` from the root prompt.

Example

When you type `show` and press `Enter` within the `port1` interface shell, the changes to the default interface configuration are displayed.

At the `(port1) #` prompt, type:

```
show
```

The screen displays:

```
config system interface
  edit "port1"
    set ip 10.2.115.5 255.255.0.0
    set allowaccess ping https ssh snmp soc-fabric http webservice
    set serviceaccess fgtupdates webfilter-antispam webfilter antispam
  next
end
```

Example

You are working in the `port1` interface shell and want to see the `system dns` configuration. At the `(port1)#` prompt, type:

```
show system dns
```

The screen displays:

```
config system dns
  set primary 172.39.139.53
  set secondary 172.39.139.63
end
```

execute branch

Use `execute` to run static commands, to reset the FortiManager unit to factory defaults, or to back up or restore the FortiManager configuration. The execute commands are available only from the root prompt.

Example

At the root prompt, type:

```
execute reboot
```

and press `Enter` to restart the FortiManager unit.

diagnose branch

Commands in the `diagnose` branch are used for debugging the operation of the FortiManager unit and to set parameters for displaying different levels of diagnostic information. The `diagnose` commands are not documented in this CLI Reference.



`diagnose` commands are intended for advanced users only. Contact Fortinet Customer Support before using these commands.

Example command sequences



The command prompt changes for each shell.

To configure the primary and secondary DNS server addresses:

1. Starting at the root prompt, type:
`config system dns`
and press **Enter**. The prompt changes to `(dns) #`.
2. At the `(dns) #` prompt, type `?`
The following options are displayed:
`set`
`unset`
`get`
`show`
`abort`
`end`
3. Enter `set ?`
The following options are displayed:
`primary`
`secondary`
4. To set the primary DNS server address to `172.16.100.100`, type:
`set primary 172.16.100.100`
and press **Enter**.
5. To set the secondary DNS server address to `207.104.200.1`, type:
`set secondary 207.104.200.1`
and press **Enter**.
6. To restore the primary DNS server address to the default address, type `unset primary` and press **Enter**.
If you want to leave the `config system dns` shell without saving your changes, type `abort` and press **Enter**.
7. To save your changes and exit the `dns` sub-shell, type `end` and press **Enter**.
8. To confirm your changes have taken effect after leaving the `dns` sub-shell, type `get system dns` and press **Enter**.

CLI basics

This section covers command line interface basic information.

Command help

You can press the question mark (`?`) key to display command help.

- Press the question mark (`?`) key at the command prompt to display a list of the commands available and a description of each command.

- Enter a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Enter a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.

Command tree

Enter `tree` to display the FortiManager CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file. For `config` commands, use the `tree` command to view all available variables and sub-commands.

Command completion

You can use the tab key or the question mark (?) key to complete commands.

- You can press the tab key at any prompt to scroll through the options available for that prompt.
- You can type the first characters of any command and press the tab key or the question mark (?) key to complete the command or to scroll through the options that are available at the current cursor position.
- After completing the first word of a command, you can press the space bar and then the tab key to scroll through the options available at the current cursor position.

Recalling commands

You can recall previously entered commands by using the Up and Down arrow keys to scroll through commands you have entered.

Editing commands

Use the left and right arrow keys to move the cursor back and forth in a recalled command. You can also use Backspace and Delete keys, and the control keys listed in the following table to edit the command.

Function	Key combination
Beginning of line	Control key + A
End of line	Control key + E
Back one character	Control key + B
Forward one character	Control key + F
Delete current character	Control key + D
Previous command	Control key + P
Next command	Control key + N
Abort the command	Control key + C
If used at the root prompt, exit the CLI	Control key + C

Line continuation

To break a long command over multiple lines, use a \ at the end of each line.

Command abbreviation

You can abbreviate commands and command options to the smallest number of non-ambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st`.

Environment variables

The FortiManager CLI supports several environment variables.

\$USERFROM	The management access type (SSH, Telnet and so on) and the IPv4 address of the logged in administrator.
\$USERNAME	The user account name of the logged in administrator.
\$SerialNum	The serial number of the FortiManager unit.

Variable names are case sensitive. In the following example, when entering the variable, you can type `$` followed by a tab to auto-complete the variable to ensure that you have the exact spelling and case. Continue pressing tab until the variable you want to use is displayed.

```
config system global
  set hostname $SerialNum
end
```

Encrypted password support

After you enter a clear text password using the CLI, the FortiManager unit encrypts the password and stores it in the configuration file with the prefix ENC. For example:

```
show system admin user user1
config system admin user
  edit "user1"
    set password ENC
      UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMFC9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcX
      dnQxskRcU3E9XqOit82PgScwzGzGuJ5a9f
    set profileid "Standard_User"
  next
end
```

It is also possible to enter an already encrypted password. For example, type:

```
config system admin
```

then press Enter.

Enter:

```
edit user1
```

then press Enter.

Enter:

```
set password ENC
    UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMFC9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxsk
    RcU3E9XqOit82PgScwzGzGuJ5a9f
```

then press Enter.

Enter:

```
end
```

then press Enter.

Entering spaces in strings

When a string value contains a space, do one of the following:

- Enclose the string in quotation marks, "Security Administrator", for example.
- Enclose the string in single quotes, 'Security Administrator', for example.
- Use a backslash ("\") preceding the space, Security\ Administrator, for example.

Entering quotation marks in strings

If you want to include a quotation mark, single quote, or apostrophe in a string, you must precede the character with a backslash character. To include a backslash, enter two backslashes.

Entering a question mark (?) in a string

If you want to include a question mark (?) in a string, you must precede the question mark with CTRL-V. Entering a question mark without first entering CTRL-V causes the CLI to display possible command completions, terminating the string.

International characters

The CLI supports international characters in strings.

Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields, but you can use them in passwords. If you use the apostrophe (') or quote (") character, you must precede it with a backslash (\) character when entering it in the CLI `set` command.

IPv4 address formats

You can enter an IPv4 address and subnet using either dotted decimal or slash-bit format. For example you can type either:

```
set ip 192.168.1.1 255.255.255.0
```

or

```
set ip 192.168.1.1/24
```

The IPv4 address is displayed in the configuration file in dotted decimal format.

Changing the baud rate

Using `execute console baudrate`, you can change the default console connection baud rate.



Changing the default baud rate is not available on all models.

Debug log levels

The following table lists available debug log levels on your FortiManager.

0	Emergency	The system has become unusable.
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An erroneous condition exists and functionality is probably affected.
4	Warning	Function might be affected.
5	Notice	Notification of normal events.
6	Information	General information about system operations.
7	Debug	Detailed information useful for debugging purposes.
8	Maximum	Maximum log level.

Administrative Domains

This chapter provides information about the ADOM functionality in FortiManager .

ADOMs overview

FortiManager can manage a large number of Fortinet devices. ADOMs enable administrators to manage only those devices that are specific to their geographic location or business division. This also includes FortiGate units with multiple configured VDOMs.

If ADOMs are enabled, each administrator account is tied to an administrative domain. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. The one exception is the `admin` administrator account which can see and maintain all administrative domains and the devices within those domains.

Administrative domains are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator. For more information, see [Configuring ADOMs on page 34](#).

The default and maximum number of administrative domains you can add depends on the FortiManager system model. The table below outlines these limits.

FortiManager Model	Administrative Domain / Network Devices
FMG-100C	30 / 30
FMG-200D	30 / 30
FMG-300D	300 / 300
FMG-400C	300 / 300
FMG-1000C	800 / 800
FMG-1000D	1000 / 1000
FMG-3000C	5000 / 5000
FMG-3900E	5000 / 5000
FMG-4000D	4000 / 4000
FMG-4000E	4000 / 4000
FMG-VM-Base	10 / 10
FMG-VM-10-UG	+10 / +10
FMG-VM-100-UG	+100 / +100
FMG-VM-1000-UG	+1000 / +1000
FMG-VM-5000-UG	+5000 / +5000
FMG-VM-U-UG	+10000 / +10000

Configuring ADOMs

To use administrative domains, the `admin` administrator must first enable the feature, create ADOMs, and assign existing FortiManager administrators to ADOMs.



Enabling ADOMs moves non-global configuration items to the `root` ADOM. Back up the FortiManager unit configuration before enabling ADOMs.



ADOMs must be enabled before adding FortiMail, FortiWeb, and FortiCarrier devices to the FortiManager system. FortiMail and FortiWeb devices are added to their respective pre-configured ADOMs.



In FortiManager 5.0.3 and later, FortiGate and FortiCarrier devices can no longer be grouped into the same ADOM. FortiCarrier devices should be grouped into a dedicated FortiCarrier ADOM.

Within the CLI, you can enable ADOMs and set the administrator ADOM. To configure the ADOMs, you must use the GUI.

To Enable/disable ADOMs:

Enter the following CLI command:

```
config system global
  set adom-status {enable | disable}
end
```

An administrative domain has two modes: normal and advanced. Normal mode is the default device mode. In normal mode, a FortiGate unit can only be added to a single administrative domain. In advanced mode, you can assign different VDOMs from the same FortiGate to multiple administrative domains.



Enabling the advanced mode option will result in more complicated management scenarios. It is recommended only for advanced users.

To change ADOM device modes:

Enter the following CLI command:

```
config system global
  set adom-mode {advanced | normal}
end
```

To assign an administrator to an ADOM:

Enter the following CLI command:

```
config system admin user
```

```
edit <name>
    set adom <adom_name>
next
end
```

where <name> is the administrator user name and <adom_name> is the ADOM name.

Concurrent ADOM Access

System administrators can enable/disable concurrent access to the same ADOM if multiple administrators are responsible for managing a single ADOM. When enabled, multiple administrators can log in to the same ADOM concurrently. When disabled, only a single administrator has read/write access to the ADOM, while all other administrators have read-only access.

Concurrent ADOM access can be enabled or disabled using the CLI or the GUI. The settings apply to all ADOMs, unless you set workspace-mode to per-ADOM. When per-ADOM is enabled, you can apply different settings to each ADOM by using the GUI.



Concurrent ADOM access is enabled by default. This can cause conflicts if two administrators attempt to make configuration changes to the same ADOM concurrently.

To enable ADOM locking and disable concurrent ADOM access for all ADOMs:

```
config system global
    set workspace-mode normal
end
```

To disable ADOM locking and enable concurrent ADOM access for all ADOMs:

```
config system global
    set workspace-mode disabled
    Warning: disabling workspaces may cause some logged in users to lose their unsaved
    data. Do you want to continue? (y/n) y
end
```

To enable workspace workflow mode for all ADOMs:

```
config system global
    set workspace-mode workflow
end
```



When workflow mode is enabled, then the admin will have an extra option in the admin page under profile to allow the admin to approve or reject workflow requests.

To enable per-ADOM workspace mode settings:

```
config system global
    set workspace-mode per-adom
end
```



When per-adom is enabled, then the admin can set the workspace mode for each ADOM by using the GUI.

system

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



FortiManager CLI commands and variables are case sensitive.

admin	dns	locallog	route	workflow approval-matrix
alert-console	docker	log	route6	
alertemail	fips	log-fetch	saml	
auto-delete	fortiview	mail	sniffer	
backup all-settings	global	metadata	snmp	
certificate	ha	ntp	soc-fabric	
connector	ha-scheduled-check	password-policy	sql	
dm	interface	report	syslog	



TCP port numbers cannot be used by multiple services at the same time with the same IP address. If a port is already in use, it cannot be assigned to another service. For example, HTTPS and HTTP cannot have the same port number.

admin

Use the following commands to configure admin related settings.

admin group

Use this command to add, edit, and delete admin user groups.

Syntax

```
config system admin group
  edit <group>
    set member <string>
  end
```

Variable	Description
<group>	Enter the name of the group you are editing or enter a new name to create an entry (character limit = 63).
member <string>	Add group members.

admin ldap

Use this command to add, edit, and delete Lightweight Directory Access Protocol (LDAP) users.

Syntax

```
config system admin ldap
edit <server>
    set adom-attr <string>
    set adom <adom-name>
    set attributes <filter>
    set ca-cert <string>
    set cnid <string>
    set connect-timeout <integer>
    set dn <string>
    set filter <string>
    set group <string>
    set memberof-attr <string>
    set password <passwd>
    set port <integer>
    set profile-attr <string>
    set secondary-server <string>
    set secure {disable | ldaps | starttls}
    set server <string>
    set tertiary-server <string>
    set type {anonymous | regular | simple}
    set username <string>
end
```

Variable	Description
<server>	Enter the name of the LDAP server or enter a new name to create an entry (character limit = 63).
adom-attr <string>	The attribute used to retrieve ADOM.
adom <adom-name>	Set the ADOM name to link to the LDAP configuration.
attributes <filter>	Attributes used for group searching (for multi-attributes, a use comma as a separator). For example: <ul style="list-style-type: none"> member uniquemember member,uniquemember

Variable	Description
ca-cert <string>	CA certificate name. This variable appears only when <code>secure</code> is set to <code>ldaps</code> or <code>starttls</code> .
cnid <string>	Enter the common name identifier (character limit = 20, default = <code>cn</code>).
connect-timeout <integer>	Set the LDAP connection timeout, in milliseconds (default = 500).
dn <string>	Enter the distinguished name.
filter <string>	Enter content for group searching. For example: (&(objectcategory=group)(member=*)) (&(objectclass=groupofnames)(member=*)) (&(objectclass=groupofuniquenames)(uniquemember=*)) (&(objectclass=posixgroup)(memberuid=*))
group <string>	Enter an authorization group. The authentication user must be a member of this group (full DN) on the server.
memberof-attr <string>	The attribute used to retrieve <code>memberof</code> .
password <passwd>	Enter a password for the username above. This variable appears only when <code>type</code> is set to <code>regular</code> .
port <integer>	Enter the port number for LDAP server communication (1 - 65535, default = 389).
profile-attr <string>	The attribute used to retrieve admin profile.
secondary-server <string>	Enter the secondary LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
secure {disable ldaps starttls}	Set the SSL connection type: <ul style="list-style-type: none"> <code>disable</code>: no SSL (default). <code>ldaps</code>: use LDAPS <code>starttls</code>: use STARTTLS
server <string>	Enter the LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
tertiary-server <string>	Enter the tertiary LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
type {anonymous regular simple}	Set a binding type: <ul style="list-style-type: none"> <code>anonymous</code>: Bind using anonymous user search <code>regular</code>: Bind using username/password and then search <code>simple</code>: Simple password authentication without search (default)
username <string>	Enter a username. This variable appears only when <code>type</code> is set to <code>regular</code> .

Example

This example shows how to add the LDAP user `user1` at the IPv4 address `206.205.204.203`.

```
config system admin ldap
edit user1
set server 206.205.204.203
set dn techdoc
```

```
set type regular
set username auth1
set password auth1_pwd
set group techdoc
end
```

admin profile

Use this command to configure access profiles. In a newly-created access profile, no access is enabled. Setting an option to `none` hides it from administrators with that profile assigned.

Syntax

```
config system admin profile
edit <profile>
    set adom-lock {none | read | read-write}
    set adom-policy-packages {none | read | read-write}
    set adom-switch {none | read | read-write}
    set allow-to-install {enable | disable}
    set app-filter {enable | disable}
    set assignment {none | read | read-write}
    set change-password {enable | disable}
    set config-retrieve {none | read | read-write}
    set config-revert {none | read | read-write}
    set consistency-check {none | read | read-write}
    set datamask {enable | disable}
    set datamask-custom-priority {enable | disable}
    set datamask-fields <fields>
    set datamask-key <passwd>
    set datamask-unmasked-time <integer>
    set deploy-management {none | read | read-write}
    set description <string>
    set device-ap {none | read | read-write}
    set device-config {none | read | read-write}
    set device-forticlient {none | read | read-write}
    set device-fortiswitch {none | read | read-write}
    set device-manager {none | read | read-write}
    set device-op {none | read | read-write}
    set device-policy-package-lock {none | read | read-write}
    set device-profile {none | read | read-write}
    set device-revision-deletion {none | read | read-write}
    set device-wan-link-load-balance {none | read | read-write}
    set event-management {none | read | read-write}
    set extension-access {none | read | read-write}
    set fabric-viewer {none | read | read-write}
    set fgd_center {none | read | read-write}
    set fgd-center-advanced {none | read | read-write}
    set fgd-center-fmw-mgmt {none | read | read-write}
    set fgd-center-licensing {none | read | read-write}
    set global-policy-packages {none | read | read-write}
    set import-policy-packages {none | read | read-write}
    set intf-mapping {none | read | read-write}
    set ips-baseline-cfg {none | read | read-write}
    set ips-baseline-ovrd {enable | disable}
```

```

set ips-filter {enable | disable}
set log-viewer {none | read | read-write}
set policy-objects {none | read | read-write}
set read-passwd {none | read | read-write}
set realtime-monitor {none | read | read-write}
set report-viewer {none | read | read-write}
set run-report {none | read | read-write}
set scope (Not Applicable)
set script-access {none | read | read-write}
set set-install-targets {none | read | read-write}
set super-user-profile {enable | disable}
set system-setting {none | read | read-write}
set term-access {none | read | read-write}
set triage-events {none | read | read-write}
set type {restricted | system}
set update-incidents {none | read | read-write}
set vpn-manager {none | read | read-write}
set web-filter {enable | disable}
config datamask-custom-fields
  edit <field>
    set field-category {alert | all | fortiview | log | euba}
    set field-status {enable | disable}
    set field-type {email | ip | mac | string}
  next
end

```

Variable	Description
<profile>	Enter the name of the access profile, enter a new name to create a new profile (character limit = 35). The pre-defined access profiles are <i>Super_User</i> , <i>Standard_User</i> , <i>Restricted_User</i> , and <i>Package_User</i> .
adom-lock {none read read-write}	<p>Configure ADOM locking permissions for profile:</p> <ul style="list-style-type: none"> • none: No permission (default). • read: Read permission. • read-write: Read-write permission. <p>Controlled functions: ADOM locking.</p> <p>Dependencies: type must be system</p>
adom-policy-packages {none read read-write}	<p>Enter the level of access to ADOM policy packages.</p> <p>This command corresponds to the Policy Packages & Objects option on the administrator profile settings page in the GUI. It is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: All the operations in ADOMs</p> <p>Dependencies: Install and re-install depends on Install to Devices in DVM settings, type must be system</p>
adom-switch {none read read-write}	<p>Configure administrative domain (ADOM) permissions for this profile (default = none).</p> <p>This command corresponds to the Administrative Domain option in the GUI.</p> <p>Controlled functions: ADOM settings in DVM, ADOM settings in All ADOMs page (under System Settings tab)</p>

Variable	Description
	Dependencies: If <code>system-setting</code> is <code>none</code> , the All ADOMs page is not accessible, <code>type</code> must be <code>system</code>
<code>allow-to-install {enable disable}</code>	Enable/disable allowing restricting users to install objects to the devices (default = enable).
<code>app-filter {enable disable}</code>	Enable/disable IPS Sensor permission for the restricted admin profile (default = disable). Dependencies: <code>type</code> must be <code>restricted</code> .
<code>assignment {none read read-write}</code>	Configure assignment permissions for this profile (default = none). This command corresponds to the Assignment option in the GUI. It is a sub-setting of <code>policy-objects</code> . Controlled functions: Global assignment in Global ADOM Dependencies: <code>type</code> must be <code>system</code>
<code>change-password {enable disable}</code>	Enable/disable allowing restricted users to change their password (default = disable).
<code>config-retrieve {none read read-write}</code>	Set the configuration retrieve settings for this profile (default = none). This command corresponds to the Retrieve Configuration from Devices option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Retrieve configuration from devices Dependencies: <code>type</code> must be <code>system</code>
<code>config-revert {none read read-write}</code>	Set the configuration revert settings for this profile (default = none). This command corresponds to the Revert Configuration from Revision History option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Revert configuration from revision history Dependencies: <code>type</code> must be <code>system</code>
<code>consistency-check {none read read-write}</code>	Configure Policy Check permissions for this profile (default = none). This command corresponds to the Policy Check option in the GUI. It is a sub-setting of <code>policy-objects</code> . Controlled functions: Policy check Dependencies: <code>type</code> must be <code>system</code>
<code>datamask {enable disable}</code>	Enable/disable data masking (default = disable).
<code>datamask-custom-priority {enable disable}</code>	Enable/disable custom field search priority.
<code>datamask-fields <fields></code>	Enter that data masking fields, separated by spaces: <ul style="list-style-type: none"> • <i>dstip</i>: Destination IP • <i>dstname</i>: Destination name • <i>email</i>: Email • <i>message</i>: Message • <i>srcip</i>: Source IP • <i>srcmac</i>: Source MAC

Variable	Description
	<ul style="list-style-type: none"> • <i>srcname</i>: Source name • <i>user</i>: User name
datamask-key <passwd>	Enter the data masking encryption key.
datamask-unmasked-time <integer>	Enter the time without data masking, in days (default = 0).
deploy-management {none read read-write}	<p>Enter the level of access to the deployment management configuration settings for this profile (default = none).</p> <p>This command corresponds to the Install to Devices option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Install to devices</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
description <string>	Enter a description for this access profile (character limit = 1023). Enclose the description in quotes if it contains spaces.
device-ap	<p>Enter the level of access to device AP settings for this profile (default = none).</p> <p>This command corresponds to the AP Manager option in the GUI.</p> <p>Controlled functions: AP Manager pane</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-config {none read read-write}	<p>Enter the level of access to device configuration settings for this profile (default = none).</p> <p>This command corresponds to the Manage Device Configuration option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Edit devices, All settings under Menu in Dashboard</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-forticlient {none read read-write}	<p>Enter the level of access to FortiClient settings for this profile (default = none).</p> <p>This command corresponds to the FortiClient Manager option in the GUI.</p> <p>Controlled functions: FortiClient Manager pane</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-fortiswitch {none read read-write}	<p>Enter the level of access to the FortiSwitch Manager module for this profile (default = none).</p> <p>This command corresponds to the FortiSwitch Manager option in the GUI.</p> <p>Controlled functions: FortiSwitch Manager pane</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-manager {none read read-write}	<p>Enter the level of access to Device Manager settings for this profile (default = none).</p> <p>This command corresponds to the Device Manager option in the GUI.</p> <p>Controlled functions: Device Manager pane</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>

Variable	Description
device-op {none read read-write}	<p>Add the capability to add, delete, and edit devices to this profile (default = none). This command corresponds to the Add/Delete Devices/Groups option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Add or delete devices or groups</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-policy-package-lock {none read read-write}	<p>Configure device policy package locking permissions for this profile (default = none).</p> <p>Controlled functions: Policy package locking.</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-profile {none read read-write}	<p>Configure device profile permissions for this profile (default = none). This command corresponds to the Provisioning Templates option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Provisioning Templates</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-revision-deletion {none read read-write}	<p>Configure device revision deletion permissions for this profile (default = none). This command corresponds to the Delete Device Revision option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Deleting device revisions</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
device-wan-link-load-balance	<p>Enter the level of access to <code>wan-link-load-balance</code> settings for this profile (default = none).</p> <p>This command corresponds to SD-WAN option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: SD-WAN</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
event-management {none read read-write}	<p>Set the Event Management permissions (default = none). This command corresponds to the Event Management option in the GUI.</p> <p>Controlled functions: Event Management pane and all its operations</p> <p>Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code>, <code>type</code> must be <code>system</code></p>
extension-access {none read read-write}	<p>Configure Extension Access permissions (default = none):</p> <ul style="list-style-type: none"> • <code>none</code>: No permission. • <code>read</code>: Read permission. • <code>read-write</code>: Read-write permission.
fabric-viewer {none read read-write}	<p>Configure Fabric Viewer permissions (default = none):</p> <ul style="list-style-type: none"> • <code>none</code>: No permission. • <code>read</code>: Read permission. • <code>read-write</code>: Read-write permission.

Variable	Description
<code>fgd_center {none read read-write}</code>	<p>Set the FortiGuard Center permissions (default = none).</p> <p>This command corresponds to the FortiGuard Center option in the GUI.</p> <p>Controlled functions: FortiGuard pane, All the settings under FortiGuard</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>fgd-center-advanced {none read read-write}</code>	<p>Set the FortiGuard Center permissions (default = none).</p> <p>This command corresponds to the Advanced option in the GUI. It is a sub-setting of <code>fgd-center</code>.</p> <p>Controlled functions: FortiGuard pane Advanced Settings options</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>fgd-center-fmw-mgmt {none read read-write}</code>	<p>Set the FortiGuard Center permissions (default = none).</p> <p>This command corresponds to the Firmware Management option in the GUI. It is a sub-setting of <code>fgd-center</code>.</p> <p>Controlled functions: FortiGuard pane Firmware Images options</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>fgd-center-licensing {none read read-write}</code>	<p>Set the FortiGuard Center permissions (default = none).</p> <p>This command corresponds to the License Management option in the GUI. It is a sub-setting of <code>fgd-center</code>.</p> <p>Controlled functions: FortiGuard pane Licensing Status options</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>global-policy-packages {none read read-write}</code>	<p>Configure global policy package permissions for this profile (default = none).</p> <p>This command corresponds to the Global Policy Packages & Objects option in the GUI. It is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: All operations in Global ADOM</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>import-policy-packages {none read read-write}</code>	<p>Configure importing policy package permissions for this profile (default = none).</p> <p>This command corresponds to the Import Policy Package option in the GUI.</p> <p>Controlled functions: Importing policy packages</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>intf-mapping {none read read-write}</code>	<p>Configure interface mapping permissions for this profile (default = none).</p> <p>This command corresponds to the Interface Mapping option in the GUI.</p> <p>Controlled functions: Mapping interfaces</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>ips-baseline-cfg {none read read-write}</code>	<p>Configure IPS baseline sensor (default = none).</p>
<code>ips-baseline-ovrd {enable disable}</code>	<p>Enable/disable overriding baseline IPS sensor (default = disable).</p>
<code>ips-filter {enable disable}</code>	<p>Enable/disable Application Sensor permission for the restricted admin profile (default = disable).</p>

Variable	Description
	Dependencies: <code>type</code> must be <code>restricted</code>
<code>log-viewer {none read read-write}</code>	<p>Set the Log View permissions (default = none).</p> <p>This command corresponds to the Log View option in the GUI.</p> <p>Controlled functions: Log View and all its operations</p> <p>Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code>, <code>type</code> must be <code>system</code></p>
<code>policy-objects {none read read-write}</code>	<p>Set the Policy & Objects permissions (default = none).</p> <p>Controlled functions: Policy & Objects pane</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>read-passwd {none read read-write}</code>	<p>Add the capability to view the authentication password in clear text to this profile (default = none).</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>realtime-monitor {none read read-write}</code>	<p>Enter the level of access to the Drill Down configuration settings for this profile (default = none).</p> <p>Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code>, <code>type</code> must be <code>system</code></p>
<code>report-viewer {none read read-write}</code>	<p>Set the Reports permissions (default = none).</p> <p>This command corresponds to the Reports option in the GUI.</p> <p>Controlled functions: Reports pane and all its operations</p> <p>Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code>, <code>type</code> must be <code>system</code></p>
<code>run-report {none read read-write}</code>	<p>Configure run reports permission for this profile (default = none):</p> <ul style="list-style-type: none"> <code>none</code>: No permission. <code>read</code>: Read permission. <code>read-write</code>: Read-write permission.
<code>scope (Not Applicable)</code>	CLI command is not in use.
<code>script-access {none read read-write}</code>	Configure script access (default = none).
<code>set-install-targets {none read read-write}</code>	<p>Configure installation targets permissions (default = none).</p> <p>This command corresponds to the Installation Targets option in policy packages in the GUI. It is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: Installation targets</p> <p>Dependencies: <code>type</code> must be <code>system</code></p>
<code>super-user-profile {enable disable}</code>	Enable/disable the super user profile (default = disable).
<code>system-setting {none read read-write}</code>	<p>Configure System Settings permissions for this profile (default = none).</p> <p>This command corresponds to the System Settings option in the GUI.</p> <p>Controlled functions: System Settings pane, all the settings under system setting</p>

Variable	Description
	Dependencies: type must be system
term-access {none read read-write}	<p>Set the terminal access permissions for this profile (default = none).</p> <p>This command corresponds to the Terminal Access option in the GUI. It is a sub-setting of device-manager.</p> <p>Controlled functions: Connect to the CLI via Telnet or SSH</p> <p>Dependencies: Depends on device-config option, type must be System Admin</p>
triage-events {none read read-write}	Set the triage events permissions for this profile (default = none).
type {restricted system}	<p>Enter the admin profile type:</p> <ul style="list-style-type: none"> restricted: Restricted admin profile system: System admin profile (default)
update-incidents {none read read-write}	Create/update incidents (default = none).
vpn-manager {none read read-write}	<p>Enter the level of access to VPN console configuration settings for this profile (default = none).</p> <p>This command corresponds to the VPN Manager option in the GUI. It is a sub-setting of policy-objects.</p> <p>Controlled functions: VPN Console</p> <p>Dependencies: type must be System Admin</p>
web-filter {enable disable}	<p>Enable/disable Web Filter Profile permission for the restricted admin profile (default = disable).</p> <p>Dependencies: type must be Restricted Admin</p>
Variables for config datamask-custom-fields subcommand:	
<field>	Enter the custom field name.
field-category {alert all fortiview log euba}	Enter the field category (default = all).
field-status {enable disable}	Enable/disable the field (default = enable).
field-type {email ip mac string}	Enter the field type (default = string).

admin radius

Use this command to add, edit, and delete administration RADIUS servers.

Syntax

```
config system admin radius
edit <server>
set auth-type {any | chap | mschap2 | pap}
set nas-ip <ipv4_address>
```

```

    set port <integer>
    set secondary-secret <passwd>
    set secondary-server <string>
    set secret <passwd>
    set server <string>
end

```

Variable	Description
<server>	Enter the name of the RADIUS server or enter a new name to create an entry (character limit = 63).
auth-type {any chap mschap2 pap}	The authentication protocol the RADIUS server will use. <ul style="list-style-type: none"> any: Use any supported authentication protocol (default). mschap2: Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). chap: Challenge Handshake Authentication Protocol (CHAP) pap: Password Authentication Protocol (PAP).
nas-ip <ipv4_address>	The network access server (NAS) IPv4 address and called station ID.
port <integer>	The RADIUS server port number (1 - 65535, default = 1812).
secondary-secret <passwd>	The password to access the RADIUS secondary-server (character limit = 64).
secondary-server <string>	The RADIUS secondary-server DNS resolvable domain name or IPv4 address.
secret <passwd>	The password to access the RADIUS server (character limit = 64).
server <string>	The RADIUS server DNS resolvable domain name or IPv4 address.

Example

This example shows how to add the RADIUS server `RAID1` at the IPv4 address `206.205.204.203` and set the shared secret as `R1a2D3i4U5s`.

```

config system admin radius
edit RAID1
    set server 206.205.204.203
    set secret R1a2D3i4U5s
end

```

admin setting

Use this command to configure system administration settings, including web administration ports, timeout, and language.

Syntax

```

config system admin setting
    set access-banner {enable | disable}
    set admin-https-redirect {enable | disable}
    set admin-login-max <integer>
    set admin_server_cert <admin_server_cert>

```


```

set allow_register {enable | disable}
set auth-addr <string>
set auth-port <integer>
set auto-update {enable | disable}
set banner-message <string>
set central-ftgd-local-cat-id {enable | disable}
set chassis-mgmt {enable | disable}
set chassis-update-interval <integer>
set device_sync_status {enable | disable}
set gui-theme <theme>
set http_port <integer>
set https_port <integer>
set idle_timeout <integer>
set idle_timeout_api <integer>
set idle_timeout_gui <integer>
set install-ifpolicy-only {enable | disable}
set mgmt-addr <string>
set mgmt-fqdn <string>
set objects-force-deletion {enable | disable}
set offline_mode {enable | disable}
set register_passwd <passwd>
set sdwan-monitor-history {enable | disable}
set sdwan-skip-unmapped-input-device {enable | disable}
set shell-access {enable | disable}
set shell-password <passwd>
set show-add-multiple {enable | disable}
set show-adom-devman {enable | disable}
set show-checkbox-in-table {enable | disable}
set show-device-import-export {enable | disable}
set show_automatic_script {enable | disable}
set show-fct-manager {enable | disable}
set show_grouping_script {enable | disable}
set show_hostname {enable | disable}
set show_schedule_script {enable | disable}
set show_tcl_script {enable | disable}
set unreg_dev_opt {add_allow_service | add_no_service}
set webadmin_language {auto_detect | english | japanese | korean | simplified_
    chinese | spanish | traditional_chinese}
end

```

Variable	Description
access-banner {enable disable}	Enable/disable the access banner (default= disable).
admin-https-redirect {enable disable}	Enable/disable redirection of HTTP admin traffic to HTTPS (default= enable).
admin-login-max <integer>	Set the maximum number of admin users that be logged in at one time (1 - 256, default = 256).
admin_server_cert <admin_server_cert>	Enter the name of an https server certificate to use for secure connections (default = server.crt).
allow_register {enable disable}	Enable/disable the ability for an unregistered device to be registered (default= disable).

Variable	Description
auth-addr <string>	Enter the IP which is used by FortiGate to authorize FortiManager.
auth-port <integer>	Set the port which is used by FortiGate to authorize FortiManager (default = 443).
auto-update {enable disable}	Enable/disable FortiGate automatic updates (default= enable).
banner-message <string>	Set the banner messages (character limit = 255).
central-ftgd-local-cat-id {enable disable}	Enable/disable central FortiGuard local category id management, and do not auto assign id during installation (default= disable).
chassis-mgmt {enable disable}	Enable/disable chassis management (default= disable).
chassis-update-interval <integer>	Set the chassis background update interval, in minutes (4 - 1440, default = 15).
device_sync_status {enable disable}	Enable/disable device synchronization status indication (default= enable).
gui-theme <theme>	Configure the GUI theme (default = blue).
http_port <integer>	Enter the HTTP port number for web administration (1 - 65535, default = 80).
https_port <integer>	Enter the HTTPS port number for web administration (1 - 65535, default = 443).
idle_timeout <integer>	Enter the idle timeout value, in seconds (60 - 28800, default = 900).
idle_timeout_api <integer>	Enter the idle timeout for the API sessions, in seconds (1 - 28800, default = 900).
idle_timeout_gui <integer>	Enter the idle timeout for the GUI sessions, in seconds (60 - 28800, default = 900).
install-ifpolicy-only {enable disable}	Enable/disable allowing only the interface policy to be installed (default = disable).
mgmt-addr <string>	FQDN/IPv4 of FortiManager used by FGFM. If the FortiManager is behind a NAT device, and a device is added in the FortiManager GUI, the FortiManager will not add its IP address to the FortiGate. Configure <code>mgmt-addr</code> with the fixed, public-facing IP address if you need FortiManager to configure the <code>set fmg <ip></code> command on managed FortiGates.
mgmt-fqdn <string>	FQDN of FortiManager used by FGFM.
objects-force-deletion {enable disable}	Enable/disable forced deletion of used objects (default = enable).
offline_mode {enable disable}	Enable/disable offline mode to shut down the protocol used to communicate with managed devices (default = disable).
register_passwd <passwd>	Enter the password to use when registering a device (character limit = 19).
sdwan-monitor-history {enable disable}	Enable/disable sdwan-monitor-history (default = disable).

Variable	Description
sdwan-skip-unmapped-input-device {enable disable}	Enable/disable skipping unmapped interface for SD-WAN/rule/input-device instead of report mapping error (default = disable).
shell-access {enable disable}	Enable/disable shell access (default = disable).
shell-password <passwd>	Enter the password to use for shell access.
show-add-multiple {enable disable}	Enable/disable show the add multiple button in the GUI (default = disable).
show-adom-devman {enable disable}	Enable/disable device manager tools on the GUI (default = enable).
show-checkbox-in-table {enable disable}	Show checkboxes in tables in the GUI (default = disable).
show-device-import-export {enable disable}	Enable/disable import/export of ADOM, device, and group lists (default = disable).
show_automatic_script {enable disable}	Enable/disable automatic script (default = disable).
show-fct-manager {enable disable}	<div> <div>  <p>Although still available in FortiManager 7.0, this command has no impact on the GUI.</p> <p>This is because the FortiClient module requires ADOM version 6.0 or earlier, whereas FortiManager 7.0 only supports ADOM versions 6.2, 6.4, and 7.0.</p> </div> </div>
show_grouping_script {enable disable}	Enable/disable grouping script (default = enable).
show_hostname {enable disable}	Enable/disable showing the hostname on the GUI login page (default = disable).
show_schedule_script {enable disable}	Enable/disable schedule script (default = disable).
show_tcl_script {enable disable}	Enable/disable TCL script (default = disable).
unreg_dev_opt {add_allow_service add_no_service}	Select action to take when an unregistered device connects to FortiManager: <ul style="list-style-type: none"> • <code>add_allow_service</code>: Add unregistered devices and allow service requests (default). • <code>add_no_service</code>: Add unregistered devices and deny service requests.
webadmin_language {auto_detect english japanese korean simplified_chinese spanish traditional_chinese}	Select the language to be used for web administration: <ul style="list-style-type: none"> • <code>auto_detect</code>: Automatically detect language (default) • <code>english</code>: English • <code>japanese</code>: Japanese • <code>korean</code>: Korean • <code>simplified_chinese</code>: Simplified Chinese

Variable	Description
	<ul style="list-style-type: none"> • <code>spanish</code>: Spanish • <code>traditional_chinese</code>: Traditional Chinese

admin tacacs

Use this command to add, edit, and delete administration TACACS+ servers.

Syntax

```
config system admin tacacs
edit <server>
    set authen-type {ascii | auto | chap | mschap | pap}
    set authorization {enable | disable}
    set key <passwd>
    set port <integer>
    set secondary-key <passwd>
    set secondary-server <string>
    set server <string>
    set tertiary-key <passwd>
    set tertiary-server <string>
end
```

Variable	Description
<server>	Enter the name of the TACACS+ server or enter a new name to create an entry (character limit = 63).
authen-type {ascii auto chap mschap pap}	Choose which authentication type to use: <ul style="list-style-type: none"> • <code>ascii</code>: ASCII • <code>auto</code>: Uses PAP, MSCHAP, and CHAP (in that order) (default). • <code>chap</code>: Challenge Handshake Authentication Protocol (CHAP) • <code>mschap</code>: Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) • <code>pap</code>: Password Authentication Protocol (PAP).
authorization {enable disable}	Enable/disable TACACS+ authorization (default = disable).
key <passwd>	Key to access the server (character limit = 128).
port <integer>	Port number of the TACACS+ server (1 - 65535, default = 49).
secondary-key <passwd>	Key to access the secondary server (character limit = 128).
secondary-server <string>	Secondary server domain name or IPv4 address.
server <string>	The server domain name or IPv4 address.
tertiary-key <passwd>	Key to access the tertiary server (character limit = 128).
tertiary-server <string>	Tertiary server domain name or IPv4 address.

Example

This example shows how to add the TACACS+ server TAC1 at the IPv4 address 206.205.204.203 and set the key as R1a2D3i4U5s.

```
config system admin tacacs
edit TAC1
set server 206.205.204.203
set key R1a2D3i4U5s
end
```

admin user

Use this command to add, edit, and delete administrator accounts.

Use the admin account or an account with System Settings read and write privileges to add new administrator accounts and control their permission levels. Each administrator account must include a minimum of an access profile. The access profile list is ordered alphabetically, capitals first. If custom profiles are defined, it may change the default profile from Restricted_User. You cannot delete the admin administrator account. You cannot delete an administrator account if that user is logged on.



You can create meta-data fields for administrator accounts. These objects must be created using the FortiManager GUI. The only information you can add to the object is the value of the field (pre-determined text/numbers). For more information, see *System Settings* in the [FortiManager Administration Guide](#).

Syntax

```
config system admin user
edit <name_str>
set login-max <integer>
set password <passwd>
set change-password {enable | disable}
set trusthost1 <ipv4_mask>
set trusthost2 <ipv4_mask>
set trusthost3 <ipv4_mask>
...
set trusthost10 <ipv4_mask>
set ipv6_trusthost1 <ipv6_mask>
set ipv6_trusthost2 <ipv6_mask>
set ipv6_trusthost3 <ipv6_mask>
...
set ipv6_trusthost10 <ipv6_mask>
set profileid <profile-name>
set adom <adom_name(s)>
set dev-group <group-name>
set adom-exclude <adom_name(s)>
set web-filter <Web Filter profile name>
set ips-filter <IPS Sensor name>
set app-filter <Application Sensor name>
set policy-package {<adom name>: <policy package id> <adom policy folder name>/
    <package name> | all_policy_packages}
```

```
set description <string>
set user_type {group | ldap | local | pki-auth | radius | tacacs-plus}
set group <string>
set ldap-server <string>
set radius_server <string>
set tacacs-plus-server <string>
set ssh-public-key1 <key-type> <key-value>
set ssh-public-key2 <key-type> <key-value>
set ssh-public-key3 <key-type> <key-value>
set avatar <string>
set wildcard {enable | disable}
set ext-auth-accprofile-override {enable | disable}
set ext-auth-adom-override {enable | disable}
set ext-auth-group-match <string>
set password-expire <yyyy-mm-dd>
set force-password-change {enable | disable}
set subject <string>
set ca <string>
set two-factor-auth {enable | disable}
set rpc-permit {none | read-only | read-write}
set use-global-theme {enable | disable}
set user-theme {astronomy | autumn | binary-tunnel | blue | calla-lily | canyon |
    cave | contrast-dark | diving | dreamy | fish | green | landscape | melongene
    | mountain | northern-light | parrot | penguin | polar-bear | red | space |
    spring | summer | technology | twilight | winter | zebra}
set last-name <string>
set first-name <string>
set email-address <string>
set phone-number <string>
set mobile-number <string>
set pager-number <string>
config meta-data
    edit <fieldname>
        set fieldlength
        set fieldvalue <string>
        set importance
        set status
    end
config dashboard-tabs
    edit tabid <integer>
        set name <string>
    end
config dashboard
    edit moduleid
        set name <string>
        set column <column_pos>
        set diskio-content-type
        set diskio-period {1hour | 24hour | 8hour}
        set refresh-inverval <integer>
        set status {close | open}
        set tabid <integer>
        set widget-type <string>
        set log-rate-type {device | log}
        set log-rate-topn {1 | 2 | 3 | 4 | 5}
        set log-rate-period {1hour | 2min | 6hours}
        set res-view-type {history | real-time}
        set res-period {10min | day | hour}
```

```

        set res-cpu-display {average | each}
        set num-entries <integer>
        set time-period {1hour | 24hour | 8hour}
    end
end

```

Variable	Description
<name_string>	Enter the name of the admin user or enter a new name to create a new user (character limit = 35).
login-max <integer>	Set the maximum number of login sessions for this user (default = 32).
password <passwd>	Enter a password for the administrator account (character limit = 128). For improved security, the password should be at least 6 characters long. This variable is available only if <code>user_type</code> is <code>local</code> .
change-password {enable disable}	Enable/disable allowing restricted users to change their password (default = disable).
trusthost1 <ipv4_mask> trusthost2 <ipv4_mask> trusthost3 <ipv4_mask> ... trusthost10 <ipv4_mask>	Optionally, type the trusted host IPv4 address and network mask from which the administrator can log in to the FortiManager system. You can specify up to ten trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. Defaults: <code>trusthost1: 0.0.0.0 0.0.0.0</code> for all <code>others: 255.255.255.255 255.255.255.255</code> for none
ipv6_trusthost1 <ipv6_mask> ipv6_trusthost2 <ipv6_mask> ipv6_trusthost3 <ipv6_mask> ... ipv6_trusthost10 <ipv6_mask>	Optionally, type the trusted host IPv6 address from which the administrator can log in to the FortiManager system. You can specify up to ten trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. Defaults: <code>ipv6_trusthost1: ::/0</code> for all <code>others: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128</code> for none
profileid <profile-name>	Enter the name of the access profile to assign to this administrator account (character limit = 35, default = <code>Restricted_User</code>). Access profiles control administrator access to FortiManager features.
adom <adom_name(s)>	Enter the name(s) of the ADOM(s) the administrator belongs to. Any configuration of ADOMs takes place via the FortiManager GUI.
dev-group <group-name>	Enter the device group that the admin use can access. This option can only be used for administrators with access to only one ADOM.
adom-exclude <adom_name(s)>	Enter the name(s) of the excluding ADOM(s).
web-filter <Web Filter profile name>	Enter the Web Filter profile to associate with the restricted admin profile. Dependencies: admin user must be associated with a restricted admin profile.
ips-filter <IPS Sensor name>	Enter the IPS Sensor to associate with the restricted admin profile. Dependencies: The admin user must be associated with a restricted admin profile.

Variable	Description
app-filter <Application Sensor name>	Enter the Application Sensor to associate with the restricted admin profile. Dependencies: The admin user must be associated with a restricted admin profile.
policy-package {<adom name>: <policy package id> <adom policy folder name>/ <package name> all_policy_packages}	Policy package access.
description <string>	Enter a description for this administrator account (character limit = 127). Enclose the description in quotes if it contains spaces.
user_type {group ldap local pki-auth radius tacacs-plus}	Select the administrator type: <ul style="list-style-type: none"> group: The administrator is a member of a administrator group. ldap: An LDAP server verifies the administrator's password. local: The FortiManager system verifies the administrator's password (default). pki-auth: The administrator uses PKI. radius: A RADIUS server verifies the administrator's password. tacacs-plus: A TACACS+ server verifies the administrator's password.
group <string>	Enter the group name. This option is only available when <code>user_type</code> is <code>group</code> .
ldap-server <string>	Enter the LDAP server name if the user type is set to LDAP. This option is only available when <code>user_type</code> is <code>ldap</code> .
radius_server <string>	Enter the RADIUS server name if the user type is set to RADIUS. This option is only available when <code>user_type</code> is <code>radius</code> .
tacacs-plus-server <string>	Enter the TACACS+ server name if the user type is set to TACACS+. This option is only available when <code>user_type</code> is <code>tacacs-plus</code> .
ssh-public-key1 <key-type> <key-value> ssh-public-key2 <key-type> <key-value> ssh-public-key3 <key-type> <key-value>	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. <key type> is <code>ssh-dss</code> for a DSA key, <code>ssh-rsa</code> for an RSA key. <key-value> is the public key string of the SSH client.
avatar <string>	Image file for the administrator's avatar (maximum 4K base64 encode).
wildcard {enable disable}	Enable/disable wildcard remote authentication (default = disable).
ext-auth-accprofile-override {enable disable}	Enable/disable allowing the use of the access profile provided by the remote authentication server (default = disable).
ext-auth-adom-override {enable disable}	Enable/disable allowing the use of the ADOM provided by the remote authentication server (default = disable).

Variable	Description
	In order to support vendor specific attributes (VSA), the authentication server requires a dictionary to define which VSAs to support. The Fortinet RADIUS vendor ID is 12365. The <code>Fortinet-Vdom-Name</code> attribute is used by this command.
<code>ext-auth-group-match <string></code>	Only admin users that belong to this group are allowed to log in.
<code>password-expire <yyyy-mm-dd></code>	When enforcing the password policy, enter the date that the current password will expire.
<code>force-password-change {enable disable}</code>	Enable/disable force password change on next log in.
<code>subject <string></code>	PKI user certificate name constraints. This command is available when a PKI administrator account is configured.
<code>ca <string></code>	PKI user certificate CA (CA name in local). This command is available when a PKI administrator account is configured.
<code>two-factor-auth {enable disable}</code>	Enable/disable two-factor authentication (certificate + password) (default = disable). This command is available when a PKI administrator account is configured.
<code>rpc-permit {none read-only read-write}</code>	Set the permission level for log in via Remote Procedure Call (RPC) (default = none).
<code>use-global-theme {enable disable}</code>	Enable/disable global theme for administration GUI (default = enable).
<code>user-theme {astronomy autumn binary-tunnel blue calla-lily canyon cave contrast-dark diving dreamy fish green landscape melongene mountain northern-light parrot penguin polar-bear red space spring summer technology twilight winter zebra}</code>	Set the color scheme to use for the admin user GUI (default = blue): <ul style="list-style-type: none"> <code>astronomy</code>: Astronomy <code>autumn</code>: Autumn <code>binary-tunnel</code>: Binary Tunnel <code>blue</code>: Blueberry <code>calla-lily</code>: Calla Lily <code>canyon</code>: Canyon <code>cave</code>: Cave <code>contrast-dark</code>: High Contrast Dark <code>diving</code>: Diving <code>dreamy</code>: Dreamy <code>fish</code>: Fish <code>green</code>: Kiwi <code>landscape</code>: Landscape <code>melongene</code>: Plum <code>mountain</code>: Mountain <code>northern-light</code>: Northern Light <code>parrot</code>: Parrot

Variable	Description
	<ul style="list-style-type: none"> penguin: Penguin polar-bear: Polar Bear red: Cherry space: Space spring: Spring summer: Summer technology: Technology twilight: Twilight winter: Winter zebra: Zebra <p>This command is available when <code>use-global-theme</code> is disabled.</p>
last-name <string>	Administrator's last name (character limit = 63).
first-name <string>	Administrator's first name (character limit = 63).
email-address <string>	Administrator's email address.
phone-number <string>	Administrator's phone number.
mobile-number <string>	Administrator's mobile phone number.
pager-number <string>	Administrator's pager number.
Variables for <code>config meta-data</code> subcommand:	
This subcommand can only change the value of an existing field. To create a new metadata field, use the <code>config system metadata</code> command.	
fieldname	The label/name of the field (read-only, default = 50). Enclose the name in quotes if it contains spaces.
fieldlength	The maximum number of characters allowed for this field (read-only, default = 50).
fieldvalue <string>	Enter a pre-determined value for the field. This is the only value that can be changed with the <code>config meta-data</code> subcommand (character limit = 255).
importance	Indicates whether the field is compulsory (<code>required</code>) or optional (<code>optional</code>) (read-only, default = <code>optional</code>).
status	The status of the field (read-only, default = <code>enable</code>).
Variables for <code>config dashboard-tabs</code> subcommand:	
tabid <integer>	Tab ID.
name <string>	Tab name.
Variables for <code>config dashboard</code> subcommand:	
moduleid	Widget ID.
name <string>	Widget name (character limit = 63).

Variable	Description
column <column_pos>	Widget column ID (default = 0).
diskio-content-type {blks iops util}	Set the Disk I/O Monitor widget's chart type. <ul style="list-style-type: none"> blks: the amount of data of I/O requests. iops: the number of I/O requests. util: bandwidth utilization (default).
diskio-period {1hour 24hour 8hour}	Set the Disk I/O Monitor widget's data period (default = 1hour).
refresh-interval <integer>	Widget refresh interval (default = 300).
status {close open}	Widget opened/closed status (default = open).
tabid <integer>	ID of the tab where the widget is displayed (default = 0).
widget-type <string>	Widget type: <ul style="list-style-type: none"> alert: Alert Message Console devsummary: Device Summary disk-io: Disk I/O jsconsole: CLI Console licinfo: License Information log-rcvd-fwd: Receive Rate v. Forwarding Rate logdb-lag: Log Insert Lag Time logdb-perf: Insert Rate vs Receive Rate logrecv: Logs/Data Received (this widget has been deprecated) raid: Disk Monitor rpteng: Report Engine (this widget has been deprecated) statistics: Statistics (this widget has been deprecated) sysinfo: System Information sysop: Unit Operation sysres: System Resources top-lograte: Log Receive Monitor
log-rate-type {device log}	Log receive monitor widget's statistics breakdown options (default = device).
log-rate-topn {1 2 3 4 5}	Log receive monitor widgets's number of top items to display (default = 5).
log-rate-period {1hour 2min 6hours}	Log receive monitor widget's data period (default = 2min).
res-view-type {history real-time}	Widget's data view type (default = history).
res-period {10min day hour}	Widget data period: <ul style="list-style-type: none"> 10min: Last 10 minutes (default). day: Last day. hour: Last hour.
res-cpu-display {average each}	Widget CPU display type: <ul style="list-style-type: none"> average: Average usage of CPU (default). each: Each usage of CPU.

Variable	Description
num-entries <integer>	Number of entries (default = 10).
time-period {1hour 24hour 8hour}	Set the Log Database Monitor widget's data period (default = 1 hour).

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IPv4 address if you define only one trusted host IPv4 address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiManager system does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

Example

Use the following commands to add a new administrator account named `admin_2` with the password set to `p8ssw0rd` and the `Super_User` access profile. Administrators that log in to this account will have administrator access to the FortiManager system from any IPv4 address.

```
config system admin user
  edit admin_2
    set description "Backup administrator"
    set password p8ssw0rd
    set profileid Super_User
  end
```

alert-console

Use this command to configure the alert console options. The alert console appears on the dashboard in the GUI.

Syntax

```
config system alert-console
  set period {1 | 2 | 3 | 4 | 5 | 6 | 7}
  set severity-level {information | notify | warning | error | critical | alert |
    emergency}
end
```

Variable	Description
period {1 2 3 4 5 6 7}	Enter the number of days to keep the alert console alerts (default = 7).
severity-level {information notify warning error critical alert emergency}	Enter the minimum severity level to display on the alert console on the dashboard: <ul style="list-style-type: none"> emergency: The unit is unusable (default). alert: Immediate action is required. critical: Functionality is affected. error: Functionality is probably affected. warning: Functionality might be affected. notification: Information about normal events. information: General information about unit operations.

Example

This example sets the alert console message display to warning for a duration of three days.

```
config system alert-console
    set period 3
    set severity-level warning
end
```

alertemail

Use this command to configure alert email settings for your FortiManager unit.

All variables are required when authentication is enabled.

Syntax

```
config system alertemail
    set authentication {enable | disable}
    set fromaddress <email-address_string>
    set fromname <string>
    set smtppassword <passwd>
    set smtpport <integer>
    set smtpserver {<ipv4_address>|<fqdn_string>}
    set smtpuser <username>
end
```

Variable	Description
authentication {enable disable}	Enable/disable alert email authentication (default = enable).
fromaddress <email-address_string>	The email address the alert message is from. This is a required variable.
fromname <string>	The SMTP name associated with the email address. Enclose the name in quotes if it contains spaces.

Variable	Description
smtppassword <passwd>	Set the SMTP server password (character limit = 39).
smtpport <integer>	The SMTP server port (1 - 65535, default = 25).
smtpserver {<ipv4_address> <fqdn_string>}	The SMTP server address, either a DNS resolvable host name or an IPv4 address.
smtpuser <username>	Set the SMTP server username (character limit= 63).

Example

Here is an example of configuring `alertemail`. Enable authentication, the alert is set in Mr. Customer's name and from his email address, the SMTP server port is the default port(25), and the SMTP server is at IPv4 address of 192.168.10.10.

```
config system alertemail
  set authentication enable
  set fromaddress customer@example.com
  set fromname "Mr. Customer"
  set smtpport 25
  set smtpserver 192.168.10.10
end
```

auto-delete

Use this command to automatically delete policies for logs, reports, and archived and quarantined files.

Syntax

```
config system auto-delete
  config dlp-files-auto-deletion
    set retention {days | weeks | months}
    set runat <integer>
    set status {enable | disable}
    set value <integer>
  end
  config quarantine-files-auto-deletion
    set retention {days | weeks | months}
    set runat <integer>
    set status {enable | disable}
    set value <integer>
  end
  config log-auto-deletion
    set retention {days | weeks | months}
    set runat <integer>
    set status {enable | disable}
    set value <integer>
  end
  config report-auto-deletion
    set retention {days | weeks | months}
```

```

        set runat <integer>
        set status {enable | disable}
        set value <integer>
    end
end

```

Variable	Description
dlp-files-auto-deletion	Automatic deletion policy for DLP archives.
quarantine-files-auto-deletion	Automatic deletion policy for quarantined files.
log-auto-deletion	Automatic deletion policy for device logs.
report-auto-deletion	Automatic deletion policy for reports.
retention {days weeks months}	Automatic deletion in days, weeks, or months (default = days).
runat <integer>	Automatic deletion run at (0 - 23) o'clock (default = 0).
status {enable disable}	Enable/disable automatic deletion (default = disable).
value <integer>	Automatic deletion in x days, weeks, or months (default = 0).

backup all-settings

Use this command to set or check the settings for scheduled backups.

Syntax

```

config system backup all-settings
    set status {enable | disable}
    set server {<ipv4_address>|<fqdn_str>}
    set user <username>
    set directory <string>
    set week_days {monday tuesday wednesday thursday friday saturday sunday}
    set time <hh:mm:ss>
    set protocol {ftp | scp | sftp}
    set passwd <passwd>
    set cert <certificate_name>
    set crtpasswd <passwd>
end

```

Variable	Description
status {enable disable}	Enable/disable scheduled backups (default = disable).
server {<ipv4_address> <fqdn_str>}	Enter the IPv4 address or DNS resolvable host name of the backup server.
user <username>	Enter the user account name for the backup server (character limit = 63).
directory <string>	Enter the name of the directory on the backup server in which to save the backup file.

Variable	Description
week_days {monday tuesday wednesday thursday friday saturday sunday}	Enter the days of the week on which to perform backups. You may enter multiple days.
time <hh:mm:ss>	Enter the time of day to perform the backup. Time is required in the form <hh:mm:ss>.
protocol {ftp scp sftp}	Enter the transfer protocol (default = sftp).
passwd <passwd>	Enter the password for the backup server (character limit = 63).
cert <certificate_name>	SSH certificate for authentication. Only available if the protocol is set to scp. The SSH certificate object must already be configured. See certificate ssh on page 67 .
crptpasswd <passwd>	Optional password to protect backup content (character limit = 63).

Example

This example shows a whack where backup server is 172.20.120.11 using the admin account with no password, saving to the /usr/local/backup directory. Backups are done on Mondays at 1:00pm using ftp.

```
config system backup all-settings
    set status enable
    set server 172.20.120.11
    set user admin
    set directory /usr/local/backup
    set week_days monday
    set time 13:00:00
    set protocol ftp
end
```

certificate

Use the following commands to configure certificate related settings.

certificate ca

Use this command to install Certificate Authority (CA) root certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.

4. Use the `system certificate ca` command to install the CA certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ca
  edit <ca_name>
    set ca <certificate>
    set comment <string>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get system certificate ca <ca_name>
```

Variable	Description
<ca_name>	Enter a name for the CA certificate (character limit = 35).
ca <certificate>	Enter or retrieve the CA certificate in PEM format.
comment <string>	Optionally, enter a descriptive comment (character limit = 127).

certificate crl

Use this command to configure CRLs.

Syntax

```
config system certificate crl
  edit <name>
    set crl <crl>
    set comment <string>
  end
```

Variable	Description
<name>	Enter a name for the CRL (character limit = 35).
crl <crl>	Enter or retrieve the CRL in PEM format.
comment <string>	Optionally, enter a descriptive comment for this CRL (character limit = 127).

certificate local

Use this command to install local certificates. When a CA processes your CSR, it sends you the CA certificate, the signed local certificate and the CRL.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate local
  edit <cert_name>
    set password <passwd>
    set comment <string>
    set certificate <certificate_PEM>
    set private-key <prkey>
    set csr <csr_PEM>
  end
```

Variable	Description
<cert_name>	Enter the local certificate name (character limit = 35).
password <passwd>	Enter the local certificate password (character limit = 67).
comment <string>	Enter any relevant information about the certificate (character limit = 127).
certificate <certificate_PEM>	Enter the signed local certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit:	
private-key <prkey>	The private key in PEM format.
csr <csr_PEM>	The CSR in PEM format.

certificate oftp

Use this command to install OFTP certificates and keys.

Syntax

```
config system certificate oftp
  set certificate <certificate>
  set comment <string>
  set local {Fortinet_Local | Fortinet_Local2}
  set mode {custom | default | local}
  set password <string>
  set private-key <key>
end
```

Variable	Description
certificate <certificate>	PEM format certificate.
comment <string>	OFTP certificate comment (character limit = 127).
local {Fortinet_Local Fortinet_Local2}	Choose from the two available local certificates.
mode {custom default local}	Mode of certificates used by OFTPD (default = default): <ul style="list-style-type: none"> custom: Use a custom certificate. default: Default mode. local: Use a local certificate.
password <string>	Password for encrypted 'private-key', unset for non-encrypted.
private-key <key>	PEM format private key.

certificate remote

Use this command to install remote certificates

Syntax

```
config system certificate remote
edit <cert_name>
set cert <certificate>
set comment <string>
next
end
```

Variable	Description
<cert_name>	Enter the remote certificate name (character limit = 35).
cert <certificate>	The remote certificate.
comment <string>	Optionally, enter a descriptive comment (character limit = 127).

certificate ssh

Use this command to install SSH certificates and keys.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.
5. Use the `system certificate ssh` command to install the SSH certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ssh
  edit <name>
    set comment <comment_text>
    set certificate <certificate>
    set private-key <key>
  end
```

Variable	Description
<name>	Enter the SSH certificate name (character limit = 63).
comment <comment_text>	Enter any relevant information about the certificate (character limit = 127).
certificate <certificate>	Enter the signed SSH certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
private-key <key>	The private key in PEM format.

connector

Use this command to configure connector related settings.

Syntax

```
config system connector
  set fssso-refresh-interval <integer>
  set fssso-sess-timeout <integer>
  set px-refresh-interval <integer>
  set px-svr-timeout <integer>
end
```

Variable	Description
fssso-refresh-interval <integer>	Set the FSSO refresh interval, in seconds (60 - 1800, default = 180).
fssso-sess-timeout <integer>	Set the FSSO session timeout, in seconds (30 - 600, default = 300).
px-refresh-interval <integer>	Set the pxGrid refresh interval, in seconds (60 - 1800, default = 300).
px-svr-timeout <integer>	Set the pxGrid session timeout, in seconds (30 - 600, default = 900).

dm

Use this command to configure Deployment Manager (DM) settings.

Syntax

```

config system dm
    set concurrent-install-image-limit <integer>
    set concurrent-install-limit <integer>
    set concurrent-install-script-limit <integer>
    set conf-merge-after-script {enable | disable}
    set discover-timeout <integer>
    set dpm-logsize <integer>
    set fgfm-install-refresh-count <integer>
    set fgfm-sock-timeout <integer>
    set fgfm_heartbeat_itvl <integer>
    set force-remote-diff {enable | disable}
    set fortiap-refresh-cnt <integer>
    set fortiap-refresh-itvl <integer>
    set fortiaext-refresh-cnt <integer>
    set install-image-timeout <integer>
    set install-tunnel-retry-itvl <integer>
    set max-revs <integer>
    set nr-retry <integer>
    set retry {enable | disable}
    set retry-intvl <integer>
    set rollback-allow-reboot {enable | disable}
    set script-logsize <integer>
    set skip-scep-check {enable | disable}
    set skip-tunnel-fcp-req {enable | disable}
    set verify-install {enable | disable | optimal}
end

```

Variable	Description
concurrent-install-image-limit <integer>	The maximum number of concurrent installs (1 - 1000, default = 500).
concurrent-install-limit <integer>	The maximum number of concurrent installs (5 - 2000, default = 480).
concurrent-install-script-limit <integer>	The maximum number of concurrent install scripts (5 - 2000, default = 480).
conf-merge-after-script {enable disable}	Merge config after running the script on the remote device, instead of a full retrieve (default = disable).
discover-timeout <integer>	Check connection timeout when discovering a device (3 - 15, default = 6).
dpm-logsize <integer>	The maximum DPM log size per device, in kilobytes (1 - 10000, default = 10000).
fgfm-install-refresh-count <integer>	The maximum FGFM install refresh attempts (default = 10).
fgfm-sock-timeout <integer>	The maximum FGFM communication socket idle time, in seconds (90 - 1800, default = 360).
fgfm_heartbeat_itvl <integer>	The FortiManager/FortiGate communication protocol keep alive interval, in seconds (30 - 600, default = 120).
force-remote-diff {enable disable}	Enable/disable always using remote diff when installing (default = disable).

Variable	Description
fortiap-refresh-cnt <integer>	Maximum auto refresh FortiAP number each time (1 - 10000, default = 500).
fortiap-refresh-itvl <integer>	Auto refresh FortiAP status interval, in minutes (1 - 1440, 0 to disable, default = 10).
fortiext-refresh-cnt <integer>	Maximum device number for FortiExtender auto refresh (1 - 10000, default = 50).
install-image-timeout <integer>	Maximum waiting time for image transfer and device upgrade, in seconds (600 - 7200, default = 3600).
install-tunnel-retry-itvl <integer>	Time to re-establish tunnel during install, in seconds (10 - 60, default = 60).
max-revs <integer>	The maximum number of revisions saved (1 - 250, default = 100).
nr-retry <integer>	The number of times the FortiManager unit will retry (default = 1).
retry {enable disable}	Enable/disable configuration installation retries (default = enable).
retry-intvl <integer>	The interval between attempting another configuration installation following a failed attempt (default = 15).
rollback-allow-reboot {enable disable}	Enable/disable allowing a FortiGate unit to reboot when installing a script or configuration (default = disable).
script-logsize <integer>	Enter the maximum script log size per device, in kilobytes (1 - 10000, default = 100).
skip-scep-check {enable disable}	Enable/disable installing scep related objects even if the scep URL is configured (default = disable).
skip-tunnel-fcp-req {enable disable}	Enable/disable skipping the FCP request sent from an FGFM tunnel (default = enable).
verify-install {enable disable optimal}	Enable/disable verify install against remote configuration: <ul style="list-style-type: none"> • disable: Disable. • enable: Always verify installation (default). • optimal: Verify installation for command errors.

Example

This example shows how to set up configuration installations. It shows how to set 5 attempts to install a configuration on a FortiGate device, waiting 30 seconds between attempts.

```
config system dm
    set retry enable
    set nr-retry 5
    set retry-intvl 30
end
```

dns

Use these commands to set the DNS server addresses. Several FortiManager functions, including sending alert email, use DNS. You can configure both IPv4 and IPv6 DNS server addresses.

Syntax

```
config system dns
  set primary <ipv4_address>
  set secondary <ipv4_address>
  set ip6-primary <ipv6_address>
  set ip6-secondary <ipv6_address>
end
```

Variable	Description
primary <ipv4_address>	Enter the primary DNS server IPv4 address.
secondary <ipv4_address>	Enter the secondary DNS IPv4 server address.
ip6-primary <ipv6_address>	Enter the primary DNS server IPv6 address.
ip6-secondary <ipv6_address>	Enter the secondary DNS IPv6 server address.

Example

This example shows how to set the primary FortiManager DNS server IPv4 address to 172.20.120.99 and the secondary FortiManager DNS server IPv4 address to 192.168.1.199.

```
config system dns
  set primary 172.20.120.99
  set secondary 192.168.1.199
end
```

docker

Use the following command to enable Docker and management extensions.

Syntax

```
config system docker
  set cpu <integer>
  set default-address-pool_base <ip&netmask>
  set default-address-pool_size <integer>
  set docker-user-login-max <integer>
  set fortiaaiops {enable | disable}
  set fortiaauthenticator {enable | disable}
  set fortiportal {enable | disable}
  set fortisigconverter {enable | disable}
  set fortisoar {enable | disable}
  set fortiwlm {enable | disable}
  set fsmcollector {enable | disable}
  set mem <integer>
  set sdwancontroller {enable | disable}
  set status {enable | disable | qa | dev}
  set universalconnector {enable | disable}
end
```

Variable	Description
cpu <integer>	Set the maximum % of CPU usage (10 - 50, default = 50).
default-address-pool_base <ip&netmask>	Set the default-address-pool CIDR. Enter the IP address and the netmask (default = 172.17.0.0 255.255.0.0).
default-address-pool_size <integer>	Set the default-address-pool size (default = 24).
docker-user-login-max <integer>	Set the maximum login sessions for the docker users (default = 32).
fortiaioops {enable disable}	Enable/disable FortiAI Ops (default = disable).
fortiauthenticator {enable disable}	Enable/disable FortiAuthenticator (default = disable).
fortiportal {enable disable}	Enable/disable FortiPortal (default = disable).
fortisigconverter {enable disable}	Enable/disable FortiSigConverter (default = disable).
fortisoar {enable disable}	Enable/disable FortiSOAR (default = disable).
fortiwlmm {enable disable}	Enable/disable Wireless Manager (default = disable).
fsmcollector {enable disable}	Enable/disable FSMCollector (default = disable).
mem <integer>	Set the maximum % of RAM usage (10 - 50, default = 50).
sdwancontroller {enable disable}	Enable/disable SD-WAN orchestration (default = disable).
status {enable disable qa dev}	Enable/disable Docker and set registry (default = disable): <ul style="list-style-type: none"> • enable: Enable production registry. • disable: Disable the docker host service. • qa: Enable QA test registry. • dev: Enable QA test registry without the signature.
universalconnector {enable disable}	Enable/disable universal connector (default = disable).

fips

Use this command to set the Federal Information Processing Standards (FIPS) status. FIPS mode is an enhanced security option for some FortiManager models. Installation of FIPS firmware is required only if the unit was not ordered with this firmware pre-installed.

Syntax

```
config system fips
  set status enable
  set entropy-token {enable | disable | dynamic}
  set re-seed-interval <integer>
```

```
end
```

Variable	Description
status enable	Enable the FIPS-CC mode of operation. Note: enable option is available only when the device is not in FIPS mode.
entropy-token {enable disable dynamic}	Configure support for the FortiTRNG entropy token when switching to FIPS mode: <ul style="list-style-type: none"> enable: The token must be present during boot up and reseeding. If the token is not present, the boot up or reseeding is interrupted until the token is inserted. disable: The current entropy implementation is used to seed the Random Number Generator (RNG) (default). dynamic: The token is used to seed or reseed the RNG if it is present. If the token is not present, the boot process is not blocked and the old entropy implementation is used.
re-seed-interval <integer>	The amount of time between RNG reseeding, in minutes (0 - 1440, default = 1440).

fortiview

fortiview setting

Use this command to configure FortiView settings.

Syntax

```
config system fortiview setting
    set not-scanned apps {exclude | include}
    set resolve-ip {enable | disable}
end
```

Variable	Description
not-scanned apps {exclude include}	Include/exclude unscanned applications in FortiView (default = include). Set to exclude to filter out never scanned applications.
resolve-ip {enable disable}	Enable/disable resolving the IP address to the hostname in FortiView (default = disable).

fortiview autocache

Use this command to configure FortiView autocache settings.

Syntax

```
config system fortiview auto-cache
```

```

    set aggressive-fortiview {enable | disable}
    set interval <integer>
    set status {enable | disable}
end

```

Variable	Description
aggressive-fortiview {enable disable}	Enable/disable aggressive auto-cache on FortiView (default = disable).
interval <integer>	The time interval for FortiView auto-cache, in hours (default = 168).
status {enable disable}	Enable/disable FortiView auto-cache (default = enable).

global

Use this command to configure global settings that affect miscellaneous FortiManager features.

Syntax

```

config system global
    set admin-lockout-duration <integer>
    set admin-lockout-threshold <integer>
    set adom-mode {advanced | normal}sh
    set adom-rev-auto-delete {by-days | by-revisions | disable}
    set adom-rev-max-backup-revisions <integer>
    set adom-rev-max-days <integer>
    set adom-rev-max-revisions <integer>
    set adom-select {enable | disable}
    set adom-status {enable | disable}
    set clone-name-option {default | keep}
    set clt-cert-req {enable | disable}
    set console-output {more | standard}
    set country-flag {enable | disable}
    set create-revision {enable | disable}
    set daylightsavetime {enable | disable}
    set detect-unregistered-log-device {enable | disable}
    set device-view-mode {regular | tree}
    set dh-params <integer>
    set disable-module {fortiview-noc}
    set enc-algorithm {high | medium | low}
    set faz-status {enable | disable}
    set fgfm-ca-cert <certificate>
    set fgfm-local-cert <certificate>
    set fgfm-ssl-protocol {ssl3 | tls1.0 | tls1.1 | tls1.2}
    set ha-member-auto-grouping {enable | disable}
    set hostname <string>
    set import-ignore-addr-cmt {enable | disable}
    set language {english | japanese | simch | spanish | trach}
    set latitude <string>
    set ldap-cache-timeout <integer>
    set ldapconntimeout <integer>
    set lock-preempt {enable | disable}

```

```

set log-checksum {md5 | md5-auth | none}
set log-forward-cache-size <integer>
set longitude <string>
set max-log-forward <integer>
set max-running-reports <integer>
set mc-policy-disabled-adoms <adom-name>
set multiple-steps-upgrade-in-autolink {enable | disable}
set object-revision-db-max <integer>
set object-revision-mandatory-note {enable | disable}
set object-revision-object-max <integer>
set object-revision-status {enable | disable}
set oftp-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2 | tlsv1.3}
set partial-install {enable | disable}
set partial-install-force {enable | disable}
set partial-install-rev {enable | disable}
set perform-improve-by-ha {enable | disable}
set per-policy-lock {enable | disable}
set policy-object-icon {enable | disable}
set policy-object-in-dual-pane {enable | disable}
set pre-login-banner {enable | disable}
set pre-login-banner-message <string>
set private-data-encryption {enable | disable}
set remoteauthtimeout <integer>
set search-all-adoms {enable | disable}
set ssl-low-encryption {enable | disable}
set ssl-protocol {tlsv1.3 | tlsv1.2 | tlsv1.1 | tlsv1.0 | sslsv3}
set ssl-static-key-ciphers {enable | disable}
set swapmem {enable | disable}
set task-list-size <integer>
set timezone <integer>
set tunnel-mtu <integer>
set usg {enable | disable}
set vdom-mirror {enable | disable}
set webservice-proto {tlsv1.3 | tlsv1.2 | tlsv1.1 | tlsv1.0 | sslsv3 | sslsv2}
set workspace-mode {disabled | normal | per-adom | workflow}
end

```

Variable	Description
admin-lockout-duration <integer>	Set the lockout duration for FortiManager administration, in seconds (default = 60).
admin-lockout-threshold <integer>	Set the lockout threshold for FortiManager administration (1 - 10, default = 3).
adom-mode {advanced normal}	Set the ADOM mode (default = normal).
adom-rev-auto-delete {by-days by-revisions disable}	Auto delete features for old ADOM revisions: <ul style="list-style-type: none"> by-days: Auto delete ADOM revisions by maximum days. by-revisions: Auto delete ADOM revisions by maximum number of revisions (default). disable: Disable auto delete function for ADOM revision.
adom-rev-max-backup-revisions <integer>	The maximum number of ADOM revisions to backup (default = 5).
adom-rev-max-days <integer>	The maximum number of days to keep old ADOM revisions (default = 30).

Variable	Description
adom-rev-max-revisions <integer>	The maximum number of ADOM revisions to keep (default = 120).
adom-select {enable disable}	Enable/disable a pop-up window that allows administrators to select an ADOM after logging in (default = enable).
adom-status {enable disable}	Enable/disable administrative domains (default = disable).
clone-name-option {default keep}	Set the cloned object name option: <ul style="list-style-type: none"> • default: Add a Clone of prefix to the name. • keep: Keep the original name for the user to edit.
clt-cert-req {enable disable}	Enable/disable requiring a client certificate for GUI login (default = disable). When both <code>clt-cert-req</code> and <code>admin-https-pki-required</code> are enabled, only PKI administrators can connect to the GUI.
console-output {more standard}	Select how the output is displayed on the console (default = standard). Select more to pause the output at each full screen until keypress. Select standard for continuous output without pauses.
country-flag {enable disable}	Enable/disable a country flag icon beside an IP address (default = enable).
create-revision {enable disable}	Enable/disable create revision by default (default = disable).
daylightsavetime {enable disable}	Enable/disable daylight saving time (default = enable). If you enable daylight saving time, the FortiManager unit automatically adjusts the system time when daylight saving time begins or ends.
detect-unregistered-log-device {enable disable}	Enable/disable unregistered log device detection (default = enable).
device-view-mode {regular tree}	Set the devices/groups view mode (default = regular).
dh-params <integer>	Set the minimum size of the Diffie-Hellman prime for SSH/HTTPS, in bits (default = 2048).
disable-module {fortiview-noc}	Disable module list.
enc-algorithm {high medium low}	Set SSL communication encryption algorithms: <ul style="list-style-type: none"> • high: SSL communication using high encryption algorithms (default). • medium: SSL communication using high and medium encryption algorithms. • low: SSL communication using all available encryption algorithms.
faz-status {enable disable}	Enable/disable FortiAnalyzer features in FortiManager (default = disable). This command is not available on the FMG-100C. Note: With FortiManager 7.0.0, you can enable FortiAnalyzer features, or you can have FortiManager HA, but not both at the same time.
fgfm-ca-cert <certificate>	Set the extra FGFM CA certificates ("" = default certificate will be used).
fgfm-local-cert <certificate>	Set the FGFM local certificate ("" = default certificate will be used).
fgfm-ssl-protocol {ssl3 tls1.0 tls1.1 tls1.2}	Set the lowest SSL protocols for fgfmsd (default = tls1.2).

Variable	Description
ha-member-auto-grouping {enable disable}	Enable/disable automatically grouping HA members when the group name is unique in your network (default = enable).
hostname <string>	FortiManager host name.
import-ignore-addr-cmt {enable disable}	Enable/disable import ignore of address comments (default = disable).
language {english japanese simch spanish trach}	GUI language: <ul style="list-style-type: none"> english: English (default) japanese: Japanese simch: Simplified Chinese spanish: Spanish trach: Traditional Chinese
latitude <string>	Set the FortiManager device's latitude.
ldap-cache-timeout <integer>	LDAP cache timeout, in seconds (default = 86400).
ldapconntimeout <integer>	LDAP connection timeout, in milliseconds (default = 60000).
lock-preempt {enable disable}	Enable/disable the ADOM lock override (default = disable).
log-checksum {md5 md5-auth none}	Record log file hash value, timestamp, and authentication code at transmission or rolling: <ul style="list-style-type: none"> md5: Record log file's MD5 hash value only. md5-auth: Record log file's MD5 hash value and authentication code. none: Do not record the log file checksum (default).
log-forward-cache-size <integer>	Set the log forwarding disk cache size, in gigabytes (default = 0).
longitude <string>	Set the FortiManager device's longitude.
max-log-forward <integer>	Set the maximum log forwarding and aggregation number (5 - 20).
max-running-reports <integer>	Maximum running reports number (1 - 10, default = 1).
mc-policy-disabled-adoms <adom-name>	Set the multicast policy disabled ADOMs, separated by spaces. Only ADOMs below version 6.0 can be included.
multiple-steps-upgrade-in-autolink {enable disable}	Enable/disable multiple steps upgrade in an autolink process (default = disable).
object-revision-db-max <integer>	Maximum revisions for a single database (10000 - 1000000, default = 100000).
object-revision-mandatory-note {enable disable}	Enable/disable mandatory note when creating a revision (default = enable).
object-revision-object-max <integer>	Set the maximum revisions for a single object (10 - 1000, default = 100).
object-revision-status {enable disable}	Enable/disable creating revisions when modifying objects (default = enable).
oftp-ssl-protocol {sslsv3 tlsv1.0 tlsv1.1 tlsv1.2 tlsv1.3}	Set the lowest SSL protocols for oftspd (default = tlsv1.2).
partial-install {enable disable}	Enable/disable partial install (install only some objects) (default = disable).

Variable	Description
	Use this command to enable pushing individual objects of the policy package down to all FortiGates in the Policy Package. Once enabled, in the GUI you can right-click an object and choose to install it.
partial-install-force {enable disable}	Enable/disable partial install when the Dev database is modified (default= disable). This option is only available when partial-install is enabled.
partial-install-rev {enable disable}	Enable/disable partial install revision (default= disable). This option is only available when partial-install is enabled.
perform-improve-by-ha {enable disable}	Enable/disable performance improvement by distributing tasks to secondary HA units (default= disable).
per-policy-lock {enable disable}	Enable/disable per policy lock (default= disable). This option is only available in workspace lock mode.
policy-object-icon {enable disable}	Enable/disable show icons of policy objects (default= disable).
policy-object-in-dual-pane {enable disable}	Enable/disable show policies and objects in dual pane (default= disable).
pre-login-banner {enable disable}	Enable/disable pre-login banner (default= disable).
pre-login-banner-message <string>	Set the pre-login banner message.
private-data-encryption {enable disable}	Enable/disable private data encryption using an AES 128 bit key (default = disable).
remoteauthtimeout <integer>	Remote authentication (RADIUS/LDAP) timeout, in seconds (default = 10).
search-all-adoms {enable disable}	Enable/disable search all ADOMs for where-used queries (default= disable).
ssl-low-encryption {enable disable}	Enable/disable SSL low-grade (40-bit) encryption (default= disable).
ssl-protocol {tls1.3 tls1.2 tls1.1 tls1.0 sslv3}	Set the SSL protocols (default = tls1.3 tls1.2).
ssl-static-key-ciphers {enable disable}	Enable/disable SSL static key ciphers (default = enable).
swapmem {enable disable}	Enable/disable virtual memory.
task-list-size <integer>	Set the maximum number of completed tasks to keep (default = 2000).
timezone <integer>	The time zone for the FortiManager unit (default = Pacific Time). See Time zones on page 79
tunnel-mtu <integer>	Set the maximum transportation unit (68 - 9000, default = 1500).
usg {enable disable}	Enable/disable contacting only FortiGuard servers in the USA (default = enable).
vdom-mirror {enable disable}	Enable/disable VDOM mirror (default = disable).

Variable	Description
	<p>Once enabled in the CLI, you can select to enable VDOM Mirror when editing a virtual domain in the <code>System > Virtual Domain</code> device tab in Device Manager. You can then add devices and VDOMs to the list so they may be mirrored. An icon is displayed in the Mirror column of the page to indicate that the VDOM is being mirrored to another device/VDOM.</p> <p>When changes are made to the primary device's VDOM database, a copy is applied to the mirror device's VDOM database. A revision is created and then installed to the devices.</p> <p>VDOM mirror is intended to be used by MSSP or enterprise companies who need to provide a backup VDOM for their customers.</p>
<code>webservice-proto {tls1.3 tls1.2 tls1.1 tls1.0 sslv3 sslv2}</code>	Web Service connection (default = <code>tls1.3</code> <code>tls1.2</code>).
<code>workspace-mode {disabled normal per-adom workflow}</code>	<p>Enable/disable Workspace and Workflow (ADOM locking):</p> <ul style="list-style-type: none"> <code>disabled</code>: Workspace is disabled (default). <code>normal</code>: Workspace lock mode enabled. <code>per-adom</code>: Per-ADOM workspace mode enabled. <code>workspace</code>: Workspace workflow mode enabled.

Example

The following command turns on daylight saving time, sets the FortiManager unit name to FMG3k, and chooses the Eastern time zone for US & Canada.

```
config system global
    set daylightsavetime enable
    set hostname FMG3k
    set timezone 12
end
```

Time zones

Integer	Time zone	Integer	Time zone
00	(GMT-12:00) Eniwetak, Kwajalein	40	(GMT+3:00) Nairobi
01	(GMT-11:00) Midway Island, Samoa	41	(GMT+3:30) Tehran
02	(GMT-10:00) Hawaii	42	(GMT+4:00) Abu Dhabi, Muscat
03	(GMT-9:00) Alaska	43	(GMT+4:00) Baku
04	(GMT-8:00) Pacific Time (US & Canada)	44	(GMT+4:30) Kabul
05	(GMT-7:00) Arizona	45	(GMT+5:00) Ekaterinburg
06	(GMT-7:00) Mountain Time (US & Canada)	46	(GMT+5:00) Islamabad, Karachi, Tashkent

Integer	Time zone	Integer	Time zone
07	(GMT-6:00) Central America	47	(GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi
08	(GMT-6:00) Central Time (US & Canada)	48	(GMT+5:45) Kathmandu
09	(GMT-6:00) Mexico City	49	(GMT+6:00) Almaty, Novosibirsk
10	(GMT-6:00) Saskatchewan	50	(GMT+6:00) Astana, Dhaka
11	(GMT-5:00) Bogota, Lima, Quito	51	(GMT+6:00) Sri Jayawardenapura
12	(GMT-5:00) Eastern Time (US & Canada)	52	(GMT+6:30) Rangoon
13	(GMT-5:00) Indiana (East)	53	(GMT+7:00) Bangkok, Hanoi, Jakarta
14	(GMT-4:00) Atlantic Time (Canada)	54	(GMT+7:00) Krasnoyarsk
15	(GMT-4:00) La Paz	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumqi
16	(GMT-4:00) Santiago	56	(GMT+8:00) Irkutsk, Ulaanbaatar
17	(GMT-3:30) Newfoundland	57	(GMT+8:00) Kuala Lumpur, Singapore
18	(GMT-3:00) Brasilia	58	(GMT+8:00) Perth
19	(GMT-3:00) Buenos Aires, Georgetown	59	(GMT+8:00) Taipei
20	(GMT-3:00) Nuuk (Greenland)	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
21	(GMT-2:00) Mid-Atlantic	61	(GMT+9:00) Yakutsk
22	(GMT-1:00) Azores	62	(GMT+9:30) Adelaide
23	(GMT-1:00) Cape Verde Is	63	(GMT+9:30) Darwin
24	(GMT) Casablanca, Monrovia	64	(GMT+10:00) Brisbane
25	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	65	(GMT+10:00) Canberra, Melbourne, Sydney
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	66	(GMT+10:00) Guam, Port Moresby
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	67	(GMT+10:00) Hobart
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris	68	(GMT+10:00) Vladivostok
29	(GMT+1:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb	69	(GMT+11:00) Magadan
30	(GMT+1:00) West Central Africa	70	(GMT+11:00) Solomon Is., New Caledonia
31	(GMT+2:00) Athens, Istanbul, Minsk	71	(GMT+12:00) Auckland, Wellington
32	(GMT+2:00) Bucharest	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is
33	(GMT+2:00) Cairo	73	(GMT+13:00) Nuku'alofa
34	(GMT+2:00) Harare, Pretoria	74	(GMT-4:30) Caracas

Integer	Time zone	Integer	Time zone
35	(GMT+2:00) Helsinki, Riga, Tallinn	75	(GMT+1:00) Namibia
36	(GMT+2:00) Jerusalem	76	(GMT-5:00) Brazil-Acre
37	(GMT+3:00) Baghdad	77	(GMT-4:00) Brazil-West
38	(GMT+3:00) Kuwait, Riyadh	78	(GMT-3:00) Brazil-East
39	(GMT+3:00) Moscow, St.Petersburg, Volgograd	79	(GMT-2:00) Brazil-DeNoronha

ha

Use the `config system ha` command to enable and configure FortiManager high availability (HA). FortiManager HA provides a solution for a key requirement of critical enterprise management and networking components: enhanced reliability.

A FortiManager HA cluster consists of up five FortiManager units of the same FortiManager model. One of the FortiManager units in the cluster operates as a primary unit and the other one to four units operate as backup units. All of the units are visible on the network. The primary unit and the backup units can be at the same location. FortiManager HA also supports geographic redundancy so the primary unit and backup units can be in different locations attached to different networks as long as communication is possible between them (for example over the Internet, over a WAN, or through a private network).

Note: With FortiManager 7.0.0, you can enable FortiAnalyzer features, or you can have FortiManager HA, but not both at the same time.

Administrators connect to the primary unit GUI or CLI to perform FortiManager operations. The primary unit also interacts with managed FortiGate devices, and FortiSwitch devices. Managed devices connect with the primary unit for configuration backup and restore. If FortiManager is being used to distribute firmware updates and FortiGuard updates to managed devices, the managed devices can connect to the primary unit or one of the backup units.

If the primary FortiManager unit fails you must manually configure one of the backup units to become the primary unit. The new primary unit will have the same IPv4 addresses as it did when it was the backup unit. For the managed devices to automatically start using the new primary unit, you should add all of the FortiManager units in the cluster to the managed devices.

For more information, see the [FortiManager Administration Guide](#).

Syntax

```
config system ha
  set clusterid <clustert_ID_int>
  set file-quota <integer>
  set hb-interval <integer>
  set hb-lost-threshold <integer>
  set local-cert <string>
  set mode {primary | secondary | standalone}
  set password <passwd>
config peer
  edit <peer_id_int>
    set ip <peer_ipv4_address>
```

```

    set ip6 <peer_ipv6_address>
    set serial-number <string>
    set status {enable | disable}
end
end

```

Variable	Description
clusterid <clusert_ID_int>	<p>A number that identifies the HA cluster (1 - 64, default = 1).</p> <p>All members of the HA cluster must have the same cluster ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different ID.</p>
file-quota <integer>	Set the HA file quota, in megabytes (2048 - 20480, default = 4096).
hb-interval <integer>	<p>The time that a cluster unit waits between sending heartbeat packets, in seconds (1 - 255, default = 10).</p> <p>The heartbeat interval is also the amount of time that a cluster unit waits before expecting to receive a heartbeat packet from the other cluster unit.</p>
hb-lost-threshold <integer>	<p>The number of heartbeat intervals that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed (1 - 255, default = 30).</p> <p>In most cases you do not have to change the heartbeat interval or failover threshold. The default settings mean that if the a unit fails, the failure is detected after 3 x 5 or 15 seconds; resulting in a failure detection time of 15 seconds.</p> <p>If the failure detection time is too short the HA cluster may detect a failure when none has occurred. For example, if the primary unit is very busy it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume that the primary unit has failed when the primary unit is actually just busy. Increase the failure detection time to prevent the backup unit from detecting a failure when none has occurred.</p> <p>If the failure detection time is too long, administrators will be delayed in learning that the cluster has failed. In most cases, a relatively long failure detection time will not have a major effect on operations. But if the failure detection time is too long for your network conditions, then you can reduce the heartbeat interval or failover threshold.</p>
local-cert <string>	Set the local HA certificate.
mode {primary secondary standalone}	<p>The HA mode (default = standalone).</p> <p>Select <code>primary</code> to configure the FortiManager unit to be the primary unit in a cluster. Select <code>secondary</code> to configure the FortiManager unit to be a backup unit in a cluster. Select <code>standalone</code> to stop operating in HA mode.</p>
password <passwd>	A group password for the HA cluster. All members of the HA cluster must have the same group password. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password (character limit: 19).
peer	<p>Add peers to the HA configuration of the FortiManager unit.</p> <p>For the primary unit, add all of the backup units as peers, up to a maximum of four.</p>

Variable	Description
	For a backup unit, only add the primary unit as a peer.
Variables for <code>config peer</code> subcommand:	
<peer_id_int>	Add a peer and add the peer's IPv4 or IPv6 address and serial number.
ip <peer_ipv4_address>	Enter the IPv4 address of the peer FortiManager unit.
ip6 <peer_ipv6_address>	Enter the IPv6 address of the peer FortiManager unit.
serial-number <string>	Enter the serial number of the peer FortiManager unit.
status {enable disable}	Enter the status of the peer FortiManager unit (default = enable).

General FortiManager HA configuration steps

The following steps assume that you are starting with four FortiManager units running the same firmware build and are set to the factory default configuration. The primary unit and the first backup unit are connected to the same network. The second and third backup units are connected to a remote network and communicate with the primary unit over the Internet.

1. Enter the following command to configure the primary unit for HA operation.

```
config system ha
  set mode primary
  set password <password_str>
  set clusterid 10
  config peer
    edit 1
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
    edit 2
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
    edit 3
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
  end
```

This command configures the FortiManager unit to operate as the primary unit, adds a password, sets the clusterid to 10, and accepts defaults for the other HA settings. This command also adds the three backup units to the primary unit as peers.

2. Enter the following command to configure the backup units for HA operation.

```
config system ha
  set mode secondary
  set password <password_str>
  set clusterid 10
  config peer
    edit 1
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
```

end

This command configures the FortiManager unit to operate as a backup unit, adds the same password, and `clusterid` as the primary unit, and accepts defaults for the other HA settings. This command also adds the primary unit to the backup unit as a peer.

3. Repeat step 2 to configure each backup unit.

ha-scheduled-check

Use this command to schedule an HA integrity check.

Syntax

```
config system ha-scheduled-check
  set status {enable | disable}
  set time <hh:mm:ss>
  set week_days {monday tuesday wednesday thursday friday saturday sunday}
end
```

Variable	Description
status {enable disable}	Enable/disable scheduled backups (default = disable).
time <hh:mm:ss>	Enter the time of day to perform the backup. Time is required in the form <hh:mm:ss> where hh: 0-23, mm: 0-59, and ss: 0-59.
week_days {monday tuesday wednesday thursday friday saturday sunday}	Enter the days of the week on which to perform backups. You may enter multiple days.

interface

Use this command to edit the configuration of a FortiManager network interface.

Syntax

```
config system interface
  edit <port>
    set status {enable | disable}
    set ip <ipv4_mask>
    set allowaccess {http https ping snmp soc-fabric ssh webservice}
    set serviceaccess {fclupdates fgtupdates webfilter-antispam}
    set update-service-ip <ip&netmask>
    set rating-service-ip <ip&netmask>
    set speed {1000full 100full 100half 10full 10half auto}
    set description <string>
    set alias <string>
    set mtu <integer>
```

```

config ipv6
    set ip6-address <ipv6 prefix>
    set ip6-allowaccess {http https https-logging ping snmp ssh webservice}
    set ip6-autoconf {enable | disable}
end
end

```

Variable	Description
<port>	The port can be set to a port number such as port1, port2, port3, or port4. Different FortiManager models have different numbers of ports.
status {enable disable}	Enable/disable the interface (default = enable). If the interface is disabled it does not accept or send packets. If you disable a physical interface, VLAN interfaces associated with it are also disabled.
ip <ipv4_mask>	Enter the interface IPv4 address and netmask. The IPv4 address cannot be on the same subnet as any other interface.
allowaccess {http https ping snmp soc-fabric ssh webservice}	Enter the types of management access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.
serviceaccess {fclupdates fgtupdates webfilter-antispam}	Enter the types of service access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required. <ul style="list-style-type: none"> fclupdates: FortiClient updates access. fgtupdates: FortiGate updates access. webfilter-antispam: Web filtering and antispam access.
update-service-ip <ip&netmask>	The IP address for the FortiGate update service. It must be on the same subnet as the interface IP address. This variable is only available when serviceaccess is fgtupdates.
rating-service-ip <ip&netmask>	The IP address for the FortiGate rating service. It must be on the same subnet as the interface IP address. This variable is only available when serviceaccess is webfilter-antispam.
speed {1000full 100full 100half 10full 10half auto}	Enter the speed and duplexing the network port uses: <ul style="list-style-type: none"> 100full: 100M full-duplex 100half: 100M half-duplex 10full: 10M full-duplex 10half: 10M half-duplex auto: Automatically negotiate the fastest common speed (default)
description <string>	Enter a description of the interface (character limit = 63).
alias <string>	Enter an alias for the interface.
mtu <integer>	Set the maximum transportation unit (68 - 9000, default = 1500).
Variables for config ipv6 subcommand:	
ip6-address <ipv6 prefix>	IPv6 address/prefix of interface.

Variable	Description
ip6-allowaccess {http https https-logging ping snmp ssh webservice}	Allow management access to the interface.
ip6-autoconf {enable disable}	Enable/disable address automatic configuration (SLAAC) (default = enable).

Example

This example shows how to set the FortiManager port1 interface IPv4 address and network mask to 192.168.100.159 and 255.255.255.0, and the management access to ping, https, and ssh.

```
config system interface
  edit port1
    set allowaccess ping https ssh
    set ip 192.168.110.26 255.255.255.0
    set status up
  end
```

locallog

Use the following commands to configure local log settings.

locallog setting

Use this command to configure locallog logging settings.

Syntax

```
config system locallog setting
  set log-interval-dev-no-logging <integer>
  set log-interval-disk-full <integer>
  set log-interval-gbday-exceeded <integer>
end
```

Variable	Description
log-interval-dev-no-logging <integer>	Interval for logging the event of no logs received from a device, in minutes (default = 1400).
log-interval-disk-full <integer>	Interval for logging the event of disk full, in minutes (default = 5).
log-interval-gbday-exceeded <integer>	Interval for logging the event of the GB/Day license exceeded, in minutes (default = 1400).

locallog disk setting

Use this command to configure the disk settings for uploading log files, including configuring the severity of log levels.

- **status must be enabled to view** diskfull,max-log-file-size and upload variables.
- **upload must be enabled to view/set** other upload* variables.

Syntax

```
config system locallog disk setting
  set status {enable | disable}
  set severity {alert | critical | debug | emergency | error | information |
    notification | warning}
  set max-log-file-size <integer>
  set roll-schedule {none | daily | weekly}
  set roll-day {sunday | monday | tuesday | wednesday | thursday | friday | saturday}
  set roll-time <hh:mm>
  set diskfull {nolog | overwrite}
  set log-disk-full-percentage <integer>
  set upload {enable | disable}
  set uploadip <ipv4_address>
  set server-type {FAZ | FTP | SCP | SFTP}
  set uploadport <integer>
  set uploaduser <string>
  set uploadpass <passwd>
  set uploadaddr <string>
  set uploadtype <event>
  set uploadzip {enable | disable}
  set uploadsched {enable | disable}
  set upload-time <hh:mm>
  set upload-delete-files {enable | disable}
end
```

Variable	Description
status {enable disable}	Enable/disable logging to the local disk (default = enable)
severity {emergency alert critical error warning notification information debug}	<p>Select the logging severity level.</p> <p>The FortiManager unit logs all messages at and above the logging severity level you select.</p> <ul style="list-style-type: none"> • emergency: The unit is unusable. • alert: Immediate action is required. • critical: Functionality is affected. • error: Functionality is probably affected. • warning: Functionality might be affected. • notification: Information about normal events. • information: General information about unit operations (default). • debug: Information used for diagnosis or debugging.
max-log-file-size <integer>	Enter the size at which the log is rolled, in megabytes (1 - 1024, default = 100).
roll-schedule {none daily weekly}	<p>Enter the period for the scheduled rolling of a log file:</p> <ul style="list-style-type: none"> • none: Not scheduled; the log rolls when max-log-file-size is reached

Variable	Description
	(default). <ul style="list-style-type: none"> daily: Every day. weekly: Every week.
roll-day {sunday monday tuesday wednesday thursday friday saturday}	Enter the day for the scheduled rolling of a log file (default = sunday).
roll-time <hh:mm>	Enter the time for the scheduled rolling of a log file.
diskfull {nolog overwrite}	Enter action to take when the disk is full: <ul style="list-style-type: none"> nolog: stop logging overwrite: overwrites oldest log entries (default)
log-disk-full-percentage <integer>	Enter the percentage at which the log disk will be considered full (50 - 90, default = 80).
upload {enable disable}	Enable/disable uploading of logs when rolling log files (default = disable).
uploadip <ipv4_address>	Enter IPv4 address of the destination server.
server-type {FTP SCP SFTP}	Enter the server type to use to store the logs: <ul style="list-style-type: none"> FTP: upload via FTP (default) SCP: upload via SCP SFTP: upload via SFTP
uploadport <integer>	Enter the port to use when communicating with the destination server (1 - 65535, default = 0).
uploaduser <string>	Enter the user account on the destination server.
uploadpass <passwd>	Enter the password of the user account on the destination server (character limit = 127).
uploaddir <string>	Enter the destination directory on the remote server.
uploadtype <event>	Enter to upload the event log files (default = event).
uploadzip {enable disable}	Enable to compress uploaded log files (default = disable).
uploadsched {enable disable}	Enable to schedule log uploads (default = disable).
upload-time <hh:mm>	Enter to configure when to schedule an upload.
upload-delete-files {enable disable}	Enable/disable deleting log files after uploading (default = enable).

Example

In this example, the logs are uploaded to an upload server and are not deleted after they are uploaded.

```
config system locallog disk setting
  set status enable
  set severity information
  set max-log-file-size 1000MB
  set roll-schedule daily
```

```
set upload enable
set uploadip 10.10.10.1
set uploadport port 443
set uploaduser myname2
set uploadpass 12345
set uploadtype event
set uploadzip enable
set uploadsched enable
set upload-time 06:45
set upload-delete-file disable
end
```

locallog filter

Use this command to configure filters for local logs. All keywords are visible only when event is enabled.

Syntax

```
config system locallog {disk | memory | fortianalyzer | fortianalyzer2 | fortianalyzer3 |
    syslogd | syslogd2 | syslogd3} filter
set aid {enable | disable}
set devcfg {enable | disable}
set devops {enable | disable}
set diskquota {enable | disable}
set dm {enable | disable}
set docker {enable | disable}
set dvm {enable | disable}
set ediscovery {enable | disable}
set epmgr {enable | disable}
set event {enable | disable}
set eventmgmt {enable | disable}
set faz {enable | disable}
set fazha {enable | disable}
set fazsys {enable | disable}
set fgd {enable | disable}
set fgfm {enable | disable}
set fips {enable | disable}
set fmgws {enable | disable}
set fmlmgr {enable | disable}
set fmwmgr {enable | disable}
set fortiview {enable | disable}
set glbcfg {enable | disable}
set ha {enable | disable}
set hcache {enable | disable}
set incident {enable | disable}
set iolog {enable | disable}
set logd {enable | disable}
set logdb {enable | disable}
set logdev {enable | disable}
set logfile {enable | disable}
set logging {enable | disable}
set lrmgr {enable | disable}
set objcfg {enable | disable}
set report {enable | disable}
```

```

set rev {enable | disable}
set rtmon {enable | disable}
set scfw {enable | disable}
set scply {enable | disable}
set scrmgr {enable | disable}
set scvpn {enable | disable}
set system {enable | disable}
set webport {enable | disable}
end

```

Variable	Description
aid {enable disable}	Enable/disable configuring aid messages (default = enable).
devcfg {enable disable}	Enable/disable logging device configuration messages (default = enable).
devops {enable disable}	Enable/disable managed device's operations messages (default = enable).
diskquota {enable disable}	Enable/disable logging FortiAnalyzer disk quota messages (default = enable).
dm {enable disable}	Enable/disable logging deployment manager messages (default = enable).
docker {enable disable}	Enable/disable docker application generic messages (default = enable).
dvm {enable disable}	Enable/disable logging device manager messages (default = enable).
ediscovery {enable disable}	Enable/disable logging device manager messages (default = enable).
epmgr {enable disable}	Enable/disable logging endpoint manager messages (default = enable).
event {enable disable}	Enable/disable configuring log filter messages (default = enable).
eventmgmt {enable disable}	Enable/disable logging FortiAnalyzer event handler messages (default = enable).
faz {enable disable}	Enable/disable logging FortiAnalyzer messages (default = enable).
fazha {enable disable}	Enable/disable logging FortiAnalyzer HA messages (default = enable).
fazsys {enable disable}	Enable/disable logging FortiAnalyzer system messages (default = enable).
fgd {enable disable}	Enable/disable logging FortiGuard service messages (default = enable).
fgfm {enable disable}	Enable/disable logging FortiGate/FortiManager communication protocol messages (default = enable).
fips {enable disable}	Enable/disable logging FIPS messages (default = enable).
fmgws {enable disable}	Enable/disable logging web service messages (default = enable).
fmlmgr {enable disable}	Enable/disable logging FortiMail manager messages (default = enable).
fmwmgr {enable disable}	Enable/disable logging firmware manager messages (default = enable).
fortiview {enable disable}	Enable/disable logging FortiAnalyzer FortiView messages (default = enable).
glbcfg {enable disable}	Enable/disable logging global database messages (default = enable).
ha {enable disable}	Enable/disable logging high availability activity messages (default = enable).
hcache {enable disable}	Enable/disable logging hcache messages (default = enable).
incident {enable disable}	Enable/disable logging FortiAnalyzer incident messages (default = enable).

Variable	Description
iolog {enable disable}	Enable/disable input/output log activity messages (default = enable).
logd {enable disable}	Enable/disable logd messages (default = enable).
logdb {enable disable}	Enable/disable logging FortiAnalyzer log DB messages (default = enable).
logdev {enable disable}	Enable/disable logging FortiAnalyzer log device messages (default = enable).
logfile {enable disable}	Enable/disable logging FortiAnalyzer log file messages (default = enable).
logging {enable disable}	Enable/disable logging FortiAnalyzer logging messages (default = enable).
lrmgr {enable disable}	Enable/disable logging log and report manager messages (default = enable).
objcfg {enable disable}	Enable/disable logging object configuration (default = enable).
report {enable disable}	Enable/disable logging FortiAnalyzer report messages (default = enable).
rev {enable disable}	Enable/disable logging revision history messages (default = enable).
rtmon {enable disable}	Enable/disable logging real-time monitor messages (default = enable).
scfw {enable disable}	Enable/disable logging firewall objects messages (default = enable).
scply {enable disable}	Enable/disable logging policy console messages (default = enable).
scrmgr {enable disable}	Enable/disable logging script manager messages (default = enable).
scvpn {enable disable}	Enable/disable logging VPN console messages (default = enable).
system {enable disable}	Enable/disable logging system manager messages (default = enable).
webport {enable disable}	Enable/disable logging web portal messages (default = enable).

Example

In this example, the local log filters are log and report manager, and system settings. Events in these areas of the FortiManager unit will be logged.

```
config system locallog filter
  set event enable
  set lrmgr enable
  set system enable
end
```

locallog fortianalyzer (fortianalyzer2, fortianalyzer3) setting

Use this command to enable or disable, and select the severity threshold of, remote logging to the FortiAnalyzer units. You can configure up to three FortiAnalyzer devices.

The severity threshold required to forward a log message to the FortiAnalyzer unit is separate from event, syslog, and local logging severity thresholds.

Syntax

```
config system locallog {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
    set reliable {enable | disable}
    set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
    set server <address>
    set secure-connection {enable | disable}
    set status {disable | realtime | upload}
    set upload-time <hh:mm>
end
```

Variable	Description
reliable {enable disable}	Enable/disable reliable realtime logging (default = disable).
severity {emergency alert critical error warning notification information debug }	Select the logging severity level (default = notification). The FortiManager unit logs all messages at and above the logging severity level you select.
server <address>	Remote FortiAnalyzer server IP address, FQDN, or hostname.
secure-connection {enable disable}	Enable/disable connection secured by TLS/SSL (default = disable).
status {disable realtime upload}	Set the log to FortiAnalyzer status: <ul style="list-style-type: none"> • disable: Do not log to FortiAnalyzer (default). • realtime: Log to FortiAnalyzer in realtime. • upload: Log to FortiAnalyzer at a scheduled time.
upload-time <hh:mm>	Set the time to upload local log files (default = 00:00).

Example

You might enable remote logging to the FortiAnalyzer unit configured. Events at the information level and higher, which is everything except debug level events, would be sent to the FortiAnalyzer unit.

```
config system locallog fortianalyzer setting
    set status enable
    set severity information
end
```

locallog memory setting

Use this command to configure memory settings for local logging purposes.

Syntax

```
config system locallog memory setting
    set diskfull {nolog | overwrite}
    set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
    set status {enable | disable}
```

```
end
```

Variable	Description
diskfull {nolog overwrite}	Enter the action to take when the disk is full: <ul style="list-style-type: none"> nolog: stop logging when disk full overwrite: overwrite oldest log entries (default)
severity {emergency alert critical error warning notification information debug}	Select the logging severity level (default = notification). The FortiManager unit logs all messages at and above the logging severity level you select.
status {enable disable}	Enable/disable logging to the memory buffer (default = disable).

Example

This example shows how to enable logging to memory for all events at the notification level and above. At this level of logging, only information and debug events will not be logged.

```
config system locallog memory
    set severity notification
    set status enable
end
```

locallog syslogd (syslogd2, syslogd3) setting

Use this command to configure the settings for logging to a syslog server. You can configure up to three syslog servers: syslogd, syslogd2 and syslogd3.

Syntax

```
config system locallog {syslogd | syslogd2 | syslogd3} setting
    set cert {Fortinet_Local | Fortinet_Local2}
    set csv {enable | disable}
    set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel |
        local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr |
        mail | news | ntp | syslog | user | uucp}
    set reliable {enable | disable}
    set secure-connection {enable | disable}
    set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
    set status {enable | disable}
    set syslog-name <string>
end
```

Variable	Description
cert {Fortinet_Local Fortinet_Local2}	Select local certificate used for secure connection.
csv {enable disable}	Enable/disable producing the log in comma separated value (CSV) format (default = disable).

Variable	Description
	If you do not enable CSV format the FortiManager unit produces space separated log files.
facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp syslog user uucp}	Enter the facility type (default = local7). The facility identifies the source of the log message to syslog. Change <i>facility</i> to distinguish log messages from different FortiManager units so you can determine the source of the log messages. <i>local0</i> to <i>local7</i> are reserved for local use.
reliable {enable disable}	Enable/disable reliable real time logging (default = disable).
secure-connection {enable disable}	Enable/disable connection secured by TLS/SSL (default = disable). This variable is available only when <i>reliable</i> is enabled.
severity {emergency alert critical error warning notification information debug}	Select the logging severity level (default = notification). The FortiManager unit logs all messages at and above the logging severity level you select.
status {enable disable}	Enable/disable logging to the remote syslog server (default = disable).
syslog-name <string>	Enter the remote syslog server name. To configure a syslog server, use the <code>config system syslog</code> command. See syslog on page 123 for information.

Example

In this example, the logs are uploaded to a previously configured syslog server named `logstorage`. The FortiManager unit is identified as facility `local0`.

```
config system locallog syslogd setting
  set facility local0
  set syslog-name logstorage
  set status enable
  set severity information
end
```

log

Use the following commands to configure log settings.

log alert

Use this command to configure log based alert settings.

Syntax

```
config system log alert
    set max-alert-count <integer>
end
```

Variable	Description
max-alert-count <integer>	Maximum number of alerts supported (100 - 10000, default = 1000).

log device-disable

Use this command to disable the client device logging.

Syntax

```
config system log device-disable
    edit <id>
        set device <string>
        set TTL <string>
    end
```

Variable	Description
<id>	The device ID.
device <string>	The device ID to be used for disabling logging. Note: The device ID is not checked against the currently registered devices in the system. The entered device ID is ignored if no match is found.
TTL <string>	Set the duration for Time to Live (TTL). For instance, enter 1d5h for 1 day and 5 hours. Supported units: <ul style="list-style-type: none">• d- day.• h- hour.• m- minute.• s- second. Leave the field unset for no expiration. Note: Do not input auto generated part from [expire:..

log interface-stats

Use this command to configure log based interface statistics settings.

Syntax

```
config system log interface-stats
    set billing-report {enable | disable}
```

```

set retention-days <integer>
set sampling-interval <integer>
set status {enable | disable}
end

```

Variable	Description
billing-report {enable disable}	Enable/disable billing report feature (default = disable).
retention-days <integer>	The number of days that interface data are stored (0 - 2000, default = 100)
sampling-interval <integer>	The interval in which interface data are received from FortiGate devices, in seconds (300 - 86400, default = 1200)
status {enable disable}	Enable/disable interface statistics (default = enable).

log ioc

Use this command to configure log based IoC (Indicators of Compromise) settings.

Syntax

```

config system log ioc
set notification {enable | disable}
set notification-throttle <integer>
set rescan-max-runner <integer>
set rescan-run-at <integer>
set rescan-status {enable | disable}
set status {enable | disable}
end

```

Variable	Description
notification {enable disable}	Enable/disable IoC notification (default = enable).
notification-throttle <integer>	Set the minute value for throttling the rate of IoC notifications (1 - 10080, default = 1440).
rescan-max-runner <integer>	Set the maximum number of concurrent IoC rescans (1 to CPU count, default = 8).
rescan-run-at <integer>	Set the hour of the day when IoC rescan runs (1 - 24, 0 = run immediately, default = 24).
rescan-status {enable disable}	Enable/disable IoC rescan (default = enable).
status {enable disable}	Enable/disable the IoC feature (default = enable).

log mail-domain

Use this command to configure FortiMail domain settings.

Syntax

```

config system log mail-domain

```

```

edit <id>
    set devices <string>
    set domain <string>
    set vdom <string>
end

```

Variable	Description
<id>	The ID of the FortiMail domain.
devices <string>	The device IDs for domain to VDOM mapping, separated by commas (default = All_FortiMails). For example: FEVM020000000000, FEVM020000000001
domain <string>	The FortiMail domain.
vdom <string>	The VDOM name that is mapping to the FortiMail domain.

log ratelimit

Use this command to log the rate limit.

Syntax

```

config system log ratelimit
    set device-ratelimit-default <integer>
    set mode {disable | manual}
    set system-ratelimit <integer>
config device
    edit id
        set device <string>
        set filter-type devid
        set ratelimit <integer>
    end
end

```

Variable	Description
device-ratelimit-default <integer>	The default maximum device log rate limit (default = 0). Note: This command is only available when the mode is set to <code>manual</code> .
mode {disable manual}	The logging rate limit mode (default = disable). In the manual mode, the system rate limit and the device rate limit both are configurable, no limit if not configured.
system-ratelimit <integer>	The maximum system log rate limit (default = 0). Note: This command is only available when the mode is set to <code>manual</code> .
device	The device log rate limit.
Variables for <code>config device</code> subcommand:	

Variable	Description
<id>	The device id.
device <string>	The device(s) filter according to the filter-type setting. Note: Wildcard expression is supported.
filter-type devid	The device filter type .
ratelimit <integer>	The maximum device log rate limit (default = 0).

log settings

Use this command to configure settings for logs.

Syntax

```
config system log settings
  set browse-max-logfiles <integer>
  set dns-resolve-dstip {enable | disable}
  set download-max-logs <integer>
  set FAC-custom-field1 <string>
  set FAZ-custom-field1 <string>
  set FCH-custom-field1 <string>
  set FCT-custom-field1 <string>
  set FDD-custom-field1 <string>
  set FGT-custom-field1 <string>
  set FMG-custom-field1 <string>
  set FML-custom-field1 <string>
  set FPX-custom-field1 <string>
  set FSA-custom-field1 <string>
  set FWB-custom-field1 <string>
  set ha-auto-migrate {enable | disable}
  set import-max-logfiles <integer>
  set log-file-archive-name {basic | extended}
  set sync-search-timeout <integer>
  config {rolling-regular | rolling-local | rolling-analyzer}
    set days {fri | mon | sat | sun | thu | tue | wed}
    set del-files {enable | disable}
    set directory <string>
    set file-size <integer>
    set gzip-format {enable | disable}
    set hour <integer>
    set ip <ipv4_address>
    set ip2 <ipv4_address>
    set ip3 <ipv4_address>
    set log-format {csv | native | text}
    set min <integer>
    set password <passwd>
    set password2 <passwd>
    set password3 <passwd>
```

```

    set port <integer>
    set port2 <integer>
    set port3 <integer>
    set server-type {ftp | scp | sftp}
    set upload {enable | disable}
    set upload-hour <integer>
    set upload-mode {backup | mirror}
    set upload-trigger {on-roll | on-schedule}
    set username <string>
    set username2 <string>
    set username3 <string>
    set when {daily | none | weekly}
end
end

```

Variable	Description
browse-max-logfiles <integer>	Maximum number of log files for each log browse attempt, per ADOM (default = 10000).
dns-resolve-stip {enable disable}	Enable/disable resolving destination IP by DNS (default = disable).
download-max-logs <integer>	Maximum number of logs for each log download attempt (default = 100000).
FAC-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FAZ-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FCH-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FCT-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FDD-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FGT-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FMG-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FML-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FPX-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FSA-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FWB-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
ha-auto-migrate {enable disable}	Enabled/disable automatically merging HA member's logs to HA cluster (default = disable).
import-max-logfiles <integer>	Maximum number of log files for each log import attempt (default = 10000).
log-file-archive-name {basic extended}	Log file name format for archiving. <ul style="list-style-type: none"> • basic: Basic format for log archive file name (default), for example: FGT20C0000000001.tlog.1417797247.log. • extended: Extended format for log archive file name, for example: FGT20C0000000001.2014-12-05-08:34:58.tlog.1417797247.log.
sync-search-timeout <integer>	The maximum amount of time that a log search session can run in synchronous mode, in seconds (1 - 86400, default = 60).

Variable	Description
Variables for <code>config {rolling-regular rolling-local rolling-analyzer}</code> subcommand:	
<code>days {fri mon sat sun thu tue wed}</code>	Log files rolling schedule (days of the week). When <code>when</code> is set to <code>weekly</code> , you can configure <code>days</code> , <code>hour</code> , and <code>min</code> values.
<code>del-files {enable disable}</code>	Enable/disable log file deletion after uploading (default = disable).
<code>directory <string></code>	The upload server directory (character limit = 127).
<code>file-size <integer></code>	Roll log files when they reach this size, in megabytes (10 - 1000, default = 200).
<code>gzip-format {enable disable}</code>	Enable/disable compression of uploaded log files (default = disable).
<code>hour <integer></code>	The hour of the day that log files are rolled (0 - 23, default = 0).
<code>ip <ipv4_address></code> <code>ip2 <ipv4_address></code> <code>ip3 <ipv4_address></code>	Upload server IPv4 addresses. Configure up to three servers.
<code>log-format {csv native text}</code>	Format of uploaded log files: <ul style="list-style-type: none"> <code>csv</code>: CSV (comma-separated value) format. <code>native</code>: Native format (text or compact) (default). <code>text</code>: Text format (convert if necessary).
<code>min <integer></code>	The minute of the hour that log files are rolled (0 - 59, default = 0).
<code>password <passwd></code> <code>password2 <passwd></code> <code>password3 <passwd></code>	Upload server log in passwords (character limit = 128).
<code>port <integer></code> <code>port2 <integer></code> <code>port3 <integer></code>	Upload server IP port number.
<code>server-type {ftp scp sftp}</code>	Upload server type (default = ftp).
<code>upload {enable disable}</code>	Enable/disable log file uploads (default = disable).
<code>upload-hour <integer></code>	The hour of the day that log files are uploaded (0 - 23, default = 0).
<code>upload-mode {backup mirror}</code>	Configure upload mode with multiple servers. Servers are tried then used one after the other upon failure to connect. <ul style="list-style-type: none"> <code>backup</code>: Servers are attempted and used one after the other upon failure to connect (default). <code>mirror</code>: All configured servers are attempted and used.
<code>upload-trigger {on-roll on-schedule}</code>	Event triggering log files upload: <ul style="list-style-type: none"> <code>on-roll</code>: Upload log files after they are rolled (default). <code>on-schedule</code>: Upload log files daily.
<code>username <string></code> <code>username2 <string></code> <code>username3 <string></code>	Upload server log in usernames (character limit = 35).
<code>when {daily none weekly}</code>	Roll log files periodically: <ul style="list-style-type: none"> <code>daily</code>: Roll log files daily.

Variable	Description
	<ul style="list-style-type: none"> • none: Do not roll log files periodically (default). • weekly: Roll log files on certain days of week.

log-fetch

Use the following commands to configure log fetching.

log-fetch client-profile

Use this command to configure the fetching client settings.

Syntax

```

config system log-fetch client-profile
  edit <id>
    set client-adom <string>
    set data-range {custom}
    set data-range-value <integer>
    set end-time <hh:mm> <yyyy/mm/dd>
    set index-fetch-logs {enable | disable}
    set log-filter-status {enable | disable}
    set log-filter-logic {and | or}
    set name <string>
    set password <passwd>
    set secure-connection {enable | disable}
    set server-adom <string>
    set server-ip <ip>
    set start-time <hh:mm> <yyyy/mm/dd>
    set sync-adom-config
    set user <string>
    config device-filter
      edit <id>
        set adom <string>
        set device <device>
        set vdom <string>
      next
    config log-filter
      edit <id>
        set field <string>
        set oper {= | != | < | > | <= | >= | contain | not-contain | match}
        set value <string>
      next
    next
  end
end

```

Variable	Description
<id>	The log-fetch client profile ID.
client-adom <string>	Log-fetch client side's adom name.
data-range {custom}	The data range settings for the fetched logs, which is always custom.
data-range-value <integer>	An integer representing the data range value.
end-time <hh:mm> <yyyy/mm/dd>	Set the end date and time of the data-range.
index-fetch-logs {enable disable}	Enable/disable indexing logs automatically after fetching logs (default = enabled).
log-filter-status {enable disable}	Enable/Disable log-filter (default = disabled).
log-filter-logic {and or}	Set the logic for the log filters (default = or).
name <string>	The name of log-fetch client profile.
password <passwd>	The log-fetch server password.
secure-connection {enable disable}	Enable/disable protecting log-fetch connection with TLS/SSL (default = enabled).
server-adom <string>	Log-fetch server side's adom name.
server-ip <ip>	The log fetch server IPv4 address.
start-time <hh:mm> <yyyy/mm/dd>	Set the start date and time of the data-range. The start date should be earlier than the end date.
sync-adom-config {enable disable}	Enable/disable synchronizing the ADOM configuration.
user <string>	The log-fetch server username.
Variables for <code>config device-filter</code> subcommand:	
<id>	Add or edit a device filter.
adom <string>	Enter the ADOM name.
device <device>	Enter the device name or serial number.
vdom <string>	Enter the VDOM, if required.
Variables for <code>config log-filter</code> subcommand:	
<id>	The log filter ID.
field <string>	Enter the field name.
oper {= != < > <= >= contain not-contain match}	Set the filter operator.
value <string>	Enter the field filter operand or free-text matching expression.

log-fetch server-setting

Use this command to configure the fetching server settings.

Syntax

```
config system log-fetch server-setting
    set max-conn-per-session <integer>
    set max-sessions <integer>
    set user <string>
end
```

Variable	Description
max-conn-per-session <integer>	The maximum number of concurrent file download connections per session (default = 3).
max-sessions <integer>	The maximum number of concurrent fetch sessions (default = 1).
session-timeout <integer>	Set the fetch session timeout period, in minutes (default = 10). This option is only available in server mode.

mail

Use this command to configure mail servers on your FortiManager unit.

Syntax

```
config system mail
    edit <id>
        set auth {enable | disable}
        set auth-type {certificate | psk}
        set local-cert {Fortinet_Local | Fortinet_Local2}
        set passwd <passwd>
        set port <integer>
        set secure-option {default | none | smtps | starttls}
        set server <string>
        set user <string>
    end
```

Variable	Description
<id>	Enter the mail service ID of the entry you would like to edit or type a new name to create an entry (character limit = 63).
auth {enable disable}	Enable/disable authentication (default = disable).
auth-type {certificate psk}	Select the SMTP authentication type (default = psk): <ul style="list-style-type: none">certificate: Use local certificate to authenticate.psk: Use username and password to authenticate.

Variable	Description
local-cert {Fortinet_Local Fortinet_Local2}	Choose from the two available local certificates. This variable is available only when the <code>auth-type</code> is <code>certificate</code> .
passwd <passwd>	Enter the SMTP account password value (character limit = 63). This variable is available only when the <code>auth-type</code> is <code>psk</code> .
port <integer>	Enter the SMTP server port (1 - 65535, default = 25).
secure-option {default none smtps starttls}	Select the communication secure option: <ul style="list-style-type: none"> <code>default</code>: Try STARTTLS, proceed as plain text communication otherwise (default). <code>none</code>: Communication will be in plain text format. <code>smtps</code>: Communication will be protected by SMTPS. <code>starttls</code>: Communication will be protected by STARTTLS.
server <string>	Enter the SMTP server name.
user <string>	Enter the SMTP account user name. This variable is available only when the <code>auth-type</code> is <code>psk</code> .

metadata

Use this command to add additional information fields to the administrator accounts of your FortiManager unit.



This command creates the metadata fields. Use `config system admin user` to add data to the metadata fields.

Syntax

```
config system metadata admins
edit <fieldname>
set field_length {20 | 50 | 255}
set importance {optional | required}
set status {enabled | disabled}
end
```

Variable	Description
<fieldname>	Enter the name of the field.
field_length {20 50 255}	Select the maximum number of characters allowed in this field (default = 50).
importance {optional required}	Select if this field is required or optional when entering standard information (default = required).
status {enabled disabled}	Enable/disable the metadata (default = enabled).

ntp

Use this command to configure automatic time setting using a network time protocol (NTP) server.

Syntax

```
config system ntp
  set status {enable | disable}
  set sync_interval <string>
  config ntpserver
    edit <id>
      set ntpv3 {enable | disable}
      set authentication {enable | disable}
      set key <passwd>
      set key-id <integer>
      set server <string>
    end
  end
```

Variable	Description
status {enable disable}	Enable/disable NTP time setting (default = disable).
sync_interval <string>	Enter how often the FortiManager unit synchronizes its time with the NTP server, in minutes (1 - 1440, default = 60).
Variables for config ntpserver subcommand:	
<id>	Time server ID.
ntpv3 {enable disable}	Enable/disable NTPv3 (default = disable).
authentication {enable disable}	Enable/disable MD5 authentication (default = disable).
key <passwd>	The authentication key (character limit = 63).
key-id <integer>	The key ID for authentication (default = 0).
server <string>	Enter the IPv4 or IPv6 address or fully qualified domain name of the NTP server.

password-policy

Use this command to configure access password policies.

Syntax

```
config system password-policy
  set status {enable | disable}
  set minimum-length <integer>
  set must-contain {lower-case-letter non-alphanumeric number upper-case-letter}
  set change-4-characters {enable | disable}
  set expire <integer>
end
```

Variable	Description
status {enable disable}	Enable/disable the password policy (default = disable).
minimum-length <integer>	Set the password's minimum length (8 - 256, default = 8).
must-contain {lower-case-letter non-alphanumeric number upper- case-letter}	Characters that a password must contain. <ul style="list-style-type: none"> lower-case-letter: the password must contain at least one lower case letter non-alphanumeric: the password must contain at least one non-alphanumeric characters number: the password must contain at least one number upper-case-letter: the password must contain at least one upper case letter.
change-4-characters {enable disable}	Enable/disable changing at least 4 characters for a new password (default = disable).
expire <integer>	Set the number of days after which admin users' passwords will expire (0 - 3650, 0 = never, default = 0).

report

Use the following command to configure report related settings.

report auto-cache

Use this command to view or configure report auto-cache settings.

Syntax

```
config system report auto-cache
    set aggressive-schedule {enable | disable}
    set order {latest-first | oldest-first}
    set status {enable | disable}
end
```

Variable	Description
aggressive-schedule {enable disable}	Enable/disable auto-cache on schedule reports aggressively (default = disable).
order {latest-first oldest-first}	The order of which SQL log table is processed first: <ul style="list-style-type: none"> latest-first: The newest SQL log table is processed first. oldest-first: The oldest SQL log table is processed first (default).
status {enable disable}	Enable/disable the SQL report auto-cache (default = enable).

report est-browse-time

Use this command to view or configure report settings.

Syntax

```
config system report est-browse-time
    set max-read-time <integer>
    set status {enable | disable}
end
```

Variable	Description
max-read-time <integer>	Set the read time threshold for each page view (1 - 3600, default = 180).
status {enable disable}	Enable/disable estimating browse time (default = enable).

report group

Use these commands to configure report groups.

Syntax

```
config system report group
    edit <group-id>
        set adom <adom-name>
        set case-insensitive {enable | disable}
        set report-like <string>
        config chart-alternative
            edit <chart-name>
                set chart-replace <string>
            end
        end
        config group-by
            edit <var-name>
                set var-expression <string>
                set var-type {enum | integer | ip | string}
            end
        end
    end
```

Variable	Description
<group-id>	The identification number of the group to be edited or created.
adom <adom-name>	The ADOM that contains the report group.
case-insensitive {enable disable}	Enable/disable case sensitivity (default = enable).
report-like <string>	Report pattern.
Variables for config chart-alternative subcommand:	
<chart-name>	The chart name.

Variable	Description
chart-replace <string>	Chart replacement.
Variables for <code>config group-by</code> subcommand:	
<var-name>	The variable name.
var-expression <string>	Variable expression.
var-type {enum integer ip string}	Variable type (default = string).

report setting

Use these commands to view or configure report settings.

Syntax

```

config system report setting
    set aggregate-report {enable | disable}
    set capwap-port <integer>
    set capwap-service <string>
    set exclude-capwap {by-port | by-service | disable}
    set hcache-lossless {enable | disable}
    set ldap-cache-timeout <integer>
    set max-table-rows <integer>
    set report-priority {auto | high | low}
    set template-auto-install {default | english}
    set week-start {mon | sun}
end

```

Variable	Description
aggregate-report {enable disable}	Enable/disable including a group report along with the per-device reports (default = disable).
capwap-port <integer>	Exclude capwap traffic by port (default = 5246).
capwap-service <string>	Exclude capwap traffic by service.
exclude-capwap {by-port by-service disable}	Exclude capwap traffic (default = by-port).
hcache-lossless {enable disable}	Enable/disable ready-with-loss hcaches (default = disable).
ldap-cache-timeout <integer>	Set the LDAP cache timeout in minutes (0 = do not use cache, default = 60).
max-table-rows <integer>	Set the maximum number of rows that can be generated in a single table (10000 - 100000, default = 10000).
report-priority {auto high low}	Set the Priority of the SQL report (default = auto).
template-auto-install {default english}	Set the language used for new ADOMs (default = default).

Variable	Description
week-start {mon sun}	Set the day that the week starts on, either <code>sun</code> (Sunday) or <code>mon</code> (Monday) (default = <code>sun</code>).

route

Use this command to view or configure static routing table entries on your FortiManager unit.

Syntax

```
config system route
edit <seq_int>
    set device <port>
    set dst <dst_ipv4mask>
    set gateway <gateway_ipv4_address>
end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <port>	Enter the port (interface) used for this route.
dst <dst_ipv4mask>	Enter the IPv4 address and mask for the destination network.
gateway <gateway_ipv4_address>	Enter the default gateway IPv4 address for this network.

route6

Use this command to view or configure static IPv6 routing table entries on your FortiManager unit.

Syntax

```
config system route6
edit <seq_int>
    set device <string>
    set dst <ipv6_prefix>
    set gateway <ipv6_address>
end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.

Variable	Description
device <string>	Enter the port (interface) used for this route.
dst <ipv6_prefix>	Enter the IPv6 address and mask for the destination network.
gateway <ipv6_address>	Enter the default gateway IPv6 address for this network.

saml

Use this command to configure global settings for SAML authentication.

Syntax

```

config system saml
  set acs-url
  set cert <certificate>
  set default-profile <string>
  set entity-id <string>
  set forticloud-sso {enable | disable}
  set idp-cert <string>
  set idp-entity-id <string>
  set idp-single-logout-url <string>
  set idp-single-sign-on-url <string>
  set login-auto-redirect {enable | disable}
  set role {FAB-SP | IDP | SP}
  set server-address <string>
  set sls-url
  set status {enable | disable}
  set user-auto-create {enable | disable}
  config service-providers
    edit <name>
      set idp-entity-id <string>
      set idp-single-logout-url <string>
      set idp-single-sign-on-url <string>
      set prefix <string>
      set sp-cert <string>
      set sp-entity-id <string>
      set sp-single-logout-url <string>
      set sp-single-sign-on-url <string>
    next
  end
  config fabric-idp
    edit <device-id>
      set idp-cert <string>
      set idp-entity-id <string>
      set idp-single-logout-url <string>
      set idp-single-sign-on-url <string>
      set idp-status {enable | disable}
    next
  end
end

```

Variable	Description
acs-url	
cert <certificate>	The certificate name.
default-profile <string>	The default profile (default = Restricted_User).
entity-id <string>	The entity ID.
forticloud-sso {enable disable}	Enable/disable FortiCloud SSO (default = disable).
idp-cert <string>	The IDP certificate name.
idp-entity-id <string>	The IDP entity ID.
idp-single-logout-url <string>	The IDP single logout URL.
idp-single-sign-on-url <string>	The IDP single sign-on URL.
login-auto-redirect {enable disable}	Enable/disable automatic redirect to the IDP login page (default = disable).
role {FAB-SP IDP SP}	The SAML role: <ul style="list-style-type: none"> • FAB-SP: Fabric service provider • IDP: Identity provider • SP: Service provider (default)
server-address <string>	The server address.
sls-url	
status {enable disable}	Enable/disable SAML authentication (default = disable).
user-auto-create {enable disable}	Enable/disable automatic user creation (default = disable).
Variables for <code>config service-providers</code> subcommand:	
This command is only available when <code>role</code> is IDP.	
<name>	Service provide name.
idp-entity-id <string>	The IDP entity ID.
idp-single-logout-url <string>	The IDP single logout URL.
idp-single-sign-on-url <string>	The IDP single sign-on URL.
prefix <string>	The prefix. Can contain only letters and numbers.
sp-cert <string>	The SP certificate name.
sp-entity-id <string>	The SP entity ID.
sp-single-logout-url <string>	The SP single sign-on URL.
sp-single-sign-on-url <string>	The SP single logout URL.
Variables for <code>config fabric-idp</code> subcommand:	
This command is only available when <code>role</code> is FAB-SP.	

Variable	Description
<device-id>	Device ID.
idp-cert <string>	The IDP certificate name.
idp-entity-id <string>	The IDP entity ID.
idp-single-logout-url <string>	The IDP single logout URL.
idp-single-sign-on-url <string>	The IDP single sign-on URL.
idp-status {enable disable}	Enable/disable SAML authentication (default = disable).

To view the service provider IdP information, use the following commands:

```
config system saml
config service-providers
edit <name>
get
```

Output:

```
name : name prefix : y9jr06vq0k sp-cert : (null) sp-entity-id :
http://https://172.27.2.225//metadata/ sp-single-sign-on-url:
https://https://172.27.2.225//saml/?acs sp-single-logout-url:
https://https://172.27.2.225//saml/?sls idp-entity-id : http://172.27.2.225/saml-
idp/y9jr06vq0k/metadata/ idp-single-sign-on-url: https://172.27.2.225/saml-
idp/y9jr06vq0k/login/ idp-single-logout-url: https://172.27.2.225/saml-
idp/y9jr06vq0k/logout/
```

sniffer

Configure packet sniffing.

Syntax

```
config system sniffer
edit <id>
set host <string>
set interface <interface>
set ipv6 {enable | disable}
set max-packet-count <integer>
set non-ip {enable | disable}
set port <string>
set protocol <string>
set vlan <string>
next
end
```

Variable	Description
<id>	Sniffer ID.

Variable	Description
host <string>	IP addresses of the hosts to filter for in sniffer traffic. Multiple individual IP addresses and ranges of addresses can be entered.
interface <interface>	The interface to sniff.
ipv6 {enable disable}	Enable/disable sniffing IPv6 packets.
max-packet-count <integer>	The maximum packet count (1 - 1000000, default - 4000).
non-ip {enable disable}	Enable/disable sniffing non-IP packets.
port <string>	The ports to sniff. Individual ports or port ranges can be entered.
protocol <string>	Integer value for the protocol type as defined by IANA (0 - 255).
vlan <string>	The VLANs to sniff.

snmp

Use the following commands to configure SNMP related settings.

snmp community

Use this command to configure SNMP communities on your FortiManager unit.

You add SNMP communities so that SNMP managers, typically applications running on computers to monitor SNMP status information, can connect to the FortiManager unit (the SNMP agent) to view system information and receive SNMP traps. SNMP traps are triggered when system events happen such as when there is a system restart, or when the log disk is almost full.

You can add up to three SNMP communities, and each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiManager unit for a different set of events.

Hosts are the SNMP managers that make up this SNMP community. Host information includes the IPv4 address and interface that connects it to the FortiManager unit.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).



Part of configuring an SNMP manager is to list it as a host in a community on the FortiManager unit that it will be monitoring. Otherwise that SNMP manager will not receive any traps or events from the FortiManager unit, and will be unable to query the FortiAnalyzer unit as well.

Syntax

```
config system snmp community
edit <index_number>
    set events <events_list>
    set name <community_name>
    set query-vl-port <integer>
```

```

set query-v1-status {enable | disable}
set query-v2c-port <integer>
set query-v2c-status {enable | disable}
set status {enable | disable}
set trap-v1-rport <integer>
set trap-v1-status {enable | disable}
set trap-v2c-rport <integer>
set trap-v2c-status {enable | disable}
config hosts
    edit <host_number>
        set interface <interface_name>
        set ip <ipv4_address>
    next
config hosts6
    edit <host_number>
        set interface <interface_name>
        set ip <ipv6_address>
    end
end

```

Variable	Description
<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.
events <events_list>	<p>Enable the events for which the FortiManager unit should send traps to the SNMP managers in this community (default = All events enabled). The <code>raid_changed</code> event is only available for devices that support RAID.</p> <ul style="list-style-type: none"> • <code>cpu-high-exclude-nice</code>: CPU usage exclude NICE threshold. • <code>cpu_high</code>: CPU usage too high. • <code>disk_low</code>: Disk usage too high. • <code>ha_switch</code>: HA switch. • <code>intf_ip_chg</code>: Interface IP address changed. • <code>lic-dev-quota</code>: High licensed device quota detected. • <code>lic-gbday</code>: High licensed log GB/day detected. • <code>log-alert</code>: Log base alert message. • <code>log-data-rate</code>: High incoming log data rate detected. • <code>log-rate</code>: High incoming log rate detected. • <code>mem_low</code>: Available memory is low. • <code>raid_changed</code>: RAID status changed. • <code>sys_reboot</code>: System reboot.
name <community_name>	<p>Enter the name of the SNMP community. Names can be used to distinguish between the roles of the hosts in the groups.</p> <p>For example the Logging and Reporting group would be interested in the <code>disk_low</code> events, but likely not the other events.</p> <p>The name is included in SNMPv2c trap packets to the SNMP manager, and is also present in query packets from, the SNMP manager.</p>
query-v1-port <integer>	Enter the SNMPv1 query port number used when SNMP managers query the FortiManager unit (1 - 65535, default = 161).
query-v1-status {enable disable}	Enable/disable SNMPv1 queries for this SNMP community (default = enable).

Variable	Description
query-v2c-port <integer>	Enter the SNMP v2c query port number used when SNMP managers query the FortiManager unit. SNMP v2c queries will include the name of the community (1 - 65535, default = 161).
query-v2c-status {enable disable}	Enable/disable SNMPv2c queries for this SNMP community (default = enable).
status {enable disable}	Enable/disable this SNMP community (default = enable).
trap-v1-rport <integer>	Enter the SNMPv1 remote port number used for sending traps to the SNMP managers (1 - 65535, default = 162).
trap-v1-status {enable disable}	Enable/disable SNMPv1 traps for this SNMP community (default = enable).
trap-v2c-rport <integer>	Enter the SNMPv2c remote port number used for sending traps to the SNMP managers (1 - 65535, default = 162).
trap-v2c-status {enable disable}	Enable/disable SNMPv2c traps for this SNMP community. SNMP v2c traps sent out to SNMP managers include the community name (default = enable).
Variables for <code>config hosts</code> subcommand:	
<host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <interface_name>	Enter the name of the FortiManager unit that connects to the SNMP manager (default = any).
ip <ipv4_address>	Enter the IPv4 address of the SNMP manager.
Variables for <code>config hosts6</code> subcommand:	
<host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <interface_name>	Enter the name of the FortiManager unit that connects to the SNMP manager (default = any).
ip <ipv6_address>	Enter the IPv6 address of the SNMP manager.

Example

This example shows how to add a new SNMP community named `SNMP_Com1`. The default configuration can be used in most cases with only a few modifications. In the example below the community is added, given a name, and then because this community is for an SNMP manager that is SNMP v1 compatible, all v2c functionality is disabled. After the community is configured the SNMP manager, or host, is added. The SNMP manager IPv4 address is 192.168.20.34 and it connects to the FortiManager unit internal interface.

```
config system snmp community
  edit 1
    set name SNMP_Com1
    set query-v2c-status disable
    set trap-v2c-status disable
  config hosts
    edit 1
      set interface internal
      set ip 192.168.10.34/24
    end
  end
end
```

```
end
```

snmp sysinfo

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

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).

Syntax

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

Variable	Description
contact-info <string>	Add the contact information for the person responsible for this FortiManager unit (character limit = 255).
description <description>	Add a name or description of the FortiManager unit (character limit = 255).
engine-id <string>	Local SNMP engine ID string (character limit = 24).
location <location>	Describe the physical location of the FortiManager unit (character limit = 255).
status {enable disable}	Enable/disable the FortiManager SNMP agent (default = disable).
trap-cpu-high-exclude-nice-threshold <percentage>	SNMP trap for CPU usage threshold (excluding NICE processes), in percent (default = 80).
trap-high-cpu-threshold <percentage>	SNMP trap for CPU usage threshold, in percent (default = 80).
trap-low-memory-threshold <percentage>	SNMP trap for memory usage threshold, in percent (default = 80).

Example

This example shows how to enable the FortiManager SNMP agent and add basic SNMP information.

```
config system snmp sysinfo
  set status enable
  set contact-info 'System Admin ext 245'
  set description 'Internal network unit'
  set location 'Server Room A121'
end
```

snmp user

Use this command to configure SNMPv3 users on your FortiManager unit. To use SNMPv3, you will first need to enable the FortiManager SNMP agent. For more information, see [snmp sysinfo](#). There should be a corresponding configuration on the SNMP server in order to query to or receive traps from FortiManager.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).

Syntax

```
config system snmp user
  edit <name>
    set auth-proto {md5 | sha}
    set auth-pwd <passwd>
    set events <events_list>
    set notify-hosts <ipv4_address>
    set notify-hosts6 <ipv6_address>
    set priv-proto {aes | des}
    set priv-pwd <passwd>
    set queries {enable | disable}
    set query-port <integer>
    set security-level {auth-no-priv | auth-priv | no-auth-no-priv}
  end
end
```

Variable	Description
<name>	Enter a SNMPv3 user name to add, edit, or delete.
auth-proto {md5 sha}	Authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable: <ul style="list-style-type: none"> md5: HMAC-MD5-96 authentication protocol sha: HMAC-SHA-96 authentication protocol (default)
auth-pwd <passwd>	Password for the authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
events <events_list>	Enable the events for which the FortiManager unit should send traps to the SNMPv3 managers in this community (default = All events enabled). The <code>raid_changed</code> event is only available for devices which support RAID. <ul style="list-style-type: none"> cpu-high-exclude-nice: CPU usage exclude nice threshold. cpu_high: The CPU usage is too high. disk_low: The log disk is getting close to being full. ha_switch: A new unit has become the primary HA. intf_ip_chg: An interface IP address has changed. lic-dev-quota: High licensed device quota detected. lic-gbday: High licensed log GB/Day detected. log-alert: Log base alert message. log-data-rate: High incoming log data rate detected. log-rate: High incoming log rate detected. mem_low: The available memory is low. raid_changed: RAID status changed.

Variable	Description
	<ul style="list-style-type: none"> <code>sys_reboot</code>: The FortiManager unit has rebooted.
<code>notify-hosts <ipv4_address></code>	Hosts to send notifications (traps) to.
<code>notify-hosts6 <ipv6_address></code>	Hosts to send notifications (traps) to.
<code>priv-proto {aes des}</code>	Privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable: <ul style="list-style-type: none"> <code>aes</code>: CFB128-AES-128 symmetric encryption protocol (default) <code>des</code>: CBC-DES symmetric encryption protocol
<code>priv-pwd <passwd></code>	Password for the privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
<code>queries {enable disable}</code>	Enable/disable queries for this user (default = enable)
<code>query-port <integer></code>	SNMPv3 query port (1 - 65535, default = 161).
<code>security-level {auth-no-priv auth-priv no-auth-no-priv}</code>	Security level for message authentication and encryption: <ul style="list-style-type: none"> <code>auth-no-priv</code>: Message with authentication but no privacy (encryption). <code>auth-priv</code>: Message with authentication and privacy (encryption). <code>no-auth-no-priv</code>: Message with no authentication and no privacy (encryption) (default).

soc-fabric

Use this command to configure the SOC Fabric.

Syntax

```
config system soc-fabric
    set name <string>
    set port <integer>
    set psk <passwd>
    set role {member | supervisor}
    set secure-connection {enable | disable}
    set status {enable | disable}
    set supervisor <string>
end
```

Variable	Description
<code>name <string></code>	Enter the Fabric name.
<code>port <integer></code>	Set the communication port (1 - 65535, default = 6443).
<code>psk <passwd></code>	Enter the Fabric authentication password.
<code>role {member supervisor}</code>	Set the SOC Fabric role (default = member).

Variable	Description
secure-connection {enable disable}	Enable/disable SSL/TLS (default = enable).
status {enable disable}	Enable/disable SOC Fabric (default = disable).
supervisor <string>	Enter the IP/FQDN of the supervisor.

sql

Configure Structured Query Language (SQL) settings.

Syntax

```
config system sql
    set background-rebuild {enable | disable}
    set compress-table-min-age <integer>
    set database-name <string>
    set database-type <postgres>
    set device-count-high {enable | disable}
    set event-table-partition-time <integer>
    set fct-table-partition-time <integer>
    set logtype {none | app-ctrl | attack | content | dlp | emailfilter | event | generic
        | history | traffic | virus | voip | webfilter | netscan}
    set password <passwd>
    set prompt-sql-upgrade {enable | disable}
    set rebuild-event {enable | disable}
    set rebuild-event-start-time <hh:mm> <yyyy/mm/dd>
    set server <string>
    set start-time <hh>:<mm> <yyyy>/<mm>/<dd>
    set status {disable | local}
    set text-search-index {enable | disable}
    set traffic-table-partition-time <integer>
    set utm-table-partition-time <integer>
    set username <string>
config custom-index
    edit <id>
        set case-sensitive
        set device-type {FortiCache | FortiGate | FortiMail | FortiManager |
            FortiSandbox | FortiWeb}
        set index-field <Field-Name>
        set log-type <Log-Enter>
    next
end
config custom-skipidx
    edit <id>
        set device-type <device>
        set index-field <Field-Name>
        set log-type <Log-Enter>
    next
end
config ts-index-field
```

```

edit <category>
    set value <string>
next
end
end

```

Variable	Description
background-rebuild {enable disable}	Disable/enable rebuilding the SQL database in the background (default = enable).
compress-table-min-age <integer>	Minimum age in days for SQL tables to be compressed (0 - 10000, default = 7). Note: 0-day allows you to compress SQL tables with less than one-day of age.
database-name <string>	Remote SQL database name (character limit = 64). Command only available when <code>status</code> is set to <code>remote</code> .
database-type <postgres>	Database type (default = postgres). This command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> .
device-count-high {enable disable}	Enable/disable a high device count (default = disable). You must set to enable if the count of registered devices is greater than 8000: <ul style="list-style-type: none"> <code>disable</code>: Set to disable if device count is less than 8000. <code>enable</code>: Set to enable if device count is equal to or greater than 8000. Caution: Enabling or disabling this command will result in an SQL database rebuild. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. This operation will also result in a device reboot.
event-table-partition-time <integer>	Maximum SQL database table partitioning time range for event logs, in minutes (6 - 1440, 0 = unlimited, default = 0).
fct-table-partition-time <integer>	Maximum SQL database table partitioning time range for FortiClient logs, in minutes (12 - 1440, 0 = unlimited, default = 360).
logtype {none app-ctrl attack content dlp emailfilter event generic history traffic virus voip webfilter netscan}	Log type. This command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> .
password <passwd>	The password that the Fortinet unit will use to authenticate with the remote database. This command only available when <code>status</code> is set to <code>remote</code> .
prompt-sql-upgrade {enable disable}	Prompt to convert log database into SQL database at start time on GUI (default = enable).
rebuild-event {enable disable}	Enable/disable a rebuild event during SQL database rebuilding (default = enable).
rebuild-event-start-time <hh:mm> <yyyy/mm/dd>	The rebuild event starting date and time (default = 00:00 2000/01/01).
server <string>	Set the database ip or hostname.
start-time <hh>:<mm> <yyyy>/<mm>/<dd>	Start date and time <hh:mm yyyy/mm/dd>. Command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> .
status {disable local}	SQL database status:

Variable	Description
	<ul style="list-style-type: none"> <code>disable</code>: Disable SQL database. <code>local</code>: Enable local database (default).
<code>text-search-index {enable disable}</code>	Enable/disable the creation of a text search index (default = disable).
<code>traffic-table-partition-time <integer></code>	Maximum SQL database table partitioning time range for traffic logs (1 - 1440, 0 = unlimited, default = 0).
<code>utm-table-partition-time <integer></code>	Maximum SQL database table partitioning time range in minutes for UTM logs (1 - 1440, 0 = unlimited, default = 0).
<code>username <string></code>	The user name that the unit will use to authenticate with the remote database (character limit = 64).
Variables for <code>config custom-index</code> subcommand:	
<code>case-sensitive</code>	Enable/disable case sensitivity.
<code>device-type {FortiAuthenticator FortiCache FortiClient FortiDDoS FortiGate FortiMail FortiManager FortiSandbox FortiWeb}</code>	Set the device type (default = FortiGate).
<code>index-field <Field-Name></code>	Enter a valid field name. Select one of the available field names. The available options for <code>index-field</code> is dependent on the <code>device-type</code> entry.
<code>log-type <Log-Enter></code>	Enter the log type. The available options for <code>log-type</code> is dependent on the <code>device-type</code> entry.
Variables for <code>config custom-skipidx</code> subcommand:	
List of additional SQL skip index fields.	
<code>device-type <device></code>	Set the device type (default = FortiGate).
<code>index-field <Field-Name></code>	Enter a valid field name. Select one of the available field names. The available options depend on the <code>device-type</code> .
<code>log-type <Log-Enter></code>	Enter the log type (default = traffic). The available options depend on the <code>device-type</code> .

Variable	Description
Variables for <code>config ts-index-field</code> subcommand:	
<category>	Category of the text search index fields. The following is the list of categories and their default fields.
Category	Value
FGT-app-ctrl	user,group,srcip,dstip,dstport,service,app,action,hostname
FGT-attack	severity,srcip,dstip,action,user,attack
FGT-content	from,to,subject,action,srcip,dstip,hostname,status
FGT-dlp	user,srcip,service,action,filename
FGT-emailfilter	user,srcip,from,to,subject
FGT-event	subtype,ui,action,msg
FGT-traffic	user,srcip,dstip,service,app,utmaction
FGT-virus	service,srcip,dstip,action,filename,virus,user
FGT-voip	action,user,src,dst,from,to
FGT-webfilter	user,srcip,dstip,service,action,catdesc,hostname
FGT-netscan	user,dstip,vuln,severity,os
FGT-fct-event	(null)
FGT-fct-traffic	(null)
FGT-fct-netscan	(null)
FGT-waf	user,srcip,dstip,service,action
FGT-gtp	msisdn,from,to,status
FGT-dns	(null)
FGT-ssh	login,srcip,dstip,direction,action
FML-emailfilter	client_name,dst_ip,from,to,subject
FML-event	subtype,msg
FML-history	classifier,disposition,from,to,client_name,direction,domain,virus
FML-virus	src,msg,from,to
FWB-attack	http_host,http_url,src,dst,msg,action
FWB-event	ui,action,msg
FWB-traffic	src,dst,service,http_method,msg

Variable	Description
value <string>	Fields of the text search filter. Enter one or more field names separated with a comma.

syslog

Use this command to configure syslog servers.

Syntax

```
config system syslog
  edit <name>
    set ip <string>
    set port <integer>
  end
end
```

Variable	Description
<name>	Syslog server name.
ip <string>	Enter the syslog server IPv4 address or hostname.
port <integer>	Enter the syslog server port (1 - 65535, default = 514).

workflow approval-matrix

Use this command to configure workflow settings.

Syntax

```
config system workflow approval-matrix
  edit <ADOM_name>
    set mail-server <string>
    set notify <string>
    config approver
      edit <sequence_number>
        set member <string>
      end
    end
end
```

Variable	Description
<ADOM_name>	The name of the ADOM.
mail-server <string>	Enter the mail server IPv4 address or hostname.

Variable	Description
notify <string>	Enter the notified users. Use a comma as a separator.
Variables for <code>config approver</code> subcommand:	
<sequence_number>	Enter the entry number.
member <string>	Enter the members of the approval group. Use a comma as a separator.

Example

This example shows configuring the `admin` administrator as an approver for the `root` ADOM.

```
config system workflow approval-matrix
  edit "root"
    config approver
      edit 1
        set member "admin"
      next
    end
    set mail-server "mail.fortinet.com"
    set notify "admin"
  end
```

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiManager unit's built-in FDS.



CLI commands and variables are case sensitive.

analyzer virusreport	fds-setting	server-override-status
av-ips	fwm-setting	service
custom-url-list	multilayer	web-spam
disk-quota	publicnetwork	
fct-services	server-access-priorities	



TCP port numbers cannot be used by multiple services at the same time with the same IP address. If a port is already in use, it cannot be assigned to another service. For example, HTTPS and HTTP cannot have the same port number.

analyzer virusreport

Use this command to enable or disable notification of virus detection to FortiGuard.

Syntax

```
config fmupdate analyzer virusreport
  set status {enable | disable}
end
```

Variable	Description
<code>status {enable disable}</code>	Enable/disable sending virus detection notification to FortiGuard (default = enable).

Example

This example enables virus detection notifications to FortiGuard.

```
config fmupdate analyzer virusreport
  set status enable
end
```

av-ips

Use the following commands to configure antivirus and IPS related settings.

av-ips advanced-log

Use this command to enable logging of FortiGuard antivirus and IPS update packages received by the FortiManager unit's built-in FDS from the external FDS.

Syntax

```
config fmupdate av-ips advanced-log
  set log-fortigate {enable | disable}
  set log-server {enable | disable}
end
```

Variable	Description
log-fortigate {enable disable}	Enable/disable logging of FortiGuard antivirus and IPS service updates of FortiGate devices (default = disable).
log-server {enable disable}	Enable/disable logging of update packages received by the built-in FDS server (default = enable).

Example

You could enable logging of FortiGuard antivirus updates to FortiClient installations and update packages downloaded by the built-in FDS from the FDS.

```
config fmupdate av-ips advanced-log
  set log-forticlient enable
  set log-server enable
end
```

av-ips web-proxy

Use this command to configure a web proxy if FortiGuard antivirus and IPS updates must be retrieved through a web proxy.

Syntax

```
config fmupdate av-ips web-proxy
  set address <string>
  set mode {proxy | tunnel}
  set password <passwd>
  set port <integer>
  set status {enable | disable}
  set username <string>
```

end

Variable	Description
address <string>	Enter the web proxy address.
mode {proxy tunnel}	Enter the web proxy mode (default = tunnel).
password <passwd>	If the web proxy requires authentication, enter the password for the user name (character limit = 63).
port <integer>	Enter the port number of the web proxy (1 - 65535, default = 80).
status {enable disable}	Enable/disable connections through the web proxy (default = disable).
username <string>	If the web proxy requires authentication, enter the user name (character limit = 63).

Example

You could enable a connection through a non-transparent web proxy on an alternate port.

```
config fmupdate av-ips web-proxy
  set status enable
  set mode proxy
  set address 10.10.30.1
  set port 8890
  set username avipsupdater
  set password cvhk3rf3u9jvsYU
end
```

custom-url-list

Use this command to configure the URL database for rating and filtering. You can select to use the FortiGuard URL database, a custom URL database, or both. When selecting to use a custom URL database, use the `fmupdate {ftp | scp | tftp} import` command to import the custom URL list. When FortiManager performs the URL rating, it will check the custom URL first. If a match is found, the custom rating is returned. If there is no match, then FortiManager will check the FortiGuard database.

Syntax

```
config fmupdate custom-url-list
  set db_selection {both | custom-url | fortiguard-db}
end
```

Variable	Description
db_selection {both custom-url fortiguard-db}	Manage the FortiGuard URL database: <ul style="list-style-type: none"> <code>both</code>: Support both custom URL database and the FortiGuard database (default) <code>custom-url</code>: Customer imported URL list. <code>fortiguard-db</code>: Fortinet's FortiGuard database

disk-quota

Use this command to configure the disk space available for use by the Upgrade Manager.

If the Upgrade Manager disk space is full or if there is insufficient space to save an update package to disk, the package will not download and an alert will be sent to notify you.

Syntax

```
config fmupdate disk-quota
  set value <size_int>
end
```

Variable	Description
value <size_int>	Configure the size of the Upgrade Manager disk quota, in megabytes (default = 51200). If you set the disk-quota smaller than the size of an update package, the update package will not download and you will get a disk full alert.

fct-services

Use this command to configure the built-in FDS to provide FortiGuard services to FortiClient installations.

Syntax

```
config fmupdate fct-services
  set status {enable | disable}
  set port <integer>
end
```

Variable	Description
status {enable disable}	Enable/disable built-in FDS service to FortiClient installations (default = enable).
port <integer>	Enter the port number on which the built-in FDS should provide updates to FortiClient installations (1 - 65535, default = 80).

Example

You could configure the built-in FDS to accommodate older versions of FortiClient installations by providing service on their required port.

```
config fmupdate fct-services
  set status enable
  set port 80
end
```

fds-setting

Use this command to set FDS settings.

Syntax

```
config fmupdate fds-setting
  set fds-clt-ssl-protocol {ssl3 | tls1.0 | tls1.1 | tls1.2}
  set fds-ssl-protocol {ssl3 | tls1.0 | tls1.1 | tls1.2}
  set fmtr-log {alert | critical | debug | disable | emergency | error | info | notice |
    warn}
  set fortiguard-anycast {enable | disable}
  set fortiguard-anycast-source {aws | fortinet}
  set linkd-log {alert | critical | debug | disable | emergency | error | info | notice
    | warn}
  set max-av-ips-version <integer>
  set max-work <integer>
  set send_report {enable | disable}
  set send_setup {enable | disable}
  set system-support-fct {5.4 5.6 6.0 6.2 | disable | emergency}
  set system-support-fdc 3.x
  set system-support-fgt {5.4 5.6 6.0 6.2}
  set system-support-fml {4.x 5.x 6.x}
  set system-support-fsa {1.x 2.x 3.x}
  set system-support-fts 4.x
  set umsvc-log {alert | critical | debug | disable | emergency | error | info | notice
    | warn}
  set unreg-dev-option {add-service | ignore | svc-only}
  set User-Agent <text>
  set wanip-query-mode {disable | ipify}
end
```

Variable	Description
fds-clt-ssl-protocol {ssl3 tls1.0 tls1.1 tls1.2}	Set the SSL protocols version for connecting FDS server (default = tls1.2).
fds-ssl-protocol {ssl3 tls1.0 tls1.1 tls1.2}	Set the SSL protocols version for FDS service (default = tls1.0).
fmtr-log {alert critical debug disable emergency error info notice warn}	The fmtr log level. Set to <code>disable</code> to disable the log (default = info).
fortiguard-anycast {enable disable}	Enable/disable use of FortiGuard's anycast network (default = disable).
fortiguard-anycast-source {aws fortinet}	Configure which servers provide FortiGuard services in FortiGuard's anycast network (default = fortinet).
linkd-log {alert critical debug disable emergency error info notice warn}	The linkd log level (default = info).

Variable	Description
max-av-ips-version <integer>	The maximum number of AV/IPS full version downloadable packages (default = 20).
max-work <integer>	The maximum number of worker processing downlink requests (default = 1).
send_report {enable disable}	Enable/disable sending reports to the FDS server (default = enable).
send_setup {enable disable}	Enable/disable sending setup to the FDS server (default = disable).
system-support-fct {5.4 5.6 6.0 6.2 disable emergency}	Set the FortiClient support version, disable the linkd log, or set the log level to emergency (default = emergency).
system-support-fdc 3.x	Set the FortiDeceptor support version.
system-support-fgt {5.4 5.6 6.0 6.2}	Set the FortiGate support version.
system-support-fml {4.x 5.x 6.x}	Set the FortiMail support version.
system-support-fsa {1.x 2.x 3.x}	Set the FortiSandbox support version.
system-support-fts 4.x	Set the FortiTester support version.
umsvc-log {alert critical debug disable emergency error info notice warn}	The um_service log level (default = info).
unreg-dev-option {add-service ignore svc-only}	Set the option for unregistered devices: <ul style="list-style-type: none"> • add-service: Add unregistered devices and allow update request (default). • ignore: Ignore all unregistered devices. • svc-only: Allow update request without add unregistered device.
User-Agent <text>	Configure the User-Agent string.
wanip-query-mode {disable ipify}	Set the public IP query mode. <ul style="list-style-type: none"> • disable: Do not query public IP (default) • ipify: Get public IP through https://api.ipify.org

fds-setting push-override

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDS sends FortiGuard antivirus and IPS push messages.

This is useful if push notifications must be sent to an IP address and/or port other than the FortiManager unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiManager unit.

Syntax

```
config fmupdate fds-setting
config push-override
set ip <ipv_address>
set port <integer>
```

```
        set status {enable | disable}
    end
end
```

Variable	Description
ip <ipv_address>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiManager unit.
port <integer>	Enter the receiving port number on the NAT device (1 - 65535, default = 9443).
status {enable disable}	Enable/disable the push updates (default = disable).

Example

You could enable the FortiManager unit's built-in FDS to receive push messages.

If there is a NAT device or firewall between the FortiManager unit and the FDS, you could also notify the FDS to send push messages to the external IP address of the NAT device, instead of the FortiManager unit's private network IP address.

```
config fmupdate fds-setting
    config push-override
        set status enable
        set ip 172.16.124.135
        set port 9000
    end
end
```

You would then configure port forwarding on the NAT device, forwarding push messages received on User Datagram Protocol (UDP) port 9000 to the FortiManager unit on UDP port 9443.

fds-setting push-override-to-client

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDS sends FortiGuard antivirus and IPS push messages.

This command is useful if push notifications must be sent to an IP address and/or port other than the FortiManager unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiManager unit.

Syntax

```
config fmupdate fds-setting
    config push-override-to-client
        set status {enable | disable}
        config <announce-ip>
            edit <id>
                set ip <ip_address>
                set port <integer>
            end
        end
    end
end
```

Variable	Description
status {enable disable}	Enable/disable the push updates (default = disable).
Variables for <code>config announce-ip</code> subcommand:	
<id>	Edit the announce IP address ID (1 - 10).
ip <ip_address>	Enter the announce IP address.
port <integer>	Enter the announce IP port (1 - 65535, default = 8890).

fds-setting server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard spam updates.

Syntax

```
config fmupdate fds-setting
  config server-override
    set status {enable | disable}
    config servlist
      edit <id>
        set ip <ipv4_address>
        set ip6 <ipv6_address>
        set port <integer>
        set server-type {fct | fds}
      end
    end
  end
```

Variable	Description
status {enable disable}	Enable/disable the override (default = disable).
Variable for <code>config servlist</code> subcommand:	
<id>	Enter the override server ID (1 - 10).
ip <ipv4_address>	Enter the IPv4 address of the override server address.
ip6 <ipv6_address>	Enter the IPv6 address of the override server address.
port <integer>	Enter the port number to use when contacting the FDS (1 - 65535, default = 443).
server-type {fct fds}	Set the override server type (default = fds).

fds-setting update-schedule

Use this command to schedule when the built-in FortiGuard retrieves antivirus and IPS updates.

Syntax

```
config fmupdate fds-setting
  config update-schedule
    set day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}
    set frequency {every | daily | weekly}
    set status {enable | disable}
    set time <hh:mm>
  end
end
```

Variable	Description
day {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}	The day that the update will occur (Sunday - Saturday, default = Monday). This option is only available if the update frequency is <code>weekly</code> .
frequency {every daily weekly}	The update frequency: every given time interval, once a day, or once a week (default = <code>every</code>).
status {enable disable}	Enable/disable scheduled updates (default = <code>enable</code>).
time <hh:mm>	The time interval between updates, or the hour and minute when the update occurs (hh: 0 - 23, mm: 0 - 59 or 60 = random, default = 00:10).

fwm-setting

Use this command to configure firmware management settings.

Syntax

```
config fmupdate fwm-setting
  set auto-scan-fgt-disk {enable | disable}
  set check-fgt-disk {enable | disable}
  set fds-failover-fmg {enable | disable}
  set fds-image-timeout <integer>
  set immx-source {cloud | fgt | fmg}
  set log {fwm | fwm_dm | fwm_dm_json}
  set multiple-steps-interval <integer>
end
```

Variable	Description
auto-scan-fgt-disk {enable disable}	Enable/disable automatic scanning of a FortiGate disk when required (default = <code>enable</code>).
check-fgt-disk {enable disable}	Enable/disable checking a FortiGate disk prior to upgrading the image (default = <code>enable</code>).

Variable	Description
fds-failover-fmg {enable disable}	Enable/disable using the a local image file on the FortiManager when the FDS download fails (default = enable).
fds-image-timeout <integer>	Set the timer for FortiGate image downloads from FortiGuard, in seconds (300 - 3600, default = 1800).
immx-source {cloud fgt fmg}	Configure which of the IMMX file to be used for choosing the upgrade patch: <ul style="list-style-type: none"> cloud: Use the IMMX file for FortiCloud. fgt: Use the IMMX file for FortiGate. fmg: Use the IMMX file for FortiManager. The default file is the one for FortiManager (default = fmg).
log {fwm fwm_dm fwm_dm_json}	Configure log setting for the firmware manager daemon (default = fwm_dm): <ul style="list-style-type: none"> fwm: Firmware Manager daemon log. fwm_dm: Firmware Manager and deployment service log. fwm_dm_json: Firmware Manager and Deployment service log with JSON data between FortiManager-FortiGate.
multiple-steps-interval <integer>	Set the waiting time between multiple step upgrades, in seconds (30 - 180, default = 60).

multilayer

Use this command to set multilayer mode configuration.

Syntax

```
config fmupdate multilayer
    set webspam-rating {enable | disable}
end
```

Variable	Description
webspam-rating {enable disable}	Enable/disable URL/antispam rating service (default = enable).

publicnetwork

Use this command to enable access to the public FDS. If this function is disabled, the service packages, updates, and license upgrades must be imported manually.

Syntax

```
config fmupdate publicnetwork
```

```

    set status {enable | disable}
end

```

Variable	Description
status {enable disable}	Enable/disable the public network (default = enable).

server-access-priorities

Use this command to configure how a FortiGate unit may download antivirus updates and request web filtering services from multiple FortiManager units and private FDS servers.

Use the `private-server` subcommand to configure multiple FortiManager units and private servers.



By default, the FortiGate unit receives updates from the FortiManager unit if the FortiGate unit is managed by the FortiManager unit and the FortiGate unit was configured to receive updates from the FortiManager unit.

Syntax

```

config fmupdate server-access-priorities
    set access-public {enable | disable}
    set av-ips {enable | disable}
    set web-spam {enable | disable}
    config private-server
        edit <id>
            set ip <ipv4_address>
            set ip6 <ipv6_address>
            set time_zone <integer>
        end
    end
end

```

Variable	Description
access-public {enable disable}	Enable/disable allowing FortiGates to access public FortiGuard servers when private servers are unavailable (default = disable).
av-ips {enable disable}	Enable/disable receiving antivirus and IPS update service for private servers (default = disable).
web-spam {enable disable}	Enable/disable Web Filter and Email Filter update service for private servers (default = enable).

Variables for `config private-server` subcommand:

<id>	Enter a number to identify the FortiManager unit or private server (1 - 10).
ip <ipv4_address>	Enter the IPv4 address of the FortiManager unit or private server.
ip6 <ipv6_address>	Enter the IPv6 address of the FortiManager unit or private server.
time_zone <integer>	Enter the correct time zone of the private server (-24 = local time zone, default = -24).

Example

The following example configures access to public FDS servers and allows FortiGate units to receive antivirus updates from other FortiManager units and private FDS servers. This example also configures three private servers.

```
config fmupdate server-access-priorities
  set access-public enable
  set av-ips enable
  config private-server
    edit 1
      set ip 172.16.130.252
    next
    edit 2
      set ip 172.31.145.201
    next
    edit 3
      set ip 172.27.122.99
    end
  end
end
```

server-override-status

Configure strict or loose server override.

Syntax

```
config fmupdate server-override-status
  set mode {loose | strict}
end
```

Variable	Description
mode {loose strict}	Set the server override mode: <ul style="list-style-type: none">loose: Allow access other servers (default).strict: Access override server only.

service

Use this command to enable or disable the services provided by the built-in FDS.

Syntax

```
config fmupdate service
  set avips {enable | disable}
  set query-antispam {enable | disable}
  set query-antivirus {enable | disable}
  set query-filequery {enable | disable}
```

```

set query-iot {enable | disable}
set query-outbreak-prevention {enable | disable}
set query-webfilter {enable | disable}
set webfilter-https-traversal {enable | disable}
end

```

Variable	Description
avips {enable disable}	Enable/disable the built-in FortiGuard to provide FortiGuard antivirus and IPS updates (default = enable).
query-antispam {enable disable}	Enable/disable antispam service (default = disable).
query-antivirus {enable disable}	Enable/disable antivirus service (default = disable).
query-filequery {enable disable}	Enable/disable file query service (default = disable).
query-iot {enable disable}	Enable/disable file query service (default = disable).
query-outbreak-prevention {enable disable}	Enable/disable outbreak prevention query service (default = disable).
query-webfilter {enable disable}	Enable/disable web filter service (default = disable).
webfilter-https-traversal {enable disable}	Enable/disable Web Filter HTTPS traversal (default = disable).

Example

```

config fmupdate service
    set avips enable
end

```

web-spam

Use the following commands to configure FortiGuard antispam related settings.

web-spam fgd-setting

Use this command to configure FortiGuard run parameters.

Syntax

```

config fmupdate web-spam fgd-setting
    set as-cache <integer>
    set as-log {all | disable | nospam}
    set as-preload {enable | disable}
    set av-cache <integer>
    set av-log {all | disable | novirus}
    set av-preload {enable | disable}
    set av2-cache <integer>
    set av2-log {all | disable | noav2}
end

```

```

set av2-preload {enable | disable}
set eventlog-query {enable | disable}
set fgd-pull-interval <integer>
set fq-cache <integer>
set fq-log {all | disable | nofilequery}
set fq-preload {enable | disable}
set iot-cache <integer>
set iot-log {all | disable | nofilequery}
set iot-preload {enable | disable}
set linkd-log {enable | disable}
set max-client-worker <integer>
set max-log-quota <integer>
set max-unrated-size <integer>
set restrict-as1-dbver <string>
set restrict-as2-dbver <string>
set restrict-as4-dbver <string>
set restrict-av-dbver <string>
set restrict-av2-dbver <string>
set restrict-fq-dbver <string>
set restrict-iots-dbver <string>
set restrict-wf-dbver <string>
set stat-log-interval <integer>
set stat-sync-interval <integer>
set update-interval <integer>
set update-log {enable | disable}
set wf-cache <integer>
set wf-dn-cache-expire-time <integer>
set wf-dn-cache-max-number <integer>
set wf-log {all | disable | nurl}
set wf-preload {enable | disable}
config server-override
    set status {enable | disable}
    config servlist
        edit <id>
            set ip <ipv4_address>
            set ip6 <ipv6_address>
            set port <integer>
            set service-type {fgc | fgd | fsa}
        end
    end
end

```

Variable	Description
as-cache <integer>	Antispam service maximum memory usage, in megabytes (maximum = physical memory-1024, 0 = no limit, default = 300).
as-log {all disable nospam}	Antispam log setting: <ul style="list-style-type: none"> all: Log all spam lookups. disable: Disable spam log. nosпам: Log non-spam events (default)
as-preload {enable disable}	Enable/disable preloading the antispam database into memory (default = disable).
av-cache <integer>	Antivirus service maximum memory usage, in megabytes (100 - 500, default = 300).

Variable	Description
av-log {all disable novirus}	Antivirus log setting: <ul style="list-style-type: none"> all: Log all virus lookups. disable: Disable virus log. novirus: Log non-virus events (default).
av-preload {enable disable}	Enable/disable preloading antivirus database to memory (default = disable).
av2-cache <integer>	Antispam service maximum memory usage, in megabytes (physical memory to 1024, 0 = no limit, default = 800).
av2-log {all disable novirus}	Outbreak prevention log setting: <ul style="list-style-type: none"> all: Log all av2 lookups. disable: Disable av2 logs. noav2: Log non-av2 events (default).
av2-preload {enable disable}	Enable/disable preloading outbreak prevention database to memory (default = disable).
eventlog-query {enable disable}	Enable/disable record query to event-log besides fgd-log (default = disable).
fgd-pull-interval <integer>	FortiGuard pull interval setting, in minutes (1 - 1440, default = 10).
fq-cache <integer>	File query service maximum memory usage, in megabytes (100 - 500, default = 300).
fq-log {all disable nofilequery}	Filequery log setting: <ul style="list-style-type: none"> all: Log all file query. disable: Disable file query log. nofilequery: Log non-file query events (default).
fq-preload {enable disable}	Enable/disable preloading the filequery database to memory (default = disable).
iot-cache <integer>	IoT service maximum memory usage, in megabytes (100 - 500, default = 300).
iot-log {all disable nofilequery}	IoT log setting (default = nofilequery).
iot-preload {enable disable}	Enable/disable preloading IoT database to memory (default = disable).
linkd-log {alert critical debug disable emergency error info notice warn}	Linkd log setting: <ul style="list-style-type: none"> alert: Immediate action is required. critical: Functionality is affected. debug: Debug information (default). disable: Linkd logging is disabled. emergency: The unit is unusable. error: Functionality is probably affected. info: General information. notice: Information about normal events. warn: Functionality might be affected.
max-client-worker <integer>	Maximum workers to use for TCP client connections (0 - 16, 0 = use CPU count, default = 0).
max-log-quota <integer>	Maximum log quota setting, in megabytes (100 - 20480, default = 6144).

Variable	Description
max-unrated-size <integer>	Maximum number of unrated site in memory, in kilobytes(10 - 5120, default = 500).
restrict-as1-dbver <string>	Restrict system update to indicated antispam(1) database version (character limit = 127).
restrict-as2-dbver <string>	Restrict system update to indicated antispam(2) database version (character limit = 127).
restrict-as4-dbver <string>	Restrict system update to indicated antispam(4) database version (character limit = 127).
restrict-av-dbver <string>	Restrict system update to indicated antivirus database version (character limit = 127).
restrict-av2-dbver <string>	Restrict system update to indicated outbreak prevention database version (character limit = 127).
restrict-fq-dbver <string>	Restrict system update to indicated file query database version (character limit = 127).
restrict-iots-dbver <string>	Restrict system update to indicated file query database version (character limit = 127).
restrict-wf-dbver <string>	Restrict system update to indicated web filter database version (character limit = 127).
stat-log-interval <integer>	Statistic log interval setting, in minutes (1 - 1440, default = 60).
stat-sync-interval <integer>	Synchronization interval for statistic of unrated site in minutes (1 - 60, default = 60).
update-interval <integer>	FortiGuard database update wait time if not enough delta files, in hours (2 - 24, default = 6).
update-log {enable disable}	Enable/disable update log setting (default = enable).
wf-cache <integer>	Web filter service maximum memory usage, in megabytes (maximum = physical memory-1024, 0 = no limit, default = 600).
wf-dn-cache-expire-time	Web filter DN cache expire time, in minutes (1 - 1440, 0 = never, default = 30).
wf-dn-cache-max-number	Maximum number of Web filter DN cache (0 = disable, default = 10000).
wf-log {all disable nouri}	Web filter log setting: <ul style="list-style-type: none"> all: Log all URL lookups. disable: Disable URL log. nouri: Log non-URL events (default).
wf-preload {enable disable}	Enable/disable preloading the web filter database into memory (default = disable).
Variables for <code>config server-override</code> subcommand:	
status {enable disable}	Enable/disable the override (default = disable).
<id>	Override server ID (1 - 10).
ip <ipv4_address>	IPv4 address of the override server.

Variable	Description
ip6 <ipv6_address>	IPv6 address of the override server.
port <integer>	Port number to use when contacting FortiGuard (1 - 65535, default = 443).
service-type {fgc fgd fsa}	Override service type.

web-spam web-proxy

Use this command to configure the web-spam web-proxy.

Syntax

```
config fmupdate web-spam web-proxy
  set address <string>
  set mode {proxy | tunnel}
  set password <passwd>
  set port <integer>
  set status {enable | disable}
end
```

Variable	Description
address <string>	Enter the web proxy address.
mode {proxy tunnel}	Enter the web proxy mode (default = tunnel).
password <passwd>	If the web proxy requires authentication, type the password for the user name.
port <integer>	Enter the port number of the web proxy (1- 65535, default = 80).
status {enable disable}	Enable/disable connections through the web proxy (default = disable).
username <string>	If the web proxy requires authentication, enter the user name.

execute

The `execute` commands perform immediate operations on the FortiManager unit. You can:

- Back up and restore the system settings, or reset the unit to factory settings.
- Set the unit date and time.
- Use ping to diagnose network problems.
- View the processes running on the FortiManager unit.
- Start and stop the FortiManager unit.
- Reset or shut down the FortiManager unit.



FortiManager CLI commands and variables are case sensitive.

add-on-license	fgfm reclaim-dev-tunnel	max-dev-licence	shutdown
add-vm-license	fmpolicy	migrate	sql-local
backup	fmprofile	ping	sql-query-dataset
bootimage	fmscript	ping6	sql-query-generic
certificate	fmupdate	raid	sql-report
chassis	format	reboot	ssh
console baudrate	iotop	remove	ssh-known-hosts
date	iotps	reset	tac
device	log	reset-sqllog-transfer	time
dmserver	log-fetch	restore	top
erasedisk	log-integrity	sdns	traceroute
factory-license	lvm	sensor	traceroute6

add-on-license

Use this command to load add-on licenses to support more devices with a license key.

Syntax

```
execute add-on-license <license>
```

Variable	Description
<license>	The add-on license string. Copy and paste the string from the license file. The license string must be enclosed with double quotes. Do not removed line breaks from the string.

add-vm-license

Add a VM license to the FortiManager.



This command is only available on FortiManager VM models.

Syntax

```
execute add-vm-license <vm_license>
```

Variable	Description
<vm_license>	The VM license string.

Example

The contents of the license file needs to be in quotes in order for it to work.

```
execute add-vm-license "-----BEGIN FMG VM LICENSE-----
QAAAAJ09s+LTe...ISJTTYPcKoDmMa6
-----END FAZ VM LICENSE-----"
```

backup

Use this command to backup the configuration or database to a file.

When you back up the unit settings from the vdom_admin account, the backup file contains global settings and the settings for each VDOM. When you back up the unit settings from a regular administrator account, the backup file contains the global settings and only the settings for the VDOM to which the administrator belongs.

Syntax

```
execute backup all-settings {ftp | scp | sftp} <ip:port> <string> <username> <passwd>
<ssh-cert> [crptpasswd] [force-docker]
execute backup logs <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
<directory> [vdlist]
```

```

execute backup logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
    <directory> [vdlist]
execute backup logs-rescue <device serial number(s)> {ftp | scp | sftp} <ip> <username>
    <passwd> <directory> [vdlist]
execute backup reports <report schedule name(s)> {ftp | scp | sftp} <ip> <username>
    <passwd> <directory> [vdlist]
execute backup reports-config <adom name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
    <directory> [vdlist]

```

Variable	Description
all-settings	Backup all FortiManager settings to a file on a server.
logs	Backup the device logs to a specified server.
logs-only	Backup device logs only to a specified server.
logs-rescue	Use this hidden command to backup logs regardless of DVM database for emergency reasons. This command will scan folders under /Storage/Logs/ for possible device logs to backup.
reports	Backup the reports to a specified server.
reports-config	Backup reports configuration to a specified server.
<device name(s)>	Enter the device name(s) separated by a comma, or enter <code>all</code> for all devices.
<device serial number(s)>	Enter the device serial number(s) separated by a comma, or enter <code>all</code> for all devices.
<report schedule name(s)>	Enter the report schedule name(s) separated by a comma, or enter <code>all</code> for all reports schedules.
<adom name(s)>	Enter the ADOM name(s) separated by a comma, or enter <code>all</code> for all ADOMs.
{ftp scp sftp}	Enter the server type: <code>ftp</code> , <code>scp</code> , or <code>sftp</code> .
<ip:port>	Enter the server IP address and optionally , for FTP servers, the port number.
<ip>	Enter the server IP address.
<string>	Enter the path and file name for the backup.
<username>	Enter username to use to log on the backup server.
<passwd>	Enter the password for the username on the backup server. Note: You cannot use <code>\\</code> in passwords.
<ssh-cert>	Enter the SSH certification for the server. This option is only available for backup operations to SCP servers.
[crptpasswd]	Optional password to protect backup content. Leave blank for no password.
<directory>	Enter the path to where the file will be backed up to on the backup server.
[vdlist]	List of VDOMs.
[force-docker]	Optional flag to stop when the docker backup fails.

Example

This example shows how to backup the FortiManager unit system settings to a file named `fmg.cfg` on a server at IP address 192.168.1.23 using the admin username, a password of 123456.

```
execute backup all-settings ftp 192.168.1.23 fmd.cfg admin 123456
Starting backup all settings...
Starting transfer the backup file to FTP server...
```

bootimage

Set the image from which the FortiManager unit will boot the next time it is restarted.



This command is only available on hardware-based FortiManager models.

Syntax

```
execute bootimage <primary | secondary>
```

Variable	Description
{primary secondary}	Select to boot from either the primary or secondary partition.

If you do not specify primary or secondary, the command will report whether it last booted from the primary or secondary boot image.

If your FortiManager unit does not have a secondary image, the bootimage command will inform you that option is not available.

To reboot your FortiManager unit, use:

```
execute reboot
```

certificate

Use these commands to manage certificates.

certificate ca

Use these commands to list CA certificates, and to import or export CA certificates.

Syntax

To list the CA certificates installed on the FortiManager unit:

```
execute certificate ca list
```

To export or import CA certificates:

```
execute certificate ca export <cert_name> <tftp_ip>
execute certificate ca import <filename> <tftp_ip> <cert_name>
```

Variable	Description
list	Generate a list of CA certificates on the FortiManager system.
<export>	Export CA certificate to TFTP server.
<import>	Import CA certificate from a TFTP server.
<cert_name>	Name of the certificate.
<tftp_ip>	IP address of the TFTP server.
<filename>	File name on the TFTP server.

certificate crl

Use this command to import CRL certificate from a TFTP server.

Syntax

```
execute certificate crl import <filename> <tftp_ip> <cert_name>
```

certificate local

Use these commands to list, import, or export local certificates, and to generate a certificate request

Syntax

```
execute certificate local export <cert_name> <tftp_ip>
execute certificate local import <filename> <tftp_ip> <cert_name>
execute certificate local import-pkcs12 {ftp | scp | sftp} <ip:port> <filename>
    <username> <password> <password> <name>
execute certificate local generate <certificate-name-string> <subject> <number>
    [<optional_information>]
execute certificate local list
```

Variable	Description
export <cert_name> <tftp_ip>	Export a certificate or request to a TFTP server. <ul style="list-style-type: none"> cert_name - Name of the certificate. tftp_ip - IP address of the TFTP server.
import <filename> <tftp_ip> <cert_name>	Import a signed certificate from a TFTP server.
import-pkcs12 {ftp scp sftp} <ip:port> <filename> <username> <password> <password> <name>	Import a certificate and private key from a PKCS#12 file. <ul style="list-style-type: none"> ftp, scp, sftp - The type of server the file will be imported from. ip:port - The server IP address and, optional, the port number. filename - The path and file name on the server. username - The user name on the server. password - The user password. password - The file password. name - The certificate name.
generate <certificate-name_str> <subject> <number> [<optional_information>]	Generate a certificate request. <ul style="list-style-type: none"> certificate-name-string - Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed. number - The size, in bits, of the encryption key, 512, 1024, 1536, or 2048. subject - Enter one of the following pieces of information to identify the FortiManager unit being certified: <ul style="list-style-type: none"> The FortiManager unit IP address The fully qualified domain name of the FortiManager unit An email address that identifies the FortiManager unit An IP address or domain name is preferable to an email address. optional_information - Enter optional_information as required to further identify the unit. See Optional information variables on page 147 for more information.
list	Generate a list of CA certificates and requests that are on the FortiManager system.

Optional information variables

You must enter the optional variables in the order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list.

For example, to enter the `organization_name_str`, you must first enter the `country_code_str`, `state_name_str`, and `city_name_str`.

While entering optional variables, you can type ? for help on the next required variable.

Variable	Description
<country_code_str>	Enter the two-character country code.
<state_name_str>	Enter the name of the state or province where the FortiManager unit is located.

Variable	Description
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiManager unit resides.
<organization-name_str>	Enter the name of the organization that is requesting the certificate for the FortiManager unit.
<organization-unit_name_str>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiManager unit.
<email_address_str>	Enter a contact email address for the FortiManager unit.
<ca_server_url>	Enter the URL of the CA (SCEP) certificate server that allows auto-signing of the request.
<challenge_password>	Enter the challenge password for the SCEP certificate server.

certificate remote

Use these commands to list, import, or export remote certificates.

Syntax

To list the remote certificates installed on the FortiManager unit:

```
execute certificate remote list
```

To export or import remote certificates:

```
execute certificate remote {<export>|<import>} <cert_name> <tftp_ip>
```

Variable	Description
list	Generate a list of remote certificates on the FortiManager system.
<export>	Export the certificate to TFTP server.
<import>	Import the certificate from a TFTP server.
<cert_name>	Name of the certificate.
<tftp_ip>	IP address of the TFTP server.

chassis

Use this command to replace a chassis device password on your device.



This command is only available on devices that support chassis management.

Syntax

```
execute chassis replace <pw>
```

Variable	Description
<pw>	Replace the chassis password.

console baudrate

Use this command to get or set the console baudrate.

Syntax

```
execute console baudrate [9600 | 19200 | 38400 | 57600 | 115200]
```

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

Setting the baudrate will disconnect your console session.

Example

Get the baudrate:

```
execute console baudrate
```

The response is displayed:

```
current baud rate is: 115200
```

Set the baudrate to 9600:

```
execute console baudrate 9600
```

date

Get or set the FortiManagersystem date.

Syntax

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

`date_str` has the form `mm/dd/yyyy`, where

- `mm` is the month and can be 01 to 12
- `dd` is the day of the month and can be 01 to 31
- `yyyy` is the year and can be 2001 to 2037

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

Dates entered will be validated - `mm` and `dd` require one or two digits, and `yyyy` requires four digits. Entering fewer digits will result in an error.

Example

This example sets the date to 29 September 2020:

```
execute date 9/29/2020
```

device

Use this command to change a device password or serial number when changing devices due to a hardware issue.

Syntax

```
execute device replace pw <device_name> <password>
execute device replace sn <device_name> <serial_number>
execute device replace user <device_name> <user>
```

Variable	Description
pw	Replace the device password.
sn	Replace the device serial number.
user	Replace the device user.
<device_name>	The name of the device.
<password>	The new password for the new device.
<serial_number>	The new serial number for the new device, for example: FWF40C391XXX0062.
<user>	The new user for the new device.

Example

```
execute device replace pw FGT600C2805030002
This operation will clear the password of the device.
Do you want to continue? (y/n)y
```

dmserver

Use these commands to manage devices and revisions.

dmserver	dmserver showdev
dmserver revlist	dmserver showrev

```
dmserver showconfig
```

dmserver delrev

Use this command to delete configuration revisions. The device name will be kept.

Syntax

```
execute dmserver delrev <device_name> <startrev> <endrev>
```

Variable	Description
<device_name>	The name of the device.
<startrev>	The starting configuration revision number that you want to delete.
<endrev>	The ending configuration revision number that you want to delete.

dmserver revlist

Use this command to show a list of revisions for a device.

Syntax

```
execute dmserver revlist <device_name>
```

Variable	Description
<device_name>	The name of the device.

dmserver showconfig

Use this command to show a specific configuration type and revision.

Syntax

```
execute dmserver showconfig <device_name>
```

Variable	Description
<device_name>	The name of the device.

dmserver showdev

Use this command to show a list of available devices. For each listed device, this command lists the device ID, device name, and serial number.

Syntax

```
execute dmserver showdev
```

dmserver showrev

Use this command to display a device's configuration revision.

Syntax

```
execute dmserver showrev <device_name> <revision>
```

Variable	Description
<device_name>	The name of the device.
<revision>	The configuration revision you want to display.

erasedisk

Overwrite the flash (boot device) with random data a specified number of times. When you run this command, you will be prompted to confirm the request.



Executing this command will overwrite all information on the FortiManager system's flash drive. The FortiManager system will no longer be able to boot up.

Syntax

```
execute erase-disk flash <erase-times>
```

Variable	Description
<erase-times>	Number of times to overwrite the flash with random data (1 - 35, default = 1).

factory-license

Use this command to enter a factory license key. This command is hidden.

Syntax

```
execute factory-license <key>
```

Variables	Description
<key>	The factory license key.

fgfm reclaim-dev-tunnel

Use this command to reclaim a management tunnel. The device name is optional.

Syntax

```
execute fgfm reclaim-dev-tunnel <device_name> force [admin] [password]
```

Variable	Description
<device_name>	Enter the device name.
force	Optionally, force the tunnel to be reclaimed
[admin]	Optionally, enter the administrator name.
[password]	Optionally, enter the administrator password.

fmpolicy

Use these commands to perform policy and object related actions:

fmpolicy check-upgrade-object

Use this command to check/upgrade objects by syntax.

Syntax

```
execute fmpolicy check-upgrade-object manual {checking | fixing} {basic | auto | misc | full}
execute fmpolicy check-upgrade-object report
execute fmpolicy check-upgrade-object reset
```

Variable	Description
<action>	Enter the auto upgrade action: <ul style="list-style-type: none"> • manual: run auto-upgrade manually. • report: show checking/upgrade report. • reset: cleanup saved checking/upgrade status
{checking fixing}	<ul style="list-style-type: none"> • checking: only do checking. • fixing: checking and fixing.
{basic auto misc full}	<ul style="list-style-type: none"> • basic: only do basic (know cases) checking/fixing. • auto: only do auto (syntax based) checking/fixing. • misc: only do misc (know cases) checking/fixing. • full: do a full basic/auto/misc checking/fixing.

fmpolicy clone-adom-object

Use this command to clone an ADOM object.

Syntax

```
execute fmpolicy clone-adom-object <src-adom> <category> <key> <target-adom> <new-key>
```

Variable	Description
<src-adom>	Enter the name of the source ADOM.
<category>	Enter the name of the category in the ADOM.
<key>	Enter the name of the object key.
<target-adom>	Enter the name of the target ADOM.
<new-key>	Enter the name of the new key.

fmpolicy copy-adom-object

Use this command to set the policy to copy an ADOM object.

Syntax

```
execute fmpolicy copy-adom-object <adom> <category> <key> <device> <vdom>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<category>	Enter the name of the category in the ADOM.

Variable	Description
<key>	Enter the name of the object key.
<device>	Enter the name of the device.
<vdom>	Enter the name of the VDOM.

fmpolicy install-config

Use this command to install the configuration for an ADOM.

Syntax

```
execute fmpolicy install-config <adom> <device_id> <revname>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<device_id>	Enter the device id of the ADOM.
<revname>	Enter the revision name.

fmpolicy print-adom-database

Use this command to display the device database configuration for an ADOM.

Syntax

```
execute fmpolicy print-adom-database <adom_name> <output_filename>
```

fmpolicy print-adom-object

Use this command to display the device objects.

Syntax

```
execute fmpolicy print-adom-object <adom_name>  
execute fmpolicy print-adom-object <adom_name> <category> {all | list} <output>  
execute fmpolicy print-adom-object Global <category> {all | list} <output>
```

Variable	Description
<adom_name>	Enter the name of the ADOM or “Global”.
<category>	Enter the category name.

Variable	Description
{all list}	<ul style="list-style-type: none"> all: Show all objects. list: Get all objects.
<output>	Output file name (output dump to file: [/tmp/pl]).

fmpolicy print-adom-package

Use this command to display the package for an ADOM.

Syntax

```
execute fmpolicy print-adom-package <adom> <template_name> <package_name> <category_name>
<object_name> [<output>]
```

Variable	Description
<adom>	Enter the name of the ADOM or “Global”.
<template_name>	Enter the policy package/template name.
<package_name>	Enter the package name ID.
<category_name>	Enter the category name.
<object_name>	Show object by name. <ul style="list-style-type: none"> all: Show all objects. list: Get all objects.
[<output>]	Output file name (output dump to file: [/tmp/pl]).

fmpolicy print-adom-package-assignment

Use this command to display the packages and provisioning templates assignment information for an ADOM.

Syntax

```
execute fmpolicy print-adom-package-assignment <adom> <policy package/template name>
```

Variable	Description
<adom>	Enter the name of the ADOM or “Global”: <ul style="list-style-type: none"> 104: FortiCarrier 149: FortiFirewall 128: Unmanaged_Devices 3: root
<policy package/template name>	Enter the policy package or the template name:

Variable	Description
	<ul style="list-style-type: none"> • 1: Policy Packages • 5: System Templates • 8: FortiClient Templates • 9: Threat Weight Templates • 10: WTP Packages • 14: FortiExtender Packages • 11: WAN Templates • 12: FortiSwitch Packages • 20: All Non-policy Packages

fmpolicy print-adom-policyblock

Use this command to display the policy block for an ADOM.

Syntax

```
execute fmpolicy print-adom-policyblock <adom> <policy_block_name> <category_name>
<object_name> <output>
```

Variable	Description
<adom>	Enter the name of the ADOM or “Global”.
<policy_block_name>	Enter the policy block name ID.
<category_name>	Enter the category name.
<object_name>	Show object by name. <ul style="list-style-type: none"> • all: Show all objects. • list: Get all objects.
<output>	Output file name (output dump to file: [/tmp/pl]).

fmpolicy print-device-database

Use this command to print the device database configuration.

Syntax

```
execute fmpolicy print-device-database <device_name> <output>
```

Variable	Description
<device_name>	Enter the name of the device.
<output>	Output file name (output dump to file: [/tmp/pl]).

fmpolicy print-device-object

Use this command to display the device objects.

Syntax

```
execute fmpolicy print-device-object <device_name> <vdom> <category> {<key> | list | all}
<output>
```

Variable	Description
<device_name>	Enter the name of the device.
<vdom>	Enter the VDOM name.
<category>	Enter the category name.
{<key> list all}	<ul style="list-style-type: none">all: Show all objects.list: Get all objects.
<output>	Output file name (output dump to file: [/tmp/pl]).

fmpolicy promote-adom-object

Use this command to promote an ADOM object.

Syntax

```
execute fmpolicy promote-adom-object <adom> <category> <key> <new-key>
```

Variable	Description
<adom>	Enter the name of the source ADOM.
<category>	Enter the name of the category in the ADOM.
<key>	Enter the name of the object key.
<new-key>	Enter the name of the new key.

fmpolicy upload-print-log

Use this command to upload the latest print command logs to a server.

Syntax

```
execute fmpolicy upload-print-log [ftp|scp|sftp] <server> <port> <path> <user> <passwd>
```

Variable	Description
[ftp scp sftp]	Enter the type of server to upload the logs to.
<server>	Enter the server IP address or DNS.
<port>	Enter the port number (0 for default).
<path>	Enter the path on the server.
<user>	Enter the username.
<passwd>	Enter the user's password.

fmprofile

Use these commands to perform profile related actions:

fmprofile copy-to-device	fmprofile import-from-device
fmprofile delete-profile	fmprofile import-profile
fmprofile export-profile	fmprofile list-profiles

fmprofile copy-to-device

Use this command to copy profile settings from a profile to a device.

Syntax

```
execute fmprofile copy-to-device <adom> <profile-id> <device_name>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<profile-id>	Enter the profile ID.
<device_name>	Enter the device ID.

fmprofile delete-profile

Use this command to delete a profile.

Syntax

```
execute fmprofile delete-profile <adom> <profile-id>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<profile-id>	Enter the profile ID.

fmprofile export-profile

Use this command to export profile configurations.

Syntax

```
execute fmprofile export-profile <adom> <profile-id> <output>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<profile-id>	Enter the profile ID.
<output>	Enter the output file name.

fmprofile import-from-device

Use this command to import profile settings from a device to a profile.

Syntax

```
execute fmprofile import-from-device <adom> <device_name> <profile-id>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<device_name>	Enter the device ID.
<profile-id>	Enter the profile ID.

fmprofile import-profile

Use this command to import profile configurations.

Syntax

```
execute fmprofile import-profile <adom> <profile_id> <filename>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<profile-id>	Enter the profile ID.
<filename>	Enter the full path to the input file containing CLI configuration.

fmprofile list-profiles

Use this command to list all profiles in an ADOM.

Syntax

```
execute fmprofile list-profiles <adom_name>
```

Variable	Description
<adom_name>	Enter the name of the ADOM.

fmscript

Use these commands to perform script related actions:

fmscript clean-sched	fmscript list
fmscript copy	fmscript run
fmscript delete	fmscript
fmscript import	

fmscript clean-sched

Clean the script schedule table for all non-existing devices.

Syntax

```
execute fmscript clean-sched
```

fmscript copy

Copy a script or scripts between ADOMs.

Syntax

```
execute fmscript copy <adom_name> <script ID> <adom> [<prefix>]
```

Variable	Description
<adom_name>	The source ADOM name.
<script ID>	The name of the script to copy (0000 = copy all scripts).
<adom>	The destination ADOM name.
[<prefix>]	Assign the conflict prefix. The default is the ADOM name.

fmscript delete

Delete a script from FortiManager.

Syntax

```
execute fmscript delete <scriptid>
```

Variable	Description
<scriptid>	The name of the script to delete.

fmscript import

Import a script from an FTP server to FortiManager.

Syntax

```
execute fmscript import <ftpsrvr_ip4> <filename> <username> <password> <scriptname>  
    <scripttype> <comment> <adom_name> <os_type> <os_version> <platform> <device_name>  
    <build_number> <hostname> <serial_number>
```

Variable	Description
<ftpsrvr_ip4>	The IPv4 address of the FTP server.
<filename>	The filename of the script to be imported to the FortiManager system.
<username>	The user name used to access the FTP server.
<password>	The password used to access the FTP server.
<scriptname>	The name of the script to import.
<scripttype>	The type of script as one of CLI or TCL.
<comment>	A comment about the script being imported, such as a brief description.

Variable	Description
<adom_name>	Name of the administrative domain.
<os_type>	The operating system type, such as FortiOS. Options include <code>any</code> , <code>FortiOS</code> , and others.
<os_version>	The operating system version, such as FortiOS. Options include <code>any</code> , <code>400</code> , and <code>500</code> .
<platform>	The hardware platform this script can be run on. Options include <code>any</code> , or the model of the device such as <code>Fortigate 60C</code> .
<device_name>	The device name to run this script on. Options include <code>any</code> , or the specific device name as it is displayed on the FortiManager system
<build_number>	The specific build number this script can be run on. Options include <code>any</code> , or the three digit build number. Build numbers can be found in the firmware name for the device.
<hostname>	The host name of the device this script can be run on. Options include <code>any</code> , or the specific host name.
<serial_number>	The serial number of the device this script can be run on. Options include <code>any</code> , or the specific serial number of the device, such as <code>FGT60C3G28033042</code> .

fmscript list

List the scripts on the FortiManager device.

Syntax

```
execute fmscript list
```

Example

This is a sample output of the `execute fmscript list` command.

```
FMG400C # execute fmscript list
scriptid=8,name=new account profile,type=CLI
scriptid=7,name=import_script,type=CLI
scriptid=6,name=group1,type=CLIGROUP
scriptid=5,name=basic_test,type=CLI
scriptid=3,name=interface info,type=CLI
scriptid=1,name=xml_script1,type=CLI
```

fmscript run

Run a script on a device, the device's object database, or on the global database. Only CLI scripts can be run on databases, and they must contain only complete commands. Any scripts that use shortened CLI commands will generate errors.

When a script is run on the database, the device will be updated with any configuration changes the next time the configuration is uploaded from the FortiManager system to the device.

Syntax

```
execute fmscript run [adom_name] <scriptid_int> <run_on> <dev/grp/pkgid>
```

Variable	Description
[adom_name]	Name of the administrative domain.
<scriptid_int>	The ID number of the script to run.
<run_on>	Select where to run the script: <ul style="list-style-type: none"> device: on the device group: on a group devicedb: on the device's object database adomdb: on a specific package globaldb: on the global database
<dev/grp/pkgid>	Enter the name of the device or group, or the ID of the package, to run the script on.

fmscript showlog

Display the log of scripts that have run on the selected device.

Syntax

```
execute fmscript showlog <device_name>
```

Variable	Description
<device_name>	The name of a managed FortiGate device.

Example

This example shows the output of `execute fmscript showlog Dev3` that displays the output from a CLI script called `xml_script1` that was run on the object database.

```
execute fmscript showlog Dev3
Starting log
config firewall address
  edit 33
    set subnet 33.33.33.33 255.255.255.0
  config firewall address
    edit 33
Running script(xml_script1) on DB success
cdb_find_entry_by_canon,52:parent=1,category=2,key=(null)
```

fmupdate

Import or export packages using the FTP, SCP, or TFTP servers.

Syntax

```
execute fmupdate {ftp | scp | tftp} import <type> <filename> <server> <port> <directory>
    <username> <password>
execute fmupdate {ftp | scp | tftp} export <type> <filename> <server> <port> <directory>
    <username> <password>
execute fmupdate {ftp | tftp} fds-export <objid> <filename> <server> <directory>
    <username> <password>
execute fmupdate fgd-db-merge {as | av | av2 | fq | iot | wf}
```

Variables	Description
{ftp scp tftp}	Select the file transfer protocol to use: ftp, scp, or tftp.
fds-export	Export the AV-IPS package to the FTP server.
fgd-db-merge {as av av2 fq iot wf}	Merge FortiGuard database immediately. Select the database type.
<type>	Select the package type to export or import: <ul style="list-style-type: none"> import: <ul style="list-style-type: none"> package = fcp package license = license package custom-url = customized URL database export: <ul style="list-style-type: none"> license = license package license-xml = license info. in xml custom-url = customized URL database
<filename>	Update manager packet file name on the server or host.
<objid>	Enter the object ID (use '-' as a separator).
<server>	Enter the FQDN or the IP address of the server.
<port>	Only available when the file transfer protocol is scp. Enter the port to connect to on the remote SCP host (1 - 65535).
<directory>	Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead.
<username>	Enter the username to log into the FTP server or SCP host
<password>	Enter the password to log into the FTP server or SCP host

format

Format the hard disk on the FortiManager system. You can select to perform a secure (deep-erase) format which overwrites the hard disk with random data. You can also specify the number of time to erase the disks.

Syntax

```
execute format <disk | disk-ext3 | disk-ext4> <RAID level> deep-erase <erase-times>
```

When you run this command, you will be prompted to confirm the request.



Executing this command will erase all device settings/images, VPN & Update Manager databases, and log data on the FortiManager system's hard drive. The FortiManager device's IP address, and routing information will be preserved.

Variable	Description
<disk disk-ext3 disk-ext4>	Select to format the hard disk or format the hard disk with ext4 file system.
<disk_partition_2>	Format hard disk partition 2 (static)
<disk_partition_2-ext4>	Format hard disk partition 2 (static) with ext4 file system.
<disk_partition_3>	Format hard disk partition 3 (dynamic)
<disk_partition_3-ext4>	Format hard disk partition 3 (dynamic) with ext4 file system.
<disk_partition_4>	Format hard disk partition 4 (misc)
<disk_partition_4-ext4>	Format hard disk partition 4 (misc) with ext4 file system.
deep-erase	Overwrite the hard disk with random data. Selecting this option will take longer than a standard format.
<erase-times>	Number of times to overwrite the hard disk with random data (1 - 35, default = 1).
<RAID level>	Enter the RAID level to be set on the device. This option is only available on FortiManager models that support RAID. Enter * to show available RAID levels.

iotop

Use this command to display system processes input/output usage information.

Syntax

```
execute iotop <parameter> <parameter> <parameter> <parameter> <parameter> <parameter>  
           <parameter> <parameter>
```

Parameter	Description
--version	Show the program's version number and exit.
-h, --help	Show this help message and exit.
-o, --only	Only show processes or threads that are actually doing I/O.
-b, --batch	Non-interactive mode.
-n NUM, --iter=NUM	The number of iterations before ending (default = infinite).
-d SEC, --delay=SEC	The delay between iterations, in seconds (default = 1).
-p PID, --pid=PID	The processes/threads to monitor (default = all).
-u USER, --user=USER	The users to monitor (default = all).
-P, --processes	Only show processes, not all threads.
-a, --accumulated	Show the accumulated I/O instead of bandwidth.
-k, --kilobytes	Use kilobytes instead of a human friendly unit.
-t, --time	Add a timestamp on each line (implies --batch).
-q, --quiet	Suppress some lines of header (implies --batch).

iotps

Use this command to list system processes sorted by their read/write system call rate.

Syntax

```
execute iotps
```

Variable	Description
<parameter>	Parameters: <ul style="list-style-type: none"> • -r • -w • -e • -t [intv]

log

Use these commands to manage device logs:

```
log adom disk_quota
```

```
log import
```

```

log device disk_quota
log device permissions
log device vdom
log dlp-files clear
log ips-pkt clear
log quarantine-files clear
log storage-warning

```

log adom disk_quota

Set the ADOM disk quota.

Syntax

```
execute log adom disk_quota <adom_name> <value>
```

Variable	Description
<adom_name>	Enter the ADOM name, or enter <code>All</code> for all ADOMs.
<value>	Enter the disk quota value in megabytes.

log device disk_quota

Set the log device disk quota.

Syntax

```
execute log device disk_quota <device_id> <value>
```

Variable	Description
<device_id>	Enter the log device ID number, or <code>All</code> for all devices.
<value>	Enter the disk quota value, in megabytes (100 - 5655).

log device permissions

Set or view the log device permissions.

Syntax

```
execute log device permissions <device_id> <permission> {enable | disable}
```

Variable	Description
<device_id>	Enter the log device ID number, or <code>All</code> for all devices.
<permission>	The following permissions are available:

Variable	Description
	<ul style="list-style-type: none"> all: All permissions logs: Log permission content: Content permission quar: Quarantine permission ips: IPS permission
{enable disable}	Enable/disable the option.

log device vdom

Use this command to add, delete, or list VDOMs.

Syntax

```
execute log device vdom add <device_name> <ADOM> <VDOM>
execute log device vdom delete <device_name> <VDOM>
execute log device vdom delete-by-id <device_name> <Id>
execute log device vdom list <device_name>
```

Variable	Description
add <device_name> <ADOM> <VDOM>	Add a new VDOM to a device with the device name, the ADOM that contains the device, and the name of the new VDOM.
delete <device_name> <VDOM>	Delete a VDOM from a device.
delete-by-id <device_name> <Id>	Delete a VDOM from a device using its ID number.
list <device_name>	List all the VDOMs on a device.

log dlp-files clear

Delete log DLP files.

Syntax

```
execute log dlp-files clear <device_name> <archive type>
```

Variable	Description
<device_name>	Enter the device name.
<archive type>	Enter the device archive type: all, email, im, ftp, http, or mms.

log import

Use this command to import log files from another device and replace the device ID on imported logs.

Syntax

```
execute log import <service> <ip_address> <user-name> <password> <file-name> <device-id>
```

Variable	Description
<service>	Select the file transfer protocol to use: ftp, sftp, scp, or tftp.
<ip:port>	Server IP address or host name. Port is optional.
<user-name>	Enter the username.
<password>	Enter the password or – for no password. The <password> field is not required when <service> is tftp.
<file-name>	The file name (e.g. dir/fgt.alog.log) or directory name (e.g. dir/subdir/).
<device-id>	Replace the device ID on imported logs. Enter a device serial number of one of your log devices.

log ips-pkt clear

Delete IPS packet files.

Syntax

```
execute log ips-pkt clear <device_name>
```

Variable	Description
<device_name>	Enter the device name.

log quarantine-files clear

Delete log quarantine files.

Syntax

```
execute log quarantine-files clear <string>
```

Variable	Description
<string>	Enter the device name.

log storage-warning

Reset the licensed VM storage size warning

Syntax

```
execute log storage-warning reset
```

log-fetch

Use the following commands to fetch logs.

log-fetch client

Use these commands to manage client sessions.

Syntax

```
execute log-fetch client cancel <profile name>
execute log-fetch client list <profile name>
execute log-fetch client pause <profile name>
execute log-fetch client resume <profile name>
execute log-fetch client run <profile name>
execute log-fetch client view <profile name>
```

Variable	Description
cancel <profile name>	Cancel one session.
list <profile name>	List all sessions.
pause <profile name>	Pause one session.
resume <profile name>	Resume one session.
run <profile name>	Start a new session.
view <profile name>	View the session status.

log-fetch server

Use this command to manager the log fetching server.

Syntax

```
execute log-fetch server approve <session id>
execute log-fetch server cancel <session id>
```

```
execute log-fetch server deny <session id>
execute log-fetch server list
execute log-fetch server pause <session id>
execute log-fetch server resume <session id>
execute log-fetch server view <session id>
```

Variable	Description
approve <session id>	Approve a session.
cancel <session id>	Pause and clear one session or all sessions.
deny <session id>	Deny a session.
list	List all sessions.
pause <session id>	Pause a session.
resume <session id>	Resume a session.
view <session id>	View the session.

log-integrity

Query the log file's MD5 checksum and timestamp.

Syntax

```
execute log-integrity <device_name> <vdom name> <log_name>
```

Variable	Description
<device_name>	The name of the log device.
<vdom name>	The VDOM name.
<log_name>	The log file name.

lvm

With Logical Volume Manager (LVM), a FortiManager VM device can have up to fifteen total log disks added to an instance. More space can be added by adding another disk and running the LVM extend command.



This command is only available on FortiManager VM models.

Syntax

```
execute lvm extend
execute lvm info
execute lvm start
```

Variables	Description
extend	Extend the LVM logical volume.
info	Get system LVM information.
start	Start using LVM.

max-dev-licence

Use this command to load add-on licenses to support more devices with a license key.



This command is only available on FortiManager VM models.

Syntax

```
execute max-dev-licence <key>
```

migrate

Use this command to migrate all backup settings from the FTP, SCP, or SFTP server.

Syntax

```
execute migrate all-settings {ftp | scp | sftp} <ip:port> <string> <username> <password>
<ssh-cert> [<crptpasswd>]
```

Variable	Description
{ftp scp sftp}	Enter the server type: ftp, scp, or sftp.
<ip:port>	Enter the server IP address and optionally, for FTP servers, the port number.
<string>	Enter the path and file name for the backup.
<username>	Enter username to use to log on the backup server.

Variable	Description
<passwd>	Enter the password for the username on the backup server.
<ssh-cert>	Enter the SSH certification for the server. This option is only available for backup operations to SCP servers.
[<crptpasswd>]	Optional password to protect backup content. Use <code>any</code> for no password.

ping

Send an ICMP echo request (ping) to test the network connection between the FortiManager system and another network device.

Syntax

```
execute ping <ip | hostname>
```

Variable	Description
<ip hostname>	IPv4 address or DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IPv4 address `192.168.1.23`:

```
execute ping 192.168.1.23
```

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiManager system and another network device.

Syntax

```
execute ping6 <ip | hostname>
```

Variable	Description
<ip hostname>	Enter the IPv6 address or DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IPv6 address `8001:0DB8:AC10:FE01:0:0:0:0`:

```
execute ping6 8001:0DB8:AC10:FE01:0:0:0:0:
```

raid

This command allows you to add and delete RAID disks.



This command is only available on hardware-based FortiManager models that support RAID.

Syntax

```
execute raid add-disk <disk index>
execute raid delete-disk <disk index>
```

Variable	Description
add-disk <disk index>	Add a disk and give it an index number.
delete-disk <disk index>	Delete the specified disk.

reboot

Restart the FortiManager system. This command will disconnect all sessions on the FortiManager system.

Syntax

```
execute reboot
```

remove

Use this command to remove all custom settings in Logview, all reports for a specific device, resync files, and a security fabric from a specific ADOM.

Syntax

```
execute remove gui-logview-settings
execute remove reports <device-id>
execute remove resync
execute remove security-facbric <adom-name> <security-fabric-name>
```

Variable	Description
<device-id>	The device identifier for the device that all reports are being removed from.
<adom-name>	The ADOM that contains the security fabric that is being removed.
<security-fabric-name>	The security fabric that is being removed.

Example

```
execute remove gui-logview-settings
This operation will Remove all custom settings in GUI LogView and reset to default for
all users.
Do you want to continue? (y/n)y

Remove all custom settings in GUI LogView ...
Done! Reset all settings in GUI LogView to default.
```

reset

Use this command to reset the FortiManager unit. These commands will disconnect all sessions and restart the FortiManager unit.

Syntax

```
execute reset adom-settings <adom> <version> <mr> <ostype>
execute reset all-except-ip
execute reset all-settings
execute reset all-shutdown
```

Variable	Description
adom-settings <adom> <version> <mr> <ostype>	Reset an ADOM's settings. <ul style="list-style-type: none"> <adom>: The ADOM name. <version>: The ADOM version. For example, 5 for 5.x releases. <mr>: The major release number. <ostype>: Supported OS type. For example, 18 for FortiDeceptor.
all-except-ip	Reset all settings except the current IP address and route information.
all-settings	Reset to factory default settings.
all-shutdown	Reset all settings and shutdown.

reset-sqllog-transfer

Use this command to resend SQL logs to the database.

Syntax

```
execute reset-sqllog-transfer <enter>
```

restore

Use this command to restore the configuration or database from a file and change the FortiManager unit image. These commands will disconnect all sessions and restart the FortiManager unit.

Syntax

```
execute restore all-settings {ftp | sftp} <ip:port> <filename> <username> <password>
    [<crptpasswd>] [option1+option2+...]
execute restore all-settings <scp> <ip> <filename> <username> <ssh-cert> [<crptpasswd>]
    [option1+option2+...]
execute restore image {ftp | scp | sftp} <filepath> <ip:port> <username> <password>
execute restore image tftp <string> <ip>
execute restore logs <device name(s)> {ftp | scp | sftp} <ip> <username> <password>
    <directory> [vdlist]
execute restore logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <password>
    <directory> [vdlist]
execute restore reports <report name(s)> {ftp | scp | sftp} <ip> <username> <password>
    <directory> [vdlist]
execute restore reports-config {<adom_name> | all} {ftp | scp | sftp} <ip> <username>
    <password> <directory> [full]
```

Variable	Description
all-settings	Restore all FortiManager settings from a file on a server. The new settings replace the existing settings, including administrator accounts and passwords.
image	Upload a firmware image from a(an) FTP/SCP/SFTP/TFTP server to the FortiManager unit. The FortiManager unit reboots, loading the new firmware.
logs	Restore the device logs.
logs-only	Restore only the device logs.
reports	Restore device reports.
reports-config	Restore the reports configuration.
ftp	Restore from an FTP server.
sftp	Restore from a SFTP server.
scp	Restore from an SCP server.
<ip:port>	Enter the IP address of the server to get the file from and optionally , for FTP servers, the port number.
<ip>	Enter the server IP address.

Variable	Description
<device name(s)>	Enter the device name(s) separated by a comma, or enter <code>all</code> for all devices.
<report name(s)>	Restore specific reports (separated by commas), <code>all</code> for all reports, or reports with names containing given pattern. A '?' matches any single character. A '*' matches any string, including the empty string, e.g.: <ul style="list-style-type: none"> <code>foo</code>: for exact match <code>*foo</code>: for report names ending with foo <code>foo*</code>: for report names starting with foo <code>*foo*</code>: for report names containing foo substring.
{<adom_name> all}	Select to backup a specific ADOM or all ADOMs.
<filename>	Enter the file to get from the server. You can enter a path with the filename, if required.
<filepath>	Enter the file to get from the server. You can enter a path with the filename, if required.
<username>	The username to log on to the server. This option is not available for restore operations from TFTP servers.
<password>	The password for username on the server. This option is not available for restore operations from TFTP servers.
<ssh-cert>	The SSH certification for the server. This option is only available for restore operations from SCP servers.
[<crptpassword>]	Optional password to protect backup content. Use <code>any</code> for no password.
[option1+option2+...]	Enter <code>keepbasic</code> to retain IP and routing information on the original unit.
<directory>	Enter the directory.
[full]	Reports configuration full restoration.

Example

This example shows how to upload a configuration file from a FTP server to the FortiManager unit. The name of the configuration file on the FTP server is `backupconfig`. The IP address of the FTP server is `192.168.1.23`. The user is `admin` with a password of `mypassword`. The configuration file is located in the `/usr/local/backups/` directory on the TFTP server.

```
execute restore all-settings 192.168.1.23 /usr/local/backups/backupconfig admin mypassword
```

sdns

Use this command to enable and reboot the SDNS system, and to load an SDNS image.



This command is only available on hardware-based FortiManager models .

Syntax

```
execute sdns enable
execute sdns image ftp <filepath> <ip> <username> <password>
```

Variable	Description
enable	Enable and reboot to SDNS system.
image ftp <filepath> <ip> <username> <password>	Load an SDNS image.

sensor

This command lists sensors and readings.



This command is only available on hardware-based FortiManager models.

Syntax

```
execute sensor detail
execute sensor list
```

Variable	Description
detail	List detailed sensors and readings.
list	List sensors and readings.

shutdown

Shut down the FortiManager system. This command will disconnect all sessions.

Syntax

```
execute shutdown
```

sql-local

Use these commands to remove the SQL database and logs from the FortiManager system and to rebuild the database and devices.



When rebuilding the SQL database, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Syntax

```
execute sql-local rebuild-adom <adom> ... <adom>
execute sql-local rebuild-db
execute sql-local rebuild-index <adom> <start-time> <end-time>
execute sql-local rebuild-skipidx <adom> <start-time> <end-time>
```

Variable	Description
rebuild-adom	Rebuild log SQL database from log data for particular ADOMs.
rebuild-db	Rebuild entire log SQL database from log data. This operation will remove the SQL database and rebuild from log data. It will also reboot the device.
rebuild-index	Rebuild indexes for an ADOM.
rebuild-skipidx	Rebuild skip-indexes.
<adom>	The ADOM name. Multiple ADOM names can be entered when rebuilding ADOMs.
<start-time>	Enter the start time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<end-time>	Enter the end time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<log type>	Enter the log type from available log types, for example: <code>emailfilter</code>

sql-query-dataset

Use this command to execute a SQL dataset against the FortiManager system.

Syntax

```
execute sql-query-dataset <adom_name> <dataset-name> <device/group name> <faz/dev>
    <start-time> <end-time>
```

Variable	Description
<adom_name>	Enter the ADOM name.
<dataset-name>	Enter the SQL dataset name.
<device/group name>	Enter the name of the device or device group.
<faz/dev>	Enter the reference time: FortiAnalyzer time or device time.
<start-time>	Enter the log start time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<end-time>	Enter the log end time (timestamp or <yyyy-mm-dd hh:mm:ss>).

sql-query-generic

Use this command to execute a SQL statement against the FortiManager system.

Syntax

```
execute sql-query-generic <string>
```

Variable	Description
<string>	Specify the SQL statement to be executed.

sql-report

Use these commands to import and display language translation and fonts files, and to run a SQL report once against the FortiManager system.

Syntax

```
execute sql-report delete-font <font-name>
execute sql-report delete-lang <language-name>
execute sql-report delete-template adom-installed <adom> <language> [title]
execute sql-report delete-template device-default <dev-type> <language> [title]
execute sql-report export-lang <language-name> <service> <ip> <argument 1> <argument 2>
    <argument 3>
execute sql-report export-template adom-installed <adom> <service> <ip> <user> <password>
    <file name> [language] [title]
execute sql-report export-template device-default <dev-type> <service> <ip> <user>
    <password> <file name> [language] [title]
execute sql-report hcache-build <adom> <schedule-name> <start-time> <end-time>
execute sql-report hcache-check <adom> <schedule-name> <start-time> <end-time>
execute sql-report import-font <service> <ip> <argument 1> <argument 2> <argument 3>
execute sql-report import-lang <language-name> <service> <ip> <argument 1> <argument 2>
    <argument 3>
execute sql-report import-template <devtype> <service> <ip> <user> <password> <file name>
```

```

execute sql-report install-template <adom> <language> <service> <ip> <user> <password>
    <file name>
execute sql-report list <adom> [days-range] [layout-name]
execute sql-report list-fonts
execute sql-report list-lang [language]
execute sql-report list-schedule <adom> [sched-only | autocache-only | detail] [detail]
execute sql-report list-template adom-installed <adom> [language]
execute sql-report list-template device-default <dev-type> [language]
execute sql-report run <adom> <schedule-name> <start-time> <end-time>
execute sql-report view <data-type> <adom> <report-name>

```

Variable	Description
delete-font	Delete one font.
delete-lang	Delete one language translation file.
delete-template	Delete templates. <ul style="list-style-type: none"> • <code>adom-installed</code> - Delete report templates installed in ADOM. • <code>device-default</code> - Delete device type default report templates.
export-lang	Export a user-defined language translation file.
export-template	Export report templates. <ul style="list-style-type: none"> • <code>adom-installed</code> - Export ADOM report templates to file. • <code>device-default</code> - Export device type default report templates to file.
hcache-build	Build report hcache.
hcache-check	Check report hcache.
import-font	Import one font.
import-lang	Import a user-defined language translation file.
import-template	Import per device type template from a configuration file.
install-template	Install specific language templates to an ADOM.
list	List recent generated reports.
list-fonts	List all imported fonts.
list-lang	Display all supported language translation files.
list-schedule	List report schedule and autocache information.
list-template	List templates. <ul style="list-style-type: none"> • <code>adom-installed</code> - Display report templates installed in ADOM. • <code>device-default</code> - Display device type default report templates.
run	Run a report once.
view	View report data.
<adom>	Specify the ADOM name.
<font-name>	The name of a font.
<dev-type>	Enter the device type abbreviation:

Variable	Description
	<ul style="list-style-type: none"> • FGT - FortiGate • FMG - FortiManager • FCT - FortiClient • FML - FortiMail • FWB - FortiWeb • FCH - FortiCache • FAZ - FortiAnalyzer • FSA - FortiSandbox • FDD - FortiDDoS • FAC - FortiAuthenticator • FPX - FortiProxy
<language-name>	<p>Enter the language name to import, export, or delete a language translation file, or select one of the following options:</p> <ul style="list-style-type: none"> • English • French • Japanese • Korean • Portuguese • Simplified_Chinese • Spanish • Traditional_Chinese
<service>	<p>Enter the transfer protocol: <code>ftp</code>, <code>sftp</code>, <code>scp</code>, or <code>tftp</code>. TFTP is not available for all commands.</p>
<ip>	Enter the server IP address.
<argument 1>	For FTP, SFTP, or SCP, type a user name. For TFTP, enter a file name.
<argument 2>	For FTP, SFTP, or SCP, type a password or ' <code>.</code> '. For TFTP, press <enter>.
<argument 3>	Enter a file name and press <enter>.
<user>	Enter a user name for the remote server.
<password>	Enter the password, or <code>-</code> , for the remote server user.
<file name>	Enter the name of the file.
<data-type>	The data type to view: <code>report-data</code> or <code>report-log</code> .
<report-name>	The name of the report to view.
<schedule-name>	Select one of the available report schedule names.
<start-time>	The start date and time of the report schedule, in the format: " <code>HH:MM yyyy/mm/dd</code> "
<end-time>	The enddate and time of the report schedule, in the format: " <code>HH:MM yyyy/mm/dd</code> "
[days-range]	The recent <code>n</code> days to list reports, from 1 to 99.
[layout-name]	One of the available SQL report layout names.
[language]	<p>Enter the language abbreviation:</p> <ul style="list-style-type: none"> • <code>en</code> - English • <code>de</code> - German • <code>ko</code> - Korean • <code>pt</code> - Portuguese

Variable	Description
	<ul style="list-style-type: none"> • <code>es</code> - Spanish • <code>fr</code> - French • <code>it</code> - Italian • <code>ja</code> - Japanese • <code>ru</code> - Russian • <code>zh</code> - Simplified Chinese • <code>zh_Hant</code> - Traditional Chinese
<code>[title]</code>	Title of a specific report template.

ssh

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

Syntax

```
execute ssh <destination> <username>
```

Variable	Description
<code><destination></code>	Enter the IP address or fully qualified DNS resolvable hostname of the system you are connecting to.
<code><username></code>	Enter the user name to use to log on to the remote system.

To leave the SSH session type `exit`. To confirm that you are connected or disconnected from the SSH session, verify the command prompt has changed.

ssh-known-hosts

Use these commands to remove all known SSH hosts.

Syntax

```
execute ssh-known-hosts remove-all
execute ssh-known-hosts remove-host <host/ip>
```

Variable	Description
<code>remove-all</code>	Remove all known SSH hosts.
<code>remove-host</code>	Remove the specified SSH hosts. <ul style="list-style-type: none"> • <code><host/IP></code> - The hostname or IP address of the SSH host to remove.

tac

Use this command to run or upload a debug report.

Syntax

```
execute tac report
execute tac upload <service> <ip> <dir> <user name> <password>
```

Variable	Description
<service>	Enter the transfer protocol: <code>ftp</code> , <code>sftp</code> , or <code>scp</code> .
<ip>	Enter the server IP address. For <code>ftp</code> , the port can be specified by adding <code>:port</code> .
<dir>	Enter the directory.
<user name>	Enter the username.
<password>	Enter the password or enter <code>-</code> for no password.

time

Get or set the system time.

Syntax

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

Variable	Description
[<time_str>]	<p>The time of day, in the form <code>hh:mm:ss</code>.</p> <ul style="list-style-type: none"><code>hh</code> is the hour and can be <code>00</code> to <code>23</code><code>mm</code> is the minutes and can be <code>00</code> to <code>59</code><code>ss</code> is the seconds and can be <code>00</code> to <code>59</code> <p>All parts of the time are required. Single digits are allowed for each of <code>hh</code>, <code>mm</code>, and <code>ss</code>.</p>

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

Example

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

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

top

Use this command to view the processes running on the FortiManager system.

Syntax

```
execute top <parameter> <parameter> ... <parameter>
```

Variable	Description
<parameter>	The following parameters can be used: -hv -bcHiOSs -d secs -n max -u U user -p pid(s) -o field -w [cols]

execute top help menu

Use the following commands when viewing the running processes. Press **h** or **?** for help.

Command	Description
Z,B,E,e	Global: 'Z' colors; 'B' bold; 'E'/'e' summary/task memory scale
l,t,m	Toggle Summary: 'l' load avg; 't' task/cpu stats; 'm' memory info
0,1,2,3,l	Toggle: '0' zeros; '1/2/3' cpus or numa node views; 'l' lrix mode
f,F,X	Fields: 'f'/'F' add/remove/order/sort; 'X' increase fixed-width
L,&,<,> .	Locate: 'L'/'&' find/again; Move sort column: '<'/'>' left/right
R,H,V,J .	Toggle: 'R' Sort; 'H' Threads; 'V' Forest view; 'J' Num justify
c,i,S,j .	Toggle: 'c' Cmd name/line; 'i' Idle; 'S' Time; 'j' Str justify
x,y.	Toggle highlights: 'x' sort field; 'y' running tasks
z,b.	Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
u,U,o,O .	Filter by: 'u'/'U' effective/any user; 'o'/'O' other criteria
n,#,^O.	Set: 'n'/'#' max tasks displayed; Show: Ctrl+'O' other filter(s)
C,....	Toggle scroll coordinates msg for: up,down,left,right,home,end
k,r	Manipulate tasks: 'k' kill; 'r' renice
d or s	Set update interval
W,Y	Write configuration file 'W'; Inspect other output 'Y'
q or <Esc>	Quit

traceroute

Test the connection between the FortiManager system and another network device, and display information about the network hops between the device and the FortiManager system.

Syntax

```
execute traceroute <host>
```

Variable	Description
<host>	Enter the IPv4 address or hostname of network device.

traceroute6

Test the connection between the FortiManager system and another network device, and display information about the network hops between the device and the FortiManager system.

Syntax

```
execute traceroute6 <host>
```

Variable	Description
<host>	Enter the IPv6 address or hostname of network device.

diagnose

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.



CLI commands and variables are case sensitive.

auto-delete	fmnetwork	log device	upload
cdb	fmupdate	pm2	vpn
debug	fortilogd	report	
dlp-archives	fwmanager	sniffer	
docker	ha	sql	
dvm	hardware	svctools	
faz-cdb	incident	system	
fgfm	license	test	

auto-delete

Use this command to diagnose auto deletion of DLP files, log files, quarantine files, and report files.

Syntax

```
diagnose auto-delete dlp-files {delete-now | list}
diagnose auto-delete log-files {delete-now | list}
diagnose auto-delete quar-files {delete-now | list}
diagnose auto-delete report-files {delete-now | list}
```

Variable	Description
dlp-files {delete-now list}	Delete or list DLP files. <ul style="list-style-type: none"><code>delete-now</code>: Delete DLP files right now according to system automatic deletion policy.<code>list</code>: List DLP files according to system automatic deletion policy.
log-files {delete-now list}	Delete or list log files. <ul style="list-style-type: none"><code>delete-now</code>: Delete log files right now according to system automatic deletion policy.<code>list</code>: List log files according to system automatic deletion policy.

Variable	Description
quar-files {delete-now list}	Delete or list quarantine files. <ul style="list-style-type: none"> <code>delete-now</code>: Delete quarantine files right now according to system automatic deletion policy. <code>list</code>: List quarantine files according to system automatic deletion policy.
report-files {delete-now list}	Delete or list report files. <ul style="list-style-type: none"> <code>delete-now</code>: Delete report files right now according to system automatic deletion policy. <code>list</code>: List report files according to system automatic deletion policy.

cdb

Use this command to check and repair or upgrade and repair the object configuration database and global policy assignment table.

Syntax

```

diagnose cdb check adom-integrity [adom]
diagnose cdb check adom-rebuild [adom]
diagnose cdb check adom-revision [adom] [preview]
diagnose cdb check policy-packages [adom]
diagnose cdb check update-devinfo logdisk-size [new value] [0 | 1] [model-name]
diagnose cdb check update-devinfo sslvpn-flag <devname>
diagnose cdb upgrade check <action>
diagnose cdb upgrade force-retry <action>
diagnose cdb upgrade log
diagnose cdb upgrade pending-list
diagnose cdb upgrade summary

```

Variable	Description
check adom-integrity [adom]	Check and repair the specified ADOM's database.
check adom-rebuild [adom]	Rebuild the specified ADOM.
check adom-revision [adom] [preview]	Check or remove invalid ADOM revision database. Optionally, preview the check before running it.
check policy-packages [adom]	Check the policy packages.
check reference-integrity [preview]	Check the ADOM reference table integrity. Optionally, preview the check before running it.
check update-devinfo logdisk-size [new value] [0 1] [model-name]	Update device log disk size. <ul style="list-style-type: none"> <code>new value</code>: Item new value. <code>0 1</code>: update only empty values (default), or always update (1) <code>model-name</code>: Only update on model name (default: all models).

Variable	Description
check update-devinfo sslvpn-flag <devname>	Upgrade the device SSL-VPN flag on the specified device.
upgrade check <action>	Perform a check to see if upgrade and repair is necessary. <ul style="list-style-type: none"> • objcfg-integrity - Object config database integrity • reference-integrity - Reference table integrity • object-sequence - Repair invalid object sequence • duplicate-uuid - Reassign duplicated uuid in ADOM database • resync-dev-vdms - Resync and add any missing vdms from device database to DVM database • invalid-install-target - Invalid policy package and template install target • fw-addr-type - Firewall address wrong FQDN type • zone-defmap-intf - Unset invalid defmap-intf field in dynamic zone
upgrade force-retry <action>	Re-run an upgrade that was already performed in previous release. <ul style="list-style-type: none"> • clear-max-policyid - Clear ADOM max_policyid cache • refresh-controller-count - Refresh controller license count • resync-dbcache - Resync device database cache
upgrade log	Display the configuration database upgrade log.
upgrade pending-list	Display the list of upgrades scheduled for the next reboot.
upgrade summary	Display the firmware upgrade summary.

debug

Use the following commands to debug the FortiManager.

debug application

Use this command to view or set the debug levels for the FortiManager applications. All of the debug levels are 0 by default.

Syntax

```

diagnose debug application alertmail <integer>
diagnose debug application apiproxyd <integer>
diagnose debug application auth <integer>
diagnose debug application clusterd <integer>
diagnose debug application connector <integer>
diagnose debug application curl <integer>
diagnose debug application ddmd <integer> <deviceName>
diagnose debug application depmanager <integer>
diagnose debug application dmapl <integer>
diagnose debug application dns <integer>

```

```
diagnose debug application docker <integer>
diagnose debug application dump
diagnose debug application execcmd <integer>
diagnose debug application fabricsyncd <integer>
diagnose debug application fazcfgd <integer>
diagnose debug application fazmaild <integer>
diagnose debug application faznotify <integer>
diagnose debug application fazsvcd <integer>
diagnose debug application fazwatchd <integer>
diagnose debug application fdssvrd <integer>
diagnose debug application fgdsrv <integer>
diagnose debug application fgdupd <integer>
diagnose debug application fgfmsd <integer> <deviceName>
diagnose debug application filefwd <integer>
diagnose debug application fileparsed <integer>
diagnose debug application fortilogd <integer>
diagnose debug application FortiManagerws <integer>
diagnose debug application fortimeter <integer>
diagnose debug application gui <integer>
diagnose debug application ha <integer>
diagnose debug application ipsec <integer>
diagnose debug application localmod <integer>
diagnose debug application logd <integer>
diagnose debug application log-fetchd <integer>
diagnose debug application logfiled <integer>
diagnose debug application logfwd <integer>
diagnose debug application lrm <integer>
diagnose debug application ntpd <integer>
diagnose debug application oftpd <integer> <IP/deviceSerial/deviceName>
diagnose debug application ptmgr <integer>
diagnose debug application ptsessionmgr <integer>
diagnose debug application rptchkd <integer>
diagnose debug application rtmmond <integer>
diagnose debug application scansched <integer>
diagnose debug application scheduled <integer>
diagnose debug application securityconsole <integer>
diagnose debug application siemagentd <integer>
diagnose debug application siemdbd <integer>
diagnose debug application sniffer <integer>
diagnose debug application snmpd <integer>
diagnose debug application sql_dashboard_rpt <integer>
diagnose debug application sql-integration <integer>
diagnose debug application sqllogd <integer>
diagnose debug application sqlplugind <integer> <filter>
diagnose debug application sqlreportd <integer> <filter>
diagnose debug application sqlrptcached <integer>
diagnose debug application srchd <integer>
diagnose debug application ssh <integer>
diagnose debug application sshd <integer>
diagnose debug application storaged <integer>
diagnose debug application syncsched <integer>
diagnose debug application uploadd <integer>
diagnose debug application vmd <integer>
```

Variable	Description
alertmail <integer>	Set the debug level of the alert email daemon.
apiproxyd <integer>	Set the debug level of the API proxy daemon.
auth <integer>	Set the debug level of the Fortinet authentication module.
clusterd <integer>	Set the debug level of the clusterd daemon.
connector <integer>	Set the debug level of the connector daemon.
curl <integer>	Set the debug level of the curl daemon. Use this CLI command to enable debug for monitoring progress when performing a backup/restore of a large database via FTP.
ddmd <integer> <deviceName>	Set the debug level of the dynamic data monitor. Enter a device name to only show messages related to that device. Note: Enter " " to reset.
depmanager <integer>	Set the debug level of the deployment manager.
dmworker <integer>	Set the debug level of the deployment manager worker.
dmapi <integer>	Set the debug level of the dmapi daemon.
dns <integer>	Set the debug level of the DNS daemon.
docker <integer>	Set the debug level of the Docker daemon.
dump	Dump services.
execmd <integer>	Set the debug level of the execmd daemon.
fabricsyncd <integer>	Set the debug level of the fabricsyncd daemon (0 - 8).
fazcfgd <integer>	Set the debug level of the fazcfgd daemon.
fazmaild <integer>	Set the debug level of the fazmaild daemon.
faznotify <integer>	Set the debug level of the faznotify daemon.
fazsvcd <integer>	Set the debug level of the fazsvcd daemon.
fazwatchd <integer>	Set the debug level of the fazwatchd daemon.
fdssvrd <integer>	Set the debug level of the FDS server daemon.
fgdsrv <integer>	Set the debug level of the FortiGuard query daemon.
fgdupd <integer>	Set the debug level of the FortiGuard update daemon.
fgfmsd <integer> <deviceName>	Set the debug level of FGFM daemon. Enter a device name to only show messages related to that device. Note: Enter " " to reset. Multiple device names should be separated by commas. For example, Host1, Host2.
filefwd <integer>	Set the debug level of the filefwd daemon.
fileparsed <integer>	Set the debug level of the fileparsed daemon.

Variable	Description
fortilogd <integer>	Set the debug level of the fortilogd daemon.
fortimanagerws <integer>	Set the debug level of the FortiManager Web Service.
fortimeter <integer>	Set the debug level of the Fortimeter.
gui <integer>	Set the debug level of the GUI.
ha <integer>	Set the debug level of high availability daemon.
ipsec <integer>	Set the debug level of the IPsec daemon.
localmod <integer>	Set the debug level of the localmod daemon.
logd <integer>	Set the debug level of the log daemon.
log-fetched <integer>	Set the debug level for the log-fetched.
logfiled <integer>	Set the debug level of the logfiled daemon.
logfwd <integer>	Set the debug level of the logfwd daemon.
lrm <integer>	Set the debug level of the Log and Report Manager.
ntpd <integer>	Set the debug level of the NTP daemon.
oftpd <integer> <IP/deviceSerial/deviceName>	Set the debug level of the oftpd daemon. Enter an IPv4 address, device serial number, or device name to only show messages related to that device or IPv4 address. Note: Enter "" to reset.
ptmgr <integer>	Set the debug level of the Portal Manager.
ptsessionmgr <integer>	Set the debug level of the Portal Session Manager.
rptchkd <integer>	Set the debug level of the rptchkd daemon.
rtmonnd <integer>	Set the debug level of the real time monitor daemon.
scansched <integer>	Set the debug level of the scan schedule daemon.
scheduled <integer>	Set the debug level of the schedule task daemon.
securityconsole <integer>	Set the debug level of the security console daemon.
siemagentd <integer>	Set the debug level of the siemagentd daemon.
siemdbd <integer>	Set the debug level of the siemdbd daemon.
sniffer <integer>	Set the debug level of the interface sniffer.
snmpd <integer>	Set the debug level of the SNMP daemon.
sql_dashboard_rpt <integer>	Set the debug level of the SQL dashboard report daemon.
sql-integration <integer>	Set the debug level of SQL applications.
sqllogd <integer>	Set the debug level of SQL log daemon.
sqlplugind <integer> <filter>	Set the debug level of the SQL plugin daemon. Set filter for sqlplugind.

Variable	Description
	Note: Enter "" to reset the filter.
sqlreportd <integer> <filter>	Set the debug level (0-8) of the SQL report daemon. Set the filter for sqlreportd. Note: Enter "" to reset the filter. Without <integer> and <filter>, it shows the current debug level and filter of sqlreportd.
sqlrptcached <integer>	Set the debug level of the SQL report caching daemon.
srchd <integer>	Set the debug level of the SRCH daemon.
ssh <integer>	Set the debug level of SSH protocol transactions.
sshd <integer>	Set the debug level of the SSH daemon.
stored <integer>	Set the debug level of communication with java clients.
syncsched <integer>	Set the debug level of the syncsched daemon.
uploadd <integer>	Set the debug level of the upload daemon.
vmd <integer>	Set the debug level for vmd.

Example

This example shows how to set the debug level to 7 for the upload daemon:

```
diagnose debug application uploadd 7
```

debug backup-oldformat-script-logs

Use this command to backup script log files that failed to be upgraded to the FTP server.

Syntax

```
diagnose debug backup-oldformat-script-logs <ip> <string> <username> <password>
```

Variable	Description
<ip>	Enter the FTP server IP address.
<string>	Enter the path/filename to save the log to the FTP server.
<username>	Enter the user name on the FTP server.
<password>	Enter the password associated with the user name.

debug cdbchk

Use these commands to enable or disable CLI CDB check debug output.

Syntax

```
diagnose debug cdbcheck {enable | disable}
```

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <integer>
```

Variable	Description
<integer>	Set the debug level of the CLI (0 - 8, default = 3).

debug console

Use this command to enable or disable console debugging.

Syntax

```
diagnose debug console {enable | disable}
```

Variable	Description
{enable disable}	Enable/disable console debugging.

debug coredump

Use this command to manage daemon and process core dumps.

Syntax

```
diagnose debug coredump crash-pid <pid>
diagnose debug coredump delete <daemon>
diagnose debug coredump disable <daemon>
diagnose debug coredump disable-pid <pid>
diagnose debug coredump enable <daemon>
diagnose debug coredump enable-once <daemon>
diagnose debug coredump enable-pid <pid>
diagnose debug coredump list
diagnose debug coredump upload <daemon> <service> <ip> <username> <password> <directory>
```

Variable	Description
crash-pid <pid>	Crash running process for core dump.
delete <daemon>	Delete core dumps for a daemon.
disable <daemon>	Disable core dump for a daemon.
disable-pid <pid>	Disable core dump of running process.
enable <daemon>	Enable core dump for a daemon.
enable-once <daemon>	Enable core dump the next time a daemon starts (one time only).
enable-pid <pid>	Enable core dump of running process.
list	List core dumps.
upload <daemon> <service> <ip> <username> <password> <directory>	Upload core dumps for a daemon to the specified server.

debug crashlog

Use this command to manage crash logs.

Syntax

```
diagnose debug crashlog clear
diagnose debug crashlog read
```

Variable	Description
clear	Delete backtrace and core files.
read	Show the crash logs. This command is hidden.

debug disable

Use this command to disable debug.

Syntax

```
diagnose debug disable
```

debug dpm

Use this command to manage the deployment manager.

Syntax

```
diagnose debug dpm comm-trace {enable | disable | status}
diagnose debug dpm conf-trace {enable | disable | status}
diagnose debug dpm probe-device <ip>
```

Variable	Description
comm-trace {enable disable status}	Enable/disable a DPM to FortiGate communication trace, or view the status of it.
conf-trace {enable disable status}	Enable/disable a DPM to FortiGate configuration trace, or view the status of it.
probe-device <ip>	Check device status.

debug enable

Use this command to enable debug.

Syntax

```
diagnose debug enable
```

debug gui

Use these commands to enable or disable the GUI debug flag.

Syntax

```
diagnose debug gui {enable | disable}
```

debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

debug klog

Use this command to show all kernel logs.

Syntax

```
diagnose debug klog
```

debug reset

Use this command reset the debug level settings. All debug settings will be reset.

Syntax

```
diagnose debug reset
```

debug service

Use this command to view or set the debug level of various service daemons.

Syntax

```
diagnose debug service anonymous <integer>
diagnose debug service cdb <integer>
diagnose debug service cmdb <integer>
diagnose debug service csf <integer>
diagnose debug service dbcach <integer>
diagnose debug service dump
diagnose debug service dvmcmd <integer>
diagnose debug service dvmdb <integer>
diagnose debug service fazcmd <integer>
diagnose debug service fazconf <integer>
diagnose debug service httpd <integer>
diagnose debug service main <integer>
diagnose debug service rpc-auth <integer>
diagnose debug service rtm <integer>
diagnose debug service sys <integer>
diagnose debug service task <integer>
```

Variable	Description
<integer>	The debug level
dump	Dump services.

The anonymous, dbcach, dump, fazcmd, and rpc-auth commands are only available on hardware devices.

debug sysinfo

Use this command to show system information.

Syntax

```
diagnose debug sysinfo
```

debug sysinfo-log

Use this command to generate one system log information log file every two minutes.

Syntax

```
diagnose debug sysinfo-log {on | off}
```

debug sysinfo-log-backup

Use this command to backup all system information log files to an FTP server.

Syntax

```
diagnose debug sysinfo-log-backup <server> <filepath> <user> <password>
```

Variable	Description
<server>	Enter the FTP server IPv4 address.
<filepath>	Enter the path/filename to save the log to the FTP server.
<user>	Enter the user name for the FTP server.
<password>	Enter the password associated with the user name.

debug sysinfo-log-list

Use this command to show system information elogs.

Syntax

```
diagnose debug sysinfo-log-list <integer>
```

Variable	Description
<integer>	Display the last n elogs (default = 10).

debug timestamp

Use this command to enable/disable debug timestamp.

Syntax

```
diagnose debug timestamp {enable | disable}
```

debug vmd

Use this command to show all the VMD (Virtual Machine Daemon) logs.

Syntax

```
diagnose debug vmd
```

debug vminfo

Use this command to show VM license information.



This command is only available on FortiManager VM models.

Syntax

```
diagnose debug vminfo
```

dlp-archives

Use this command to manage the DLP archives.

Syntax

```
diagnose dlp-archives quar-cache list-all-process
diagnose dlp-archives quar-cache kill-process <pid>
diagnose dlp-archives rebuild-quar-db
diagnose dlp-archives remove
diagnose dlp-archives statistics {show | flush}
diagnose dlp-archives status
diagnose dlp-archives upgrade
```

Variable	Description
quar-cache list-all-process	List all processes that are using the quarantine cache.
quar-cache kill-process <pid>	Kill a process that is using the quarantine cache.

Variable	Description
rebuild-quar-db	Rebuild Quarantine Cache DB
remove	Remove all upgrading DLP archives.
statistics {show flush}	Display or flush the quarantined and DLP archived file statistics.
status	Running status.
upgrade	Upgrade the DLP archives.

docker

Use this command to view Docker status, clean up Docker data, and upgrade Docker management extensions.

Syntax

```
diagnose docker cleanup
diagnose docker reset {fortiaioops | fortiauthenticator | fortiportal | fortisigconverter
    | fortisoar | fortiwlm | fsmcollector | sdwancontroller | universalconnector}
diagnose docker status
diagnose docker upgrade {fortiaioops | fortiauthenticator | fortiportal |
    fortisigconverter | fortisoar | fortiwlm | fsmcollector | sdwancontroller |
    universalconnector} [tag]
```

Variable	Description
cleanup	Remove unused Docker data.
reset {fortiaioops fortiauthenticator fortiportal fortisigconverter fortisoar fortiwlm fsmcollector sdwancontroller universalconnector}	Reset a docker. Select to remove a docker volume and restart.
status	Show docker status.
upgrade {fortiaioops fortiauthenticator fortiportal fortisigconverter fortisoar fortiwlm fsmcollector sdwancontroller universalconnector} [tag]	Upgrade the specified management extension. Optionally, enter a tag to upgrade to (for debugging only).

Example

```
# diagnose docker status
fortiaioops : disabled
```

```
fortiauthenticator: disabled
fortiportal: disabled
fortisoar: disabled
fortisigconverter: disabled
fortiwlm: disabled
fsmcollector: disabled
sdwancontroller: disabled
universalconnector : disabled
```

dvm

Use the following commands for DVM related settings.

dvm adom

Use this command to list or clone ADOMs.

Syntax

```
diagnose dvm adom clone <adom> <new_adom>
diagnose dvm adom list
```

Variable	Description
clone <adom> <new_adom>	Clone an ADOM. Enter the name of the ADOM that will be cloned, and the name of the clone.
list	List ADOMs, state, product, OS version (OSVER), major release (MR), name, mode, VPN management, and IPS.

dvm capability

Use this command to set the DVM capability.

Syntax

```
diagnose dvm capability set {all | standard}
diagnose dvm capability show
```

Variable	Description
set {all standard}	Set the capability to all or standard.
show	Show what the capability is set to.

dvm chassis

Use this command to list chassis and supported chassis models.

Syntax

```
diagnose dvm chassis list
diagnose dvm chassis supported models
```

Variable	Description
list	List chassis.
supported-models	List supported chassis models.

dvm check-integrity

Use this command to check the DVM database integrity.

Syntax

```
diagnose dvm check-integrity
```

dvm csf

Use this command to print the CSF configuration.

Syntax

```
diagnose dvm csf <adom> <category>
```

Variable	Description
<adom>	The ADOM name.
<category>	The category: <ul style="list-style-type: none">all: Dump all CSF categoriesgroup: Dump CSF groupintf-role: Dump interface roleuser-device: Dump user device

dvm dbstatus

Use this command to print the database status.

Syntax

```
diagnose dvm dbstatus
```

dvm debug

Use this command to enable/disable debug channels, and show debug message related to DVM.

Syntax

```
diagnose dvm debug {enable | disable} <channel> <channel> <channel> <channel> <channel>
diagnose dvm debug trace [filter]
```

Variable	Description
{enable disable}	Enable/disable debug channels.
trace	Show the DVM debug message.
<channel>	The following channels are available: all, dvm_db, dvm_dev, shelfmgr, ipmi, lib, dvmcmd, dvmcore, gui, and monitor
<filter>	The following filters are available: all, dvm_db, dvm_dev, shelfmgr, ipmi, lib, dvmcmd, dvmcore, gui, and monitor.

dvm device

Use this command to list devices or objects referencing a device.

Syntax

```
diagnose dvm device delete <adom> <device>
diagnose dvm device dynobj <device>
diagnose dvm device list <device> <vdom>
diagnose dvm device monitor <device> <api>
diagnose dvm device object-reference <device> <vdom> <category> <object>
```

Variable	Description
delete <adom> <device>	Delete a device in a specific ADOM.
dynobj <device>	List dynamic objects on this device.
list <device> <vdom>	List devices. Optionally, enter a device or VDOM name.
monitor <device> <api>	JSON API for device monitor. Specify the device name and the monitor API name.
object-reference <device> <vdom> <category> <object>	List object reference. Specify the device name, VDOM, category (or <i>all</i> for all categories), and object.

Example

The following example shows the results of running the monitor command for WiFi clients.

```
FMG-VM64 # diagnose dvm device monitor FortiGate-VM64 wifi/client
```

Request :

```
{
  "id": 1473975442,
  "method": "exec",
  "params": [
    {
      "data": {
        "action": "get",
        "resource": "/api/v2/monitor/wifi/client",
        "target": [
          "adom/root/device/FortiGate-VM64"
        ]
      },
      "url": "sys/proxy/json"
    }
  ]
}
```

Response :

```
{
  "id": 1473975442,
  "result": [
    {
      "data": [
        {
          "response": {
            "action": "select",
            "build": 0113,
            "http_method": "GET",
            "name": "client",
            "path": "wifi",
            "results": null,
            "serial": "FGVMEV0000000000",
            "status": "success",
            "vdom": "root",
            "version": "v7.0.1"
          },
          "status": {
            "code": 0,
            "message": "OK"
          },
          "target": "FortiGate-VM64"
        }
      ],
      "status": {
        "code": 0,
        "message": "OK"
      },
      "url": "sys/proxy/json"
    }
  ]
}
```

dvm device-tree-update

Use this command to enable/disable device tree automatic updates.

Syntax

```
diagnose dvm device-tree-update {enable | disable}
```

Variable	Description
{enable disable}	Enable/disable device tree automatic updates.

dvm extender

Use these commands to list FortiExtender devices, synchronize FortiExtender data via JSON, and perform other actions.

Syntax

```
diagnose dvm extender copy-data-to-device <device>
diagnose dvm extender import-template <device> <extender id>
diagnose dvm extender list [device]
diagnose dvm extender reset-adom <adom> [clear-only] [skip-restart]
diagnose dvm extender set-template <device> <extender id> <template>
diagnose dvm extender sync-extender-data <device> [savedb] [syncadom] [task]
```

Variable	Description
copy-data-to-device <device>	Copy extender data (data plan and SIM profile) to the device. Enter the device name.
import-template <device> <extender id>	Import dataplan and SIM profile to the ADOM template. Enter the device name or ID, and the extender ID.
list [device]	List FortiExtender devices, or those connected to a specific device.
reset-adom <adom> [clear-only] [skip-restart]	Reset all extender data in the ADOM: <ul style="list-style-type: none"> • adom: Enter 104 for FortiCarrier, 130 for FortiFirewall, 134 for Unmanaged_Devices, and 3 for root <p>Optionally, use the following variables:</p> <ul style="list-style-type: none"> • clear-only: Do not sync extender data to the ADOM • skip-restart: Do not restart FortiManager after the operation
set-template <device> <extender id> <template>	Set template to the extender modem. Enter the device name or ID, extender ID, and template.
sync-extender-data <device> [savedb] [syncadom] [task]	Synchronize FortiExtender data by JSON. Optionally: save the data to the database, synchronize the ADOM, and/or create a task.

dvm fap

Use this command to list the FortiAP devices connected to a device.

Syntax

```
diagnose dvm fap list <devname>
```

Variable	Description
<devname>	The name of the device.

dvm fsw

Use this command to list the FortiSwitch devices connected to a device.

Syntax

```
diagnose dvm fsw list <devname>
```

Variable	Description
<devname>	The name of the device.

dvm group

Use this command to list groups.

Syntax

```
diagnose dvm group list
```

Variable	Description
list	List groups.

dvm lock

Use this command to print the DVM lock states.

Syntax

```
diagnose dvm lock
```

dvm proc

Use this command to list DVM process (dvmcmd) information.

Syntax

```
diagnose dvm proc list
```

dvm remove

Use this command to remove all unused IPS package files.

Syntax

```
diagnose dvm remove unused-ips-packages
```

dvm supported-platforms

Use this command to list supported platforms and firmware versions.

Syntax

```
diagnose dvm supported-platforms list <detail>
diagnose dvm supported-platforms mr-list
diagnose dvm supported-platforms fortiswitch
```

Variable	Description
list <detail>	List supported platforms by device type. Enter <i>detail</i> to show details with syntax support.
mr-list	List supported platforms by major release.
fortiswitch	List supported platforms in FortiSwitch manager.

dvm task

Use this command to repair or reset the task database.

Syntax

```
diagnose dvm task list <adom> <type>
diagnose dvm task repair
diagnose dvm task reset
```

Variable	Description
list <adom> <type>	List task database information.
repair	Repair the task database while preserving existing data where possible. The FortiManager will reboot after the repairs.
reset	Reset the task database to its factory default state. All existing tasks and the task history will be erased. The FortiManager will reboot after the reset.

dvm taskline

Use this command to repair the task lines.

Syntax

```
diagnose dvm taskline repair
```

Variable	Description
repair	Repair the task lines while preserving data wherever possible. The FortiManager will reboot after the repairs.

dvm transaction-flag

Use this command to edit or display DVM transaction flags.

Syntax

```
diagnose dvm transaction-flag [abort | debug | none]
```

Variable	Description
transaction-flag [abort debug none]	Set the transaction flag.

dvm workflow

Use this command to edit or display workflow information.

Syntax

```
diagnose dvm workflow log-list <adom_name> <workflow_session_ID>  
diagnose dvm workflow session-list [<adom_name>]
```

Variable	Description
log list <adom_name> <workflow_session_ID>	List workflow session logs.
session list [<adom_name>]	List workflow sessions.

faz-cdb

Use these commands for FortiAnalyzer database configuration related settings.

faz-cdb fix

Use this command to fix the FortiAnalyzer configuration database.

Syntax

```
diagnose faz-cdb fix check-report-folder <adom name>
diagnose faz-cdb fix fix-report-folder <adom name>
```

Variable	Description
check-report-folder	Check FortiAnalyzer configuration database report folders from the last upgrade backup.
fix-report-folder	Fix FortiAnalyzer configuration database report folders from the last upgrade.
<adom name>	Enter the ADOM name or enter <code>all</code> for all ADOMs.

faz-cdb reset

Use this command to reset the FortiAnalyzer configuration database.

Syntax

```
diagnose faz-cdb reset
```

faz-cdb upgrade

Use this command to upgrade the FortiAnalyzer configuration database.

Syntax

```
diagnose faz-cdb upgrade check-adom <adom name>
diagnose faz-cdb upgrade check-global
```

```

diagnose faz-cdb upgrade export-config <adom name> <service> <ip> <user> <password>
    <path/filename>
diagnose faz-cdb upgrade import-config <adom name> <service> <ip> <user> <password>
    <path/filename>
diagnose faz-cdb upgrade log
diagnose faz-cdb upgrade summary

```

Variable	Description
check-adom	Check the last ADOM upgrade result.
check-global	Check the last global upgrade result.
export-config	Export the FortiAnalyzer configuration database files.
import-config	Import the FortiAnalyzer configuration database files.
log	Display the FortiAnalyzer configuration database upgrade log.
summary	Display the FortiAnalyzer configuration database summary.
<adom name>	Enter the ADOM name or enter <code>all</code> for all ADOMs.
<service>	Enter the transfer protocol one of: <code>ftp</code> , <code>sftp</code> , or <code>scp</code> .
<ip>	Enter the server IP address. For FTP, the port can be specified by adding <code>:port</code> to the server IP address.
<user>	Enter a user name of the remote server.
<password>	Enter the password or <code>' - '</code> for user.
<path/filename>	Enter the path/ filename on remote server.

fgfm

Use this command to get installation session, object, and session lists.

Syntax

```

diagnose fgfm install-session
diagnose fgfm object-list
diagnose fgfm session-list <device ID>

```

Variable	Description
install-session	Get installations session lists.
object-list	Get object lists.
session-list <device ID>	Get session lists.

fmnetwork

Use the following commands for network related settings.

fmnetwork arp

Use this command to manage ARP.

Syntax

```
diagnose fmnetwork arp del <intf-name> <IP>
diagnose fmnetwork arp list
```

Variable	Description
del <intf-name> <IP>	Delete an ARP entry.
list	List ARP entries.

fmnetwork interface

Use this command to view interface information.

Syntax

```
diagnose fmnetwork interface detail <portX>
diagnose fmnetwork interface list <portX>
```

Variable	Description
detail <portX>	View a specific interface's details, for example: port1.
list <portX>	List all interface details.

fmnetwork netstat

Use this command to view network statistics.

Syntax

```
diagnose fmnetwork netstat list [-r]
diagnose fmnetwork netstat tcp [-r]
diagnose fmnetwork netstat udp [-r]
```

Variable	Description
list [-r]	List all connections, or use -r to list only resolved IP addresses.
tcp [-r]	List all TCP connections, or use -r to list only resolved IP addresses.
udp [-r]	List all UDP connections, or use -r to list only resolved IP addresses.

fmupdate

Use this command to diagnose update services.

Syntax

```

diagnose fmupdate check-disk-quota <string> <clean>
diagnose fmupdate crdb {generate | view}
diagnose fmupdate dbcontract [serial]
diagnose fmupdate del-device {fct | fds | fgd | fgc} <serial> <uid>
diagnose fmupdate del-log
diagnose fmupdate del-object {fds | fct | fgd | fgc | fgd-fgfq} <type> <version>
diagnose fmupdate del-serverlist {fct | fds | fgd | fgc}
diagnose fmupdate fct-getobject
diagnose fmupdate fds-dump {breg | fds-log | fect | fmgi | immx | oblt | srul}
diagnose fmupdate fds-get-downstream-device <serial>
diagnose fmupdate fds-getobject <filter type> <filter> <other options>
diagnose fmupdate fds-update-info
diagnose fmupdate fgd-asdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} {all |
    <serial>} <integer>
diagnose fmupdate fgd-asserver-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d}
diagnose fmupdate fgd-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fgd-dbver {wf | as | av-query}
diagnose fmupdate fgd-del-db {wf | as | av-query | file-query}
diagnose fmupdate fgd-get-downstream-device
diagnose fmupdate fgd-test-client <ip> <serial> <string> <integer>
diagnose fmupdate fgd-url-rating <ip> <serial> <version> <url>
diagnose fmupdate fgd-wfas-clear-log
diagnose fmupdate fgd-wfas-log {name | ip} <string>
diagnose fmupdate fgd-wfas-rate {wf | av | as_ip | as_url | as_hash}
diagnose fmupdate fgd-wfdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} {all |
    <serial>} {periods}
diagnose fmupdate fgd-wfserver-stat {top10sites | top10devices} {10m | 30m | 1h | 6h |
    12h | 24h | 7d}
diagnose fmupdate fgt-del-statistics
diagnose fmupdate fgt-del-um-db
diagnose fmupdate fmg-statistic-info
diagnose fmupdate fortitoken {seriallist | add | del} {add | del | required}
diagnose fmupdate get-device {fct | fds | fgd | fgc} <serial>
diagnose fmupdate list-object {fds | fct | fgd | fgc | fgd-fgfq} [type] [version]
diagnose fmupdate priority-download {clear | list | view}
diagnose fmupdate service-restart {fds | fct | fgd | fgc}
diagnose fmupdate show-bandwidth {fct | fgt | fml | faz} {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate show-dev-obj [serial_num]
diagnose fmupdate updatenow {fds | fgd | fct}

```

```

diagnose fmupdate update-status {fds | fct | fgd | fgc}
diagnose fmupdate view-configure {fds | fct | fgd | fgc}
diagnose fmupdate view-linkd-log {fct | fds | fgd | fgc}
diagnose fmupdate view-serverlist {fds | fct | fgd | fgc}
diagnose fmupdate view-service-info {fds | fgd}
diagnose fmupdate vm-license

```

Variable	Description
check-disk-quota <string> <clean>	Check the related directory size. <ul style="list-style-type: none"> <string>: Directory for the object. Use <code>export-import</code>, <code>fds</code>, <code>fgd</code>, or <code>all</code> as the string. <clean>: Clean the directory if necessary. Only cleans the export/import directory.
crdb {generate view}	Generate or view certificate files from the database.
dbcontract [serial]	Dumb the subscriber contract.
del-device {fct fds fgd fgc} <serial> <uid>	Delete a device. UID is required for FortiClient (fct) only.
del-log	Delete all the logs for FDS and FortiGuard update events.
del-object {fds fct fgd fgc fgd-fgq} <type> <version>	Remove all objects from the specified service. Optionally, enter the object type and version or time.
del-serverlist {fct fds fgd fgc}	Delete the server list file (fdni.dat) from the specified service.
fct-getobject	Get the versions of all FortiClient objects.
fds-dump {breg fds-log fect fmgi immx obl srul}	Dumb FDS files: <ul style="list-style-type: none"> <code>breg</code>: Dump the FDS beta serial numbers. <code>fds-log</code>: Dump the FDS svrd log. Optionally, enter a rolling number from 0 to 10. <code>fect</code>: Dump the FortiClient image file. Choose from the two available options of dumping the FortiClient file for the server or the client. <code>fmgi</code>: Dump FMGI (Object description details) file. <code>immx</code>: Dump the image upgrade matrix file. You can dump the IMMX files for FortiManager, FortiGate, or FortiCloud. <code>obl</code>: Dump the object list file. You can dump the object list files for FortiGate or FortiClient service. <code>srul</code>: Dump the FDS select filtering rules.
fds-get-downstream-device <serial>	Get information of all downstream FortiGate antivirus-IPS devices. Optionally, enter the device serial number.
fds-getobject <filter type> <filter> <other options>	Get the versions of all FortiGate objects for antivirus-IPS. <ul style="list-style-type: none"> <filter type>: Enter product or objid as the filter type. <filter>: Choose from the seven available filters. These filters are available only when you select product as your filter type. <other options>: Show the response in raw JSON format or show used-only objects.

Variable	Description
fds-update-info	Display scheduled update information.
fgd-asdevice-stat {10m 30m 1h 6h 12h 24h 7d} {all <serial>} <integer>	Display antispam device statistics for single or all devices. <ul style="list-style-type: none"> <integer>: Number of time periods to display (optional, default = 1).
fgd-asserver-stat {10m 30m 1h 6h 12h 24h 7d}	Display antispam server statistics.
fgd-bandwidth {1h 6h 12h 24h 7d 30d}	Display the download bandwidth.
fgd-dbver {wf as av-query}	Get the version of the database. Optionally, enter the database type.
fgd-del-db {wf as av-query file-query}	Delete FortiGuard database. Optionally, enter the database type.
fgd-get-downstream-device	Get information on all downstream FortiGate web filter and spam devices.
fgd-test-client <ip> <serial> <string> <integer>	Execute FortiGuard test client. Optionally, enter the hostname or IPv4 address of the FGD server, the serial number of the device, and the query number per second or URL.
fgd-url-rating <ip> <serial> <version> <url>	Rate URLs within the FortiManager database using the FortiGate serial number. Optionally, enter the category version and URL.
fgd-wfas-clear-log	Clear the FortiGuard service log file.
fgd-wfas-log {name ip} <string>	View the FortiGuard service log file. Optionally, enter the device filter type, and device name or IPv4 address.
fgd-wfas-rate {wf av as_ip as_url as_hash}	Get the web filter / antispam rating speed. Optionally, enter the server type.
fgd-wfdevice-stat {10m 30m 1h 6h 12h 24h 7d} <serialnum>	Display web filter device statistics. Optionally, enter a specific device's serial number.
fgd-wfserver-stat {top10sites top10devices} {10m 30m 1h 6h 12h 24h 7d}	Display web filter server statistics for the top 10 sites or devices. Optionally, enter the time frame to cover.
fgt-del-statistics	Remove all statistics (antivirus / IPS and web filter / antispam). This command requires a reboot.
fgt-del-um-db	Remove UM and UM-GUI databases. This command requires a reboot. Note: um.db is a sqlite3 database that update manager uses internally. It will store AV/IPS package information of downloaded packages. This command removes the database file information. The package is not removed. After the reboot, the database will be recreated. Use this command if you suspect the database file is corrupted.
fmg-statistic-info	Display statistic information for FortiManager and Java Client.

Variable	Description
fortitoken {seriallist add del} {add del required}	FortiToken related operations.
get-device {fct fds fgd fgc} <serialnum>	Get device information. Optionally, enter a serial number.
list-object {fds fct fgd fgc fgd-fgq} [type] [version]	List downloaded objects of linkd service. Optional enter the object type and version or time.
priority-download {clear list view}	Command for priority download: <ul style="list-style-type: none"> clear: view config. list: list object id of list. view: clear config.
service-restart {fds fct fgd fgc}	Restart the linkd service.
show-bandwidth {fct fgt fml faz} {1h 6h 12h 24h 7d 30d}	Display the download bandwidth for a device type over a specified time period.
show-dev-obj [serial_num]	Display an objects version of a device. Optionally, enter a serial number.
updatenow {fds fgd fct}	Update immediately.
update-status {fds fct fgd fgc}	Display the update status.
view-configure {fds fct fgd fgc}	Dump the running configuration.
view-linkd-log {fct fds fgd fgc}	View the linkd log file.
view-serverlist {fds fct fgd fgc}	Dump the server list.
view-service-info {fds fgd}	Display the service information.
vm-license	Dump the FortiGate VM license.

fortilogd

Use this command to view FortiLog daemon information.

Syntax

```
diagnose fortilogd lograte
diagnose fortilogd lograte-adom
diagnose fortilogd lograte-device [filter]
diagnose fortilogd lograte-total
diagnose fortilogd lograte-type
diagnose fortilogd logvol-adom
diagnose fortilogd msgrate
diagnose fortilogd msgstat [flush]
diagnose fortilogd status
```

Variable	Description
lograte	Display the log rate.
lograte-adom	Display log rate by ADOM.
lograte-device [filter]	Display log rate by device.
lograte-total	Display log rate by total.
lograte-type	Display log rate by type.
logvol-adom	Display the GB/day by ADOM.
msgrate	Display log message rate.
msgstat [flush]	Display or flush log message statuses.
status	Running status.

fwmanager

Use these commands to manage firmware.

Syntax

```

diagnose fwmanager cancel-schedule <taskid>
diagnose fwmanager fwm-log
diagnose fwmanager get-all-schedule [filter by status]
diagnose fwmanager get-dev-schedule <device> [filter by status]
diagnose fwmanager get-grp-schedule <group> [filter by status]
diagnose fwmanager image-delete <file>
diagnose fwmanager image-download <platform> <version>
diagnose fwmanager image-list <product>
diagnose fwmanager service-restart
diagnose fwmanager set-controller-schedule <device> <controller_id> <version> [flags]
    [date_time]
diagnose fwmanager set-dev-schedule <device> <version> [flags] [date_time]
diagnose fwmanager set-grp-schedule <group> <version> [flags] [date_time]
diagnose fwmanager show-dev-disk-check-status <device>
diagnose fwmanager show-dev-upgrade-path <device> <version> [debug]
diagnose fwmanager show-grp-disk-check-status <group>
diagnose fwmanager test-upgrade-path <platform> <from-version> <to-version> [debug]

```

Variable	Description
cancel-schedule <taskid>	Cancel an upgrade schedule for a device.
fwm-log	View the firmware manager log file.
get-all-schedule [filter by status]	Display all recorded upgrade schedules. Optionally, filter for the schedule (succeeded, failed, or unfinished).

Variable	Description
get-dev-schedule <device> [filter by status]	Get scheduled upgrades for the specified device. Optionally, filter for the schedule (succeeded, failed, or unfinished).
get-grp-schedule <group> [filter by status]	Get scheduled upgrades for the specified group name or ID. Optionally, filter for the schedule (succeeded, failed, or unfinished).
image-delete <file>	Delete a local image.
image-download <platform> <version>	Download the official image. Enter the platform name and version.
image-list <product>	Get the local firmware image list for the product: <ul style="list-style-type: none"> • FGT: FortiGate • FMG: FortiManager • FAZ: FortiAnalyzer • FAP: FortiAP • FSW: FortiSwitch • FXT: FortiExtender
service-restart	Restart the firmware manager server.
set-controller-schedule <device> <controller_id> <version> [flags] [date_time]	Create a controller upgrade schedule for a device.
set-dev-schedule <device> <version> [flags] [date_time]	Create an upgrade schedule for a device. The build number is only needed for special images, use 0 for regular images.
set-grp-schedule <group> <version> <flags> <date_time>	Create an upgrade schedule for a group.
show-dev-disk-check-status <device>	Show whether the device needs a disk check
show-dev-upgrade-path <device> <version> [debug]	Show the possible upgrade path
show-grp-disk-check-status <group>	Show whether the devices in the group need disk checks
test-upgrade-path <platform> <from-version> <to-version> [debug]	Show possible FortiGate upgrade paths.

ha

Use this command to view and manage high availability.

Syntax

```
diagnose ha check-data {start | stop | status}
diagnose ha data-check-report {read | delete}
diagnose ha dump-datalog
diagnose ha force-resync
diagnose ha stats
```

Variable	Description
check-data {start stop status}	Start/stop or check status of database hash and revision files.
data-check-report {read delete}	Read or delete the data check validation report.
dump-datalog	Dump the HA data log.
force-resync	Force HA to re-synchronize the configuration.
stats	Get HA statistics.

hardware

Use this command to view hardware information.

Syntax

```
diagnose hardware info
```

incident

Use this command to view incident attachment information

Syntax

```
diagnose incident attachment status <adom> <attachment type> [detail]
```

Variable	Description
attachment	Incident's Attachment.
status	Attachment status information.
<adom>	ADOM name or <code>all</code> for all ADOMs.
<attachment type>	The attachment type: <code>report</code> , <code>alertevent</code> , <code>note</code> , <code>file</code> , or <code>all</code> for all types.
[detail]	Show detailed information.

license

Use this command to check license information.

Syntax

```
diagnose license list
diagnose license update
```

Variable	Description
list	List the FortiAnalyzer license information.
update	Update the FortiAnalyzer license information.

log device

Use this command to view and manage device logging. If required, filter by device ID or ADOM.

Syntax

```
diagnose log device [<device-id> | adom] [adom-name | all | *]
```

Variable	Description
[<device-id> adom]	Optionally filter by device ID or ADOM.
[adom-name all *]	Optional filter by ADOM name when filtering by ADOM.

pm2

Use this command to print from and check the integrity of the policy manager database.

Syntax

```
diagnose pm2 check-integrity {all adom device global ips task ncldb}
diagnose pm2 print <log-type>
```

Variable	Description
check-integrity {all adom device global ips task ncldb}	Check policy manager database integrity. Multiple database categories can be checked at once.
print <log-type>	Print policy manager database log messages.

report

Use these commands to check the SQL database.

Syntax

```
diagnose report clean {ldap-cache | report-queue}
diagnose report status {pending | running}
```

Variable	Description
clean {ldap-cache report-queue}	Cleanup the SQL report queue or LDAP cache.
status {pending running}	Check status information on pending and running reports.

sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiManager units have a built-in sniffer. Packet capture on FortiManager units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output is printed to your CLI display until you stop it by pressing **CTRL + C**, or until it reaches the number of packets that you have specified to capture.



Packet capture can be very resource intensive. To minimize the performance impact on your FortiManager unit, use packet capture only during periods of minimal traffic, with a serial console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

Syntax

```
diagnose sniffer packet <interface> <filter> <verbose> <count> <Timestamp format>
```

Variable	Description
<interface>	Enter the name of a network interface whose packets you want to capture, such as <code>port1</code> , or type <code>any</code> to capture packets on all network interfaces.
<filter>	Enter either <code>none</code> to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as <code>'tcp port 25'</code> . Surround the filter string in quotes.

Variable	Description
	<p>The filter uses the following syntax:</p> <pre>'[[src dst] host {<host1_fqdn> <host1_ipv4>}] [and or] [[src dst] host {<host2_fqdn> <host2_ipv4>}] [and or] [[arp ip gre esp udp tcp] port <port1_int>] [and or] [[arp ip gre esp udp tcp] port <port2_int>]'</pre> <p>To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or only reply packets, indicate which host is the source and which is the destination.</p> <p>For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter:</p> <pre>'udp and port 1812 and src host 1.example.com and dst \ (2.example.com or 2.example.com \)'</pre>
<verbose>	<p>Enter one of the following numbers indicating the depth of packet headers and payloads to capture:</p> <ul style="list-style-type: none"> 1: print header of packets (default) 2: print header and data from IP of packets 3: print header and data from ethernet of packets (if available) <p>For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).</p>
<count>	<p>Enter the number of packets to capture before stopping.</p> <p>If you do not specify a number, the command will continue to capture packets until you press CTRL + C.</p>
<Timestamp format>	<p>Enter the timestamp format.</p> <ul style="list-style-type: none"> a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms otherwise: relative to the start of sniffing, ss.ms

Example 1

The following example captures the first three packets' worth of traffic, of any port number or protocol and between any source and destination (a filter of `none`), that passes through the network interface named `port1`. The capture uses a low level of verbosity (indicated by `1`).

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
Packet capture can be very resource intensive. To minimize the performance impact on your
FortiManager unit, use packet capture only during periods of minimal traffic, with a
serial console CLI connection rather than a Telnet or SSH CLI connection, and be
sure to stop the command when you are finished.# diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port `22` is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example 2

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by 1). Because the filter does not specify either host as the source or destination in the IPv4 header (`src` or `dst`), the sniffer captures both forward and reply traffic.

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses the control key + C. The sniffer then confirms that five packets were seen by that network interface.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
Packet capture can be very resource intensive. To minimize the performance impact on your
FortiManager unit, use packet capture only during periods of minimal traffic, with a
serial console CLI connection rather than a Telnet or SSH CLI connection, and be
sure to stop the command when you are finished. # diag sniffer packet port1 'host
192.168.0.2 or host 192.168.0.1 and tcp port 80' 1
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example 3

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IPv4 address. The capture uses a high level of verbosity (indicated by 3).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses the control key + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
Packet capture can be very resource intensive. To minimize the performance impact on your
FortiManager unit, use packet capture only during periods of minimal traffic, with a
serial console CLI connection rather than a Telnet or SSH CLI connection, and be
sure to stop the command when you are finished. # diag sniffer port1 'tcp port 443'
3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 .....E.
0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f.....
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or.....
0x0040 86bb 0000 0000 0103 0303 .....
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encoding other than US-ASCII. It is usually preferable to analyze the output by loading it into a network protocol analyzer application such as Wireshark (<http://www.wireshark.org/>).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software, such as [PuTTY](#)
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software, such as [Wireshark](#)

To view packet capture output using PuTTY and Wireshark:

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the Fortinet appliance using either a local serial console, SSH, or Telnet connection.
3. Enter the packet capture command, such as:

```
diagnose sniffer packet port1 'tcp port 541' 3 100
```

but do not press Enter yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*. A dialog appears where you can configure PuTTY to save output to a plain text file.
5. In the *Category* tree on the left, go to *Session > Logging*.
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)
8. Click *Apply*.
9. Press Enter to send the CLI command to the FortiMail unit, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press the `control key + C` to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.
13. Delete the first and last lines, which look something like this:

```
===== PuTTY log 2022.09.29 08:03:40 =====  
Fortinet-2000 #
```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.
14. Convert the plain text file to a format recognizable by your network protocol analyzer application.
You can convert the plain text file to a format (`.pcap`) recognizable by Wireshark using the `fgt2eth.pl` Perl script. To download `fgt2eth.pl`, see the [Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer](#).



The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

To use fgt2eth.pl, open a command prompt, then enter a command such as the following:

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt

- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved

15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

For additional information on packet capture, see the [Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer](#).

sql

Use these commands to diagnose the SQL database.

Syntax

```
diagnose sql config auto-cache-delay [set <seconds>| reset]
diagnose sql config debug-filter [set | test] <daemon> <string>
diagnose sql config deferred-index-timespan [set <value>]
diagnose sql config hcache-agg-step [reset | set <integer>]
diagnose sql config hcache-base-trim-interval [reset | set <integer>]
diagnose sql config hcache-max-fv-row [reset | set <integer>]
diagnose sql config hcache-max-rpt-row [reset | set <integer>]
diagnose sql config sampling-max-row [reset | set <integer>]
diagnose sql config sampling-status [reset | set <integer>]
diagnose sql config sampling-type [reset | set <integer>]
diagnose sql debug hcache-agg dbgoff
diagnose sql debug hcache-agg dbgon
diagnose sql debug hcache-agg delete
diagnose sql debug hcache-agg show [<filter>][<NUM>]
diagnose sql debug hcache-agg upload {ftp | sftp} <host> <dir> <user name> <password>
diagnose sql debug logview dbgoff
diagnose sql debug logview dbgon <level value>
diagnose sql debug logview delete
diagnose sql debug logview show [<filter>] [<NUM>]
diagnose sql debug logview upload {ftp | sftp} <host> <dir> <user name> <password>
diagnose sql debug sqlqry dbgoff
diagnose sql debug sqlqry dbgon <level value>
diagnose sql debug sqlqry delete
diagnose sql debug sqlqry show [<filter>][<NUM>]
diagnose sql debug sqlqry upload {ftp | sftp} <host> <dir> <user name> <password>
diagnose sql hcache add-task agg <adom> <norm-query-hash> <agg-level> <timestamp> <num-
  of-days>
diagnose sql hcache add-task agg-update <adom> <hid>
diagnose sql hcache dump-task <filter>
diagnose sql hcache list <adom> <query-hash/tag> <filter> <detail>
diagnose sql hcache plan <adom> <start-time> <end-time> <query-tag/norm-qry-hash/sql>
  <is-fortiview> <max-time-scale>
diagnose sql hcache rebuild-both <start-time> <end-time>
diagnose sql hcache rebuild-fortiview <start-time> <end-time>
diagnose sql hcache rebuild-report <start-time> <end-time>
diagnose sql hcache rebuild-status
diagnose sql hcache show hcache <adom> <id>
```

```

diagnose sql hcache show hcache-query <adom> <norm-qry-hash>
diagnose sql hcache show hcache-res-tbl <adom> <res-tbl-id>
diagnose sql hcache show time <time> <time> <time> <time>
diagnose sql hcache status {all | all-summary | <adom>}
diagnose sql process kill <pid>
diagnose sql process list [full]
diagnose sql remove {hcache <adom> [fast] | query-cache | rebuild-db-flag | tmp-tabe}
diagnose sql show {db-size | hcache-size | log-filters | log-stfile <device-id> <vdom> |
    policy info <adom> }
diagnose sql status {rebuild-adom <adom> | rebuild-db | run_sql_rpt | sqlplugind |
    sqlreportd}
diagnose sql upload {ftp | tftp} <host> <directory> <user_name> <password>

```

Variable	Description
config auto-cache-delay [set <seconds> reset]	Show, set, or reset the auto-cache delay, in seconds (default = 300).
config debug-filter {set test} <daemon> <string>	Show sqlplugind and sqlreportd debug filter. Enter sqlplugind, sqlreportd or both as the <daemon>. Enter the filter string.
config deferred-index-timespan [set <value>]	View or set the time span for the deferred index (default = 10000).
config hcache-agg-step [reset set <integer>]	Show, set, or reset the hcache aggregation step (default = 10).
config hcache-base-trim-interval [reset set <integer>]	Show, set, or reset the hcache base trim interval (default = 172800).
config hcache-max-fv-row [reset set <integer>]	Show, set, or reset max row number for fortiview hcache (default = 100000).
config hcache-max-rpt-row [reset set <integer>]	Show, set, or reset max row number for report hcache (default = 18000).
config sampling-max-row [reset set <integer>]	Show, set, or reset max row number for sampling (default = 1000000).
config sampling-status [reset set <integer>]	Show, set, or reset the sampling status. Enter 0 for disabling and 1 for enabling the sample status (default = 1).
config sampling-type [reset set <integer>]	Show, set, or reset the type of sampling (default = 0).
debug hcache-agg dbgoff	Disable hcache-agg debug output.
debug hcache-agg dbgon	Enable hcache-agg debug output.
debug hcache-agg delete	Delete hcache-agg debug file.
debug hcache-agg show [<filter>] [<NUM>]	Show the last 10 lines of the hcache-agg debug file. Set filter for the debug file, and show the last NUM lines of the debug file. The filter and NUM variables optional.

Variable	Description
debug hcache-agg upload {ftp sftp} <host> <dir> <user name> <password>	Upload hcache-agg debug file to FTP or SFTP server. Enter host IP address, directory, user name, and password.
debug logview dbgoff	Disable Log view debug output.
debug logview dbgon <level value>	Enable log view debug output. Set log view debug level (1-5). Default level is 1.
debug logview delete	Delete log view debug file.
debug logview show [<filter>] [<NUM>]	Show the last 10 lines of the Log view debug file. Set filter for debug file, and show last NUM lines of the debug file. The filter and NUM variables are optional.
debug logview upload {ftp sftp} <host> <dir> <user name> <password>	Upload log view debug file to FTP or SFTP server. Enter host IP address, directory, user name, and password.
debug sqlqry dbgoff	Disable SQL query debug output.
debug sqlqry dbgon <level value>	Enable SQL query debug output. Set SQL query debug level (1-5). The default level is 1. Note: When the debug level is 5, the final SQL running in sqlreportd will show in the debug output as well.
debug sqlqry delete	Delete the SQL query debug file.
debug sqlqry show [<filter>] [<NUM>]	Show the last 10 lines of the SQL query debug file. Set filter for the debug file, and show the last NUM lines of the debug file. The filter and NUM variables are optional.
debug sqlqry upload {ftp sftp} <host> <dir> <user name> <password>	Upload SQL query debug file to FTP or SFTP server. Enter host IP address, directory, user name, and password.
hcache add-task agg <adom> <norm-query-hash> <agg-level> <timestamp> <num-of-days>	Add an hcache agg task: <ul style="list-style-type: none"> • adom: The ADOM name. • norm-query-hash: The normalized query hash. • agg-level: The aggregation level. • timestamp: The timestamp (format = yyyy-mm-dd hh:mm:ss). • num-of-days: The number of days (1, 3, or 30).
hcache add-task agg-update <adom> <hid>	Add an hcache agg update task: <ul style="list-style-type: none"> • adom: The ADOM name. • hid: The hcache agg ID.
hcache dump-task <filter>	Dump hcache tasks. Enter the task filter.
hcache list <adom> <query-hash/tag> <filter> <detail>	List hcache tasks: <ul style="list-style-type: none"> • adom: The ADOM name. • query-hash/tag: The hash or tag filter query, or all for all hcache tasks. • filter: Narrow down the hcache list search result by using a filter. The filter

Variable	Description
	<p>keywords include:</p> <ul style="list-style-type: none"> status: The hcache status. 0(Ready), 1(Ready-Loss), 2(In-Building), 3(Error), 4(Invalid-SQL), 5(No-Data), 6(Not-Ready). fv_flag: List FortiView/report only. 1(fortiview), 0(report). sql: The SQL query match. '*' for wildcard, e.g. *select*. time_start: Start of the log time. format: yyyy-mm-dd hh:MM:ss. time_end: End of the log time. format: yyyy-mm-dd hh:MM:ss. <p>The following shows an example of the variable <filter>:</p> <ul style="list-style-type: none"> "status=0,1,5 sql=\"*srcip, dstip*\" time_start>=\"2020-11-01 00:00:00\" time_end<=\"2020-11-30 23:59:59\"". <p>Enter "" for no filter.</p> <ul style="list-style-type: none"> detail: Show detailed information.
hcache plan <adom> <start-time> <end-time> <query-tag/norm-qry-hash/sql> <is-fortiview> <max-time-scale>	<p>Plan hcache:</p> <ul style="list-style-type: none"> adom: The ADOM name. start-time: The start time (format: yyyy-mm-dd hh:mm:ss). end-time: The end time (format: yyyy-mm-dd hh:mm:ss). query-tag/norm-qry-hash/sql: The query tag, normalized query hash, or sql statement. is-fortiview: Enter 1 for FortiView, or 0 for report. max-time-scale: Maximum timescale.
hcache rebuild-both <start-time> <end-time>	Rebuild hcache for both report and FortiView. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
hcache rebuild-fortiview <start-time> <end-time>	Rebuild hcache for FortiView only. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
hcache rebuild-report <start-time> <end-time>	Rebuild hcache for report only. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
hcache rebuild-status	Show report hcache rebuild/check status.
hcache show hcache <adom> <id>	Show hcache information. Enter the ADOM name and hcache ID.
hcache show hcache-query <adom> <norm-qry-hash>	Show hcache query information. Enter the ADOM name and the normalized query hash.
hcache show hcache-res-tbl <adom> <res-tbl-id>	Show hcache result table information. Enter the ADOM name and the result table ID.
hcache show time <time> <time> <time> <time>	Show hcache time. Enter up to four timestamps.
hcache status {all all-summary <adom>}	Show detailed hcache information. Enter the ADOM name, <code>all-summary</code> for the summary, or <code>all</code> for all ADOMs.

Variable	Description
process kill <pid>	Kill a running query.
process list [full]	List running query processes.
remove {hcache <adom> [fast] query-cache rebuild-db-flag tmp-table}	Remove the selected information: <ul style="list-style-type: none"> hcache: Remove the hcache tables created for the SQL report. Enter <i>fast</i> to not remove the hcache result tables. query-cache: Remove the SQL query cache for log search. rebuild-db-flag: Remove the rebuild database flag. The system will exit the rebuild database state. tmp-table: Remove the SQL database temporary tables.
show {db-size hcache-size log-filters log-stfile <device-id> <vdom> policy-info <adom>}	Show the database, hcache size, log filters, or log status file: <ul style="list-style-type: none"> db-size: Show database size. hcache-size: Show hcache size. log-filters: Show log view searching filters. log-stfile: Show logstatus file for the specified device (for HA cluster, input the member's serial number) and VDOM. policy-info: Show policy uuid and name map.
status {rebuild-adom <adom> rebuild-db run_sql_rpt sqlplugind sqlreportd}	Show the status: <ul style="list-style-type: none"> rebuild-adom <adom>: Show SQL log database rebuild status of ADOMs. rebuild-db: Show SQL log database rebuild status. run-sql-rpt: Show run_sql_rpt status. sqlplugind: Show sqlplugind status. sqlreportd: Show sqlreportd status.
upload {ftp tftp} <host> <directory> <user_name> <password>	Upload sqlplugind messages / pgsvr logs with FTP or TFTP.

svctools

Import or export the FortiAnalyzer configuration (when FortiAnalyzer features are enabled), and run JSON files.

Syntax

```
diagnose svctools export local
diagnose svctools export remote <ip> <string> <username> <password>
diagnose svctools import local name <adom>
diagnose svctools import remote <ip> <string> <username> <password> <adom>
diagnose svctools run local filename
diagnose svctools run remote <ip> <string> <username> <password>
```

Variable	Description
export local	Export the configuration locally.
export remote <ip> <string> <username> <password>	Export the configuration to a remote FTP server.
import local name <adom>	Import a local configuration from the specified ADOM.
import remote <ip> <string> <username> <password> <adom>	Import a remote configuration from an FTP server to the specified ADOM.
run local filename	Run a local JSON file on the target.
run remote <ip> <string> <username> <password>	Run a remote file from an FTP server.

Example

```
# diagnose svctools export local
Export FortiAnalyzer(121), 1 of 15 ADOM.
Export FortiAuthenticator(137), 2 of 15 ADOM.
Export FortiCache(125), 3 of 15 ADOM.
Export FortiCarrier(117), 4 of 15 ADOM.
Export FortiClient(127), 5 of 15 ADOM.
Export FortiDDoS(135), 6 of 15 ADOM.
Export FortiMail(119), 7 of 15 ADOM.
Export FortiManager(131), 8 of 15 ADOM.
Export FortiNAC(141), 9 of 15 ADOM.
Export FortiProxy(139), 10 of 15 ADOM.
Export FortiSandbox(133), 11 of 15 ADOM.
Export FortiWeb(123), 12 of 15 ADOM.
Export Syslog(129), 13 of 15 ADOM.
Export others(115), 14 of 15 ADOM.
Export root(3), 15 of 15 ADOM.
Exported to /var/tmp/svctools_export
```

system

Use the following commands for system related settings.

system admin-session

Use this command to view and kill log in sessions.

Syntax

```
diagnose system admin-session kill <sid>
diagnose system admin-session list
```

```
diagnose system admin-session status
```

Variable	Description
kill <sid>	Kill a current session. <ul style="list-style-type: none"> <sid>: Session ID
list	List log in sessions.
status	Show the current session.

system disk

Use this command to view disk diagnostic information.



Only `usage` is available on FortiManager-VM. Other `disk` related commands are only available on the hardware-based FortiManager.

Syntax

```
diagnose system disk attributes
diagnose system disk disable
diagnose system disk enable
diagnose system disk health
diagnose system disk info
diagnose system disk errors
diagnose system disk usage <parameter> <parameter> <parameter> <parameter> <parameter>
    <parameter> <parameter> <parameter> <parameter> <parameter>
```

Variable	Description						
attributes	Show vendor specific SMART attributes.						
disable	Disable SMART support.						
enable	Enable SMART support.						
health	Show the SMART health status.						
info	Show the SMART information.						
errors	Show the SMART error logs.						
usage <parameter> ... <parameter>	Display the disk usage. Enter a parameter.						
	<table> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>-a</td><td>Show file sizes.</td></tr> <tr> <td>-L</td><td>Follow all symlinks.</td></tr> </table>	Parameter	Description	-a	Show file sizes.	-L	Follow all symlinks.
Parameter	Description						
-a	Show file sizes.						
-L	Follow all symlinks.						

Variable	Description	
	Parameter	Description
	-H	Follow symlinks on the command line.
	-d N	Limit output to directories (and files with -a) of depth < N.
	-c	Show the grand total.
	-l	Count sizes many times if hard linked.
	-s	Display only a total for each argument.
	-x	Skip directories on different file systems.
	-h	Sizes in human readable format (e.g., 1K 243M 2G).
	-m	Sizes in megabytes.
	-k	Sizes in kilobytes (default).

system export

Use this command to export logs.

Syntax

```

diagnose system export crashlog <ftp server> <username> <password> <directory> <filename>
diagnose system export dminstallog <devid> <ftp server> <username> <password> <directory>
<filename>
diagnose system export fmwslog {ftp | sftp} <type> <(s)ftp server> <username> <password>
<directory> <filename>
diagnose system export raidlog <ftp server> <username> <password> [remote path]
[filename]
diagnose system export umlog {ftp | sftp} <type> <(s)ftp server> <username> <password>
<directory> <filename>
diagnose system export upgradelog <ftp server> <username> <password> <directory>
<filename>
diagnose system export vartmp <ftp server> <username> <password> <directory> <filename>

```

Variable	Description
crashlog <ftp server> <username> <password> <directory> <filename>	Export the crash log.
dminstallog <devid> <ftp server> <username> <password> <directory> <filename>	Export the deployment manager install log.
fmwslog {ftp sftp} <type> <(s)ftp server> <username> <password> <directory> <filename>	Export the web service log files. The type is the log file prefix and can be: SENT, RECV, or TEST.

Variable	Description
raidlog <ftp server> <username> <password> [remote path] [filename]	Export the RAID log. This command is only available on devices that support RAID.
umlog {ftp sftp} <type> <(s)ftp server> <username> <password> <directory> <filename>	Export the update manager and firmware manager log files. The type options are: fdslinkd, fctlinkd, fgdlinkd, fgdsvr, update, service, misc, umad, and fwmlinkd
upgradelog <ftp server> <username> <password> <directory> <filename>	Export the upgrade error log.
vartmp <ftp server> <username> <password> <directory> <filename>	Export the system log files in /var/tmp.

system flash

Use this command to diagnose the flash memory.

Syntax

```
diagnose system flash list
```

Variable	Description
list	List flash images. The information displayed includes the image name, version, total size (KB), used (KB), percent used, boot image, and running image.

system fsck

Use this command to check and repair the filesystem.

Syntax

```
diagnose system fsck harddisk
diagnose system fsck reset-mount-count
```

Variable	Description
harddisk	Check and repair the file system, then reboot the system.
reset-mount-count	Reset the mount-count of the disk on the next reboot.

system geoup

Use these commands to get geographic IP information.

FortiManager uses a [MaxMind GeoLite](#) database of mappings between geographic regions and all public IPv4 addresses that are known to originate from them.

Syntax

```
diagnose system geoip dump
diagnose system geoip info
diagnose system geoip ip <ip>
```

Variable	Description
dump	Display all geographic IP information.
info	Display a brief geography IP information.
ip <ip>	Find the specified IP address' country.

Example

Find the country of the IP address 4.3.2.1:

```
FMG-VM64 # diagnose system geoip ip 4.3.2.1
4.3.2.1 : US - United States
```

system geoip-city

Use these commands to get geographic IP information at a city level.

Syntax

```
diagnose system geoip-city info
diagnose system geoip-city ip <ip>
```

Variable	Description
info	Display geographic IP information.
ip <ip>	Find the specified IP address' city.

system interface

Use this command to diagnose the interface.

Syntax

```
diagnose system interface segmentation-offload <intf-name> <action>
```

Variable	Description
segmentation-offload <intf-name> <action>	Print/set segmentation-offload for all interfaces: <ul style="list-style-type: none"><intf-name>: Enter the interface name (or enter <code>all</code> for all interfaces)<action>: Enter one of <code>show/on/off</code> to show or switch on/off interfaces

system mapserver

Use this command to access the map server information.

Syntax

```
diagnose system mapserver get
diagnose system mapserver reset
diagnose system mapserver set <url>
diagnose system mapserver test
```

Variable	Description
get	Get the current map server.
reset	Reset the map server session.
set <url>	Set the map server. Enter the map server URL.
test	Test the map server connection.

system ntp

Use this command to list NTP server information.

Syntax

```
diagnose system ntp status
```

Variable	Description
status	List NTP server information.

system print

Use this command to print server information.

Syntax

```
diagnose system print certificate
diagnose system print connector [adom] <server_type> <server>
diagnose system print cpuinfo
diagnose system print df [arg0] [arg1] [arg2] .... [arg9]
diagnose system print hosts
diagnose system print interface <interface>
diagnose system print loadavg
diagnose system print netstat
diagnose system print partitions
diagnose system print route
diagnose system print rtcache
diagnose system print slabinfo
diagnose system print sockets
diagnose system print uptime
```

Variable	Description
certificate	Print the IPsec certificate.
connector [adom] <server_type> <server>	Print connector information. Enter the ADOM name, or Global, the server type (pxGrid, clearpass, or nsx), and then the server name.
cpuinfo	Print the CPU information.
df [arg0] [arg1] [arg2] [arg9]	Print the file system disk space usage. Optionally, enter arguments.
hosts	Print the static table lookup for host names.
interface <interface>	Print the specified interface's information.
loadavg	Print the average load of the system.
netstat	Print the network statistics for active Internet connections (servers and established).
partitions	Print the disk partition information.
route	Print the main route list.
rtcache	Print the contents of the routing cache.
slabinfo	Print the slab allocator statistics.
sockets	Print the currently used socket ports.
uptime	Print how long the system has been running.

system process

Use this command to view and kill processes.

Syntax

```
diagnose system process kill -<signal> <pid>
diagnose system process killall {Scriptmgr | deploymgr | fgfm}
```

```
diagnose system process list
```

Variable	Description
kill -<signal> <pid>	Kill a process: <ul style="list-style-type: none">• -<signal>: Signal name or number, such as -9 or -KILL• <pid>: Process ID
killall {Scriptmgr deploymgr fgfm}	Kill all the related processes.
list	List all processes running on the FortiManager. The information displayed includes the PID, user, VSZ, stat, and command.

system raid

Use this command to view RAID information.



This command is only available on FortiManager models that support RAID.

Syntax

```
diagnose system raid hwinfomdiagnose system raid status
```

Variable	Description
hwinfomdiagnose system raid status	Show RAID controller hardware information.
status	Show RAID status.

system route

Use this command to help diagnose routes. The listed information includes the destination IP, gateway IP, netmask, flags, metric, reference, use, and interface for each IPv4 route.

Syntax

```
diagnose system route list
```

system route6

Use this command to help diagnose routes. The listed information includes the destination IP, gateway IP, netmask, flags, metric, reference, use, and interface for each IPv6 route.

Syntax

```
diagnose system route6 list
```

system server

Use this command to start the FortiManager server.

Syntax

```
diagnose system server start
```

test

Use the following commands to test the FortiManager.

test application

Use this command to test applications. Multiple variables can be entered for each command.

Syntax

```
diagnose test application apiproxyd <integer> <integer> ... <integer>
diagnose test application clusterd <integer> <integer> ... <integer>
diagnose test application execmd <integer> <integer> ... <integer>
diagnose test application fabricsyncd <integer> <integer> ... <integer>
diagnose test application fazcfgd <integer> <integer> ... <integer>
diagnose test application fazmaild <integer> <integer> ... <integer>
diagnose test application faznotify <integer> <integer> ... <integer>
diagnose test application fazsvcd <integer> <integer> ... <integer>
diagnose test application fazwatchd <integer> <integer> ... <integer>
diagnose test application filefwd <integer> <integer> ... <integer>
diagnose test application fileparsed <integer> <integer> ... <integer>
diagnose test application fortilogd <integer> <integer> ... <integer>
diagnose test application logfiled <integer> <integer> ... <integer>
diagnose test application logfwd <integer> <integer> ... <integer>
diagnose test application log-fetchd <integer> <integer> ... <integer>
diagnose test application miglogd <integer> <integer> ... <integer>
diagnose test application oftpd <integer> <integer> ... <integer>
diagnose test application rptchkd <integer> <integer> ... <integer>
diagnose test application scansched <integer> <integer> ... <integer>
diagnose test application siemagentd <integer> <integer> ... <integer>
diagnose test application siemdbd <integer> <integer> ... <integer>
diagnose test application snmpd <integer> <integer> ... <integer>
diagnose test application sqllogd <integer> <integer> ... <integer>
diagnose test application sqlplugind <integer> <integer> ... <integer>
diagnose test application sqlreportd <integer> <integer> ... <integer>
diagnose test application sqlrptcached <integer> <integer> ... <integer>
```

```
diagnose test application syncsched <integer> <integer> ... <integer>
diagnose test application uploadd <integer> <integer> ... <integer>
```

Variable	Description
apiproxyd <integer> ...	API proxy daemon test usage: <ul style="list-style-type: none"> 1: show PID 2: show statistics and state 20: fsa tracer log request 21: fsa tracer log request 99: restart daemon
clusterd <integer> ...	Clusterd daemon test usage: <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: Thread pool status 3: Log Cluster core 4: Devices cache module 5: Logging Topology module 6: Avatar uploading module 7: Meta-CSF uploading module 9: Tunnel module 10: oftpd file fwd module 11: Service module 97: HA module 98: Monitor status 99: Restart clusterd 100: Restart clusterd and clusterd-monitor 102: Various tests
execcmd <integer> ...	Execcmd daemon test usage: <ul style="list-style-type: none"> 1: show PID 2: show statistics and state 3: reset statistics and state 4: show statistics of cmd tool 5: reset statistics of cmd tool 99: restart daemon
fabricsyncd <integer> ...	Fabricsyncd daemon test usage.
fazcfgd <integer> ...	Fazcfg daemon test usage: <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show statistics 3: show merged ca info 40: DVM cache diag info 41: CSF diag info 42: IntfRole diag info 43: reload csf info in devtable 44: show log device group stats 45: check log device group

Variable	Description
	<ul style="list-style-type: none"> • 48: test update link prefixes file • 49: test update webfilter categories description file • 50: test get app icon • 51: test update app logo files • 52: dvm call stats • 53: dvm call stats clear • 54: check ips/app meta-data update • 55: log disk readahead get • 56: log disk readahead toggle • 57: fix redis service • 58: check redis service • 59: test update faz license • 60: test fortigate restful api • 65: log aggregation server stats • 66: log aggregation server stats toggle (debug only) • 82: list avatar meta-data • 83: rebuild avatar meta-data table • 84: rebuild ips meta-data table • 85: rebuild app meta-data table • 86: rebuild FortiClient Vulnerability meta-data table • 88: update ffdb meta-data • 90: use built-in TIDB package and disable updating it • 91: enable updating TIDB package • 92: disable updating TIDB package • 93: switch on/off adom default report schedule • 94: switch on/off report schedule by name • 99: restart daemon <p>This test is only functional when FortiAnalyzer features are enabled</p>
fazmaild <integer> ...	<p>Fazmaild daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID and daemon status • 2: show runtime status • 90: pause sending mail • 91: resume sending mail • 99: restart fazmaild daemon <p>This test is only functional when FortiAnalyzer features are enabled</p>
faznotify <integer> ...	<p>Faznotify daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show faznotify statistics [clear] • 10: send a faznotify <adom> <id> <send-data> • 20: show active channel • 29: delete active channel <adom> <id> • 30: pause active channel <seconds>

Variable	Description
	<ul style="list-style-type: none"> 99: restart <p>This test is only functional when FortiAnalyzer features are enabled</p>
fazsvcd <integer> ...	<p>Fazsvcd daemon test usage:</p> <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show daemon stats and status 3: list async search threads 4: dump async search slot info 5: show cache builder stats 6: dump cache builder playlist 7: dump log search filters 10: show database log stats aggregated per day 11: show received log stats aggregated per day 20: show avatar request stats 50: enable or disable cache builder 51: enable or disable auto custom index 57: Fazbroker stats 58: reset Fazbroker stats 60: rawlog idx cache test 61: logbrowse cache stats 62: FortiView Session Stats 70: show stats for device vdom cache 71: show stats for remote fortiview and reports 72: show filterable and sortable fields for fortiview. <v3.0 view name> 75: data masking test: <passwd> <plaint test> <1 0 (high secure)> [do_unmasking] 76: fazsvcd fabric service diagnostics 99: restart daemon 100: log FAZ debugs 101: Close FAZ debug log 200: gui api test 201: diag for jsonrpc .. <p>This test is only functional when FortiAnalyzer features are enabled</p>
fazwatchd <integer> ...	<p>Fazwatchd daemon test usage:</p> <ul style="list-style-type: none"> 1: show process summary and report stats 2: show playbook stats 4: show nac asset stats 5: show playbook task log 6: show ha command execution stats 7: show casb metadata stats 99: restart daemon <p>This test is only functional when FortiAnalyzer features are enabled</p>
filefwd <integer> ...	<p>Filefwd daemon test usage:</p> <ul style="list-style-type: none"> 1: show daemon PID

Variable	Description
	<ul style="list-style-type: none"> • 2: show daemon stats • 3: show threads stats • 99: restart daemon
fileparsed <integer> ...	Fileparsed daemon test usage: <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: show devtable local cache status • 4: reload devtable local cache. • 11: show FortiGate interface cache status • 12: show FortiGate interface parsers status • 13: show FortiGate interface archived files disk usage • 14: show FortiGate interface archived files retention days • 15: show FortiGate interface info • 16: show total number of interfaces trimmed from database • 98: rebuild FortiGate interface SQL tables • 99: restart daemon
fortilogd <integer> ...	Fortilogd Diag test usage: <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: dump message status • 3: logstat status • 4: client devices status • 5: print log received • 6: switch on/off debug messages • 7: log forwarding prep status • 8: show logUID info • 9: device log cache reloading status • 10: dz_client cache status • 11: file stats • 12: stop/restart receiving logs • 14: show cached adom lograte status • 15: show cached adom log volume status • 16: show appevent logs receiving info • 17: show logging rate of the system and per-device • 90: show or set fortilogd working status • 95: show runtime logs. option format: pid=0:current,-1:all,PID duration=DURA filter=STR • 98: memory check • 99: restart fortilogd
logfiled <integer> ...	Logfile daemon test usage: <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 4: show ADOM statistics

Variable	Description
	<ul style="list-style-type: none"> • 5: show device statistics • 6: show auto-del statistics • 7: show log file disk usage • 8: update log file disk usage • 9: show inode usage • 10: enable or disable debug filter of device and vdom • 11: du cache diag commands • 90: reset statistics and state • 91: force to preen content files info • 99: restart daemon
logfwd <integer> ...	<p>Logfwd daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ..) • 2: Dump thread-pool status • 3: Dump log-forward configurations • 4: Dump log-forwarding status • 5: Overall and converter stats • 6: Dump HA CID info • 7: show runtime logs. option format: pid=0:current,-1:all,PID duration=DURATION filter=STR • 8: show cfile list status [all: for all cfiles] • 9: show max duration of loss in memory mode, 120 seconds default, 0 to disable memory mode • 10: Force logfwd to run in disk mode [1:enable, 0:disable] • 97: memory check • 98: Reset log-forwarding stats • 99: Restart logfwd
log-fetchd <integer> ...	<p>Log-fetch daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show states • 3: show running sessions • 99: restart the daemon
miglogd <integer> ...	<p>Miglogd daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: dump memory pool • 99: restart daemon
oftpd <integer> ...	<p>Oftpd daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: show connected device name and IP • 4: show detailed session state • 5: show oftp request statistics • 6: show cmdb device cache

Variable	Description
	<ul style="list-style-type: none"> • 7: show logfwd thread stats • 8: show tasklist statistics • 9: show unreg dev cache • 10: log cluster bridge stats • 11: show helper threads stats • 12: show HA group cache • 13: show file fwd stats • 14: show fct software inventory cache • 15: show fgt interface stats • 16: show fos-auto device dump. [dev] to dump device list • 17: show device logging rate & rate-limit. [enable] to force tracking log-rate or [disable] to track only rate-limited devices. [config] to show config • 21: dump oftp-restapi-sched stats • 22: dump oftp-restapi-sched status • 30: dump csf groups data in all adoms in json string • 31: show csf groups update stats • 32: reschedule all restapi task for designated devid • 40: test loading a CA cert from local path • 42: device logging disable [show] add del reload • 50: display logtypes for all devid • 60: display login requests stats • 90: reload un-reg device tree • 91: delete designated csf group • 92: reload reg dev cache • 95: debug output • 99: restart daemon
rptchkd <integer> ...	<p>Sqldrptcache daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 4: list adoms • 6: list schedules • 55: re-check an adom • 99: restart daemon • 910: enable rptchkd • 911: disable rptchkd
scansched <integer> ...	<p>Scansched daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 11: show ioc-rescan task status • 99: restart daemon
siemagentd <integer> ...	<p>Siemagentd daemon test usage:</p>

Variable	Description
	<ul style="list-style-type: none"> • 1: show PID • 2: show daemon statistics • 3: show daemon worker statistics • 4: show daemon worker status stats • 5: show supported device-log types • 11: worker process run • 12: worker process suspend • 13: worker process exit • 14: worker process reload config • 20: show the siem stream storage info • 21: show the latest siem stream submitted in redis • 98: restart daemon controller • 99: restart daemon • 201-209: send diag cmd to worker
siemdbd <integer> ...	<p>Siemdbd daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 3: show running processes • 4: show writers info • 5: show splitter info • 6: show Adom database info • 7: show trimmer info • 8: show the shared Materialized View disk usage info • 41: show writer 1 info • 42: show writer 2 info • 43: show writer 3 info • 97: clear redis stream • 99: restart daemon
snmpd <integer> ...	<p>SNMP daemon test usage:</p> <ul style="list-style-type: none"> • 1: display daemon pid • 2: display snmp statistics • 3: clear snmp statistics • 4: generate test trap (cpu high) • 5: generate test traps (log alert, rate, data rate) • 6: generate test traps (licensed gb/day, device quota) • 99: restart daemon
sqllogd <integer> ...	<p>SqlLog daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 3: show worker init state

Variable	Description
	<ul style="list-style-type: none"> • 4: show worker thread info • 5: show log device scan info, optionally filter by <devid> • 7: show ADOM device list by <adom-name> • 8: show logUID info • 9: show ADOM scan sync info, optionally filter by <adom> • 10: show FortiClient dev to sql-ID (sID) map • 11: show devtable cache info • 12: show intfrole cache info • 41: show worker 1 info • 51: show worker 1 registered log devices • 61: show worker 1 open log file cache • 70: show sql database building progress • 71: show the progress of upgrading log files into per-vdom storage • 72: run the upgrading log files into per-vdom storage • 80: show daemon status flags • 81: show debug zone devices status • 82: show all adoms with member devices or filter by <adom-name> • 83: show all registered logdevs • 84: show all unreg logdevs • 85: show fazid map stats • 95: request to rebuild SQL database for local event logs • 96: resend all pending batch files to sqlplugind • 97: rebuilding warm restart • 98: set worker assignment to policy 'round-robin' or 'adom-affinity', daemon will restart on policy change. • 99: restart daemon • 200: diag for log based alert (event mgmt) .. • 201: diag for utmref cache .. • 202: diag for fgt-fct corelation .. • 203: diag for logstat .. • 204: diag for loC .. • 205: diag for endpoint and enduser .. • 206: diag for ueba .. • 207: diag for FSA scan session .. • 208: diag for audit report event process .. • 209: diag for shadow it info .. • 221: estimated browsing time stats • 222: fsa devmap cache info • 224: fgt lograte cache info • 225: dump enum field error cache • 226: reset enum field error cache • 227: dump tz field error cache • 228: reset tz field error cache
sqlplugind <integer> ...	Sqlplugind daemon test usage:

Variable	Description
	<ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show daemon stats 3: show SIEM table stats 4: show table compressor stats 5: show table compressor Adom stats 91: scan hcache query templates and clean up unused 98: scan and clean zombie cstore files 99: restart daemon
sqlreportd <integer> ...	Sqlreportd daemon test usage: <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show daemon stats
sqlrptcached <integer> ...	Sqlrptcache daemon test usage: <ul style="list-style-type: none"> 1: show PID 2: show statistics and state 3: reset statistics and state 5: dump auto-cache charts 99: restart daemon
syncsched <integer> ...	Syncsched daemon test usage: <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show report nodes states 3: show report syncing state 4: show ha sync peers 5: reset ha sync queue 6: show ha elog sync 10: sync reports with peer 11: fsync stat 12: fsync reload 13: trim sync dir stat 99: restart daemon
uploadadd <integer> ...	Uploadadd daemon test usage: <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show statistics and state 3: reset statistics and state 4: show uploadadd queues content 5: show upload server state 50: clear log queue [mirror server1] 51: clear log queue [mirror server2] 52: clear log queue [mirror server3] 53: clear log queue [backup] 54: clear log queue [original request] 55: clear log queues [all] 56: clear report queue

Variable	Description
	<ul style="list-style-type: none">• 60: cloud storage bget backlog info• 61: cloud storage get setting pending info <setting name>• 62: cloud storage test connector <connector> <remote path>• 63: cloud storage get usage info• 99: restart daemon

test connection

Use this command to test connections.

Syntax

```
diagnose test connection fortianalyzer <ip>
diagnose test connection mailserver <server-name> <mail-from> <mail-to>
diagnose test connection syslogserver <server-name>
```

Variable	Description
fortianalyzer <ip>	Test the connection to the FortiAnalyzer.
mailserver <server-name> <mail-from> <mail-to>	Test the connection to the mail server.
syslogserver <server-name>	Test the connection to the syslog server.

test deploymanager

Use this command to test the deployment manager.

Syntax

```
diagnose test deploymanager getcheckin <devid>
diagnose test deploymanager reloadconf <devid>
```

Variable	Description
getcheckin <devid>	Get configuration check-in information from the FortiGate.
reloadconf <devid>	Reload configuration from the FortiGate.

test policy-check

Use this command to list or flush policy consistency checks.

Syntax

```
diagnose test policy-check flush
diagnose test policy-check list
```

Variable	Description
flush	Flush all policy check sessions.
list	List all policy check sessions.

test search

Use this command to test the search daemon.

Syntax

```
diagnose test search flush
diagnose test search list
```

Variable	Description
flush	Flush all search sessions.
list	List all search sessions.

test sftp

Use this command to test the secure file transfer protocol (SFTP) scheduled backup.

Syntax

```
diagnose test sftp auth <sftp server> <username> <password> <directory>
```

Variable	Description
<sftp server>	SFTP server IP address.
<username>	SFTP server username.
<password>	SFTP server password.
<directory>	The directory on the SFTP server where you want to put the file (default = /).

upload

Use these commands to perform request related actions.

upload clear

Use this command to clear the upload request.

Syntax

```
diagnose upload clear log {all | original | backup | mirror 1 | mirror 2 | mirror 3}
diagnose upload clear report
```

Variable	Description
log {all original backup mirror 1 mirror 2 mirror 3}	Clear log uploading requests. <ul style="list-style-type: none">• all: Clear all log uploading requests.• backup: Clear log uploading requests in the backup queue.• mirror 1: Clear log uploading requests in the mirror queue for server 1.• mirror 2: Clear log uploading requests in the mirror queue for server 2.• mirror 3: Clear log uploading requests in the mirror queue for server 3.• original: Clear log uploading requests in the original queue.
report	Clear all report upload requests.

upload status

Use this command to get the running status.

Syntax

```
diagnose upload status
```

vpn

Use this command to flush SAD entries and list tunnel information.

Syntax

```
diagnose vpn tunnel flush-SAD
diagnose vpn tunnel list
```

Variable	Description
flush-SAD	Flush the SAD entries.
list	List tunnel information.

get

The `get` command displays all settings, even if they are still in their default state.



Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands that display that part of the configuration. Get and show commands use the same syntax as their related `config` command, unless otherwise specified.



CLI commands and variables are case sensitive.

The `get` command displays all settings, including settings that are in their default state.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

fmupdate analyzer	fmupdate web-spam	system fortiview	system ntp	system syslog
fmupdate av-ips	system admin	system global	system password-policy	system workflow
fmupdate custom-url-list	system alert-console	system ha	system performance	
fmupdate disk-quota	system alertemail	system ha-scheduled-check	system report	
fmupdate fct-services	system auto-delete	system ha-status	system route	
fmupdate fds-setting	system backup	system interface	system route6	
fmupdate fwm-setting	system certificate	system locallog	system saml	
fmupdate multilayer	system connector	system log	system sniffer	
fmupdate publicnetwork	system dm	system log fetch	system snmp	
fmupdate server-access-priorities	system dns	system loglimits	system soc-fabric	

fmupdate server-override-status	system docker	system mail	system sql
fmupdate service	system fips	system metadata	system status

fmupdate analyzer

Use this command to view forward virus report to FDS.

Syntax

```
get fmupdate analyzer virusreport
```

fmupdate av-ips

Use these commands to view AV/IPS update settings.

Syntax

```
get fmupdate av-ips advanced-log
get fmupdate av-ips web-proxy
```

Example

This example shows the output for `get fmupdate av-ips web-proxy`:

```
ip : 0.0.0.0
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

fmupdate custom-url-list

Use this command to view the custom URL database.

Syntax

```
get fmupdate custom-url-list
```

fmupdate disk-quota

Use this command to view the disk quota for the update manager.

Syntax

```
get fmupdate disk-quota
```

Example

This example shows the output for `get fmupdate disk-quota`:

```
value : 51200
```

fmupdate fct-services

Use this command to view FortiClient update services configuration.

Syntax

```
get fmupdate fct-services
```

Example

This example shows the output for `get fmupdate fct-services`:

```
status : enable  
port : 80
```

fmupdate fds-setting

Use this command to view FDS parameters.

Syntax

```
get fmupdate fds-setting
```

Example

This example shows the output for `get fmupdate fds-setting`:

```
User-Agent : Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident /5.0)  
fds-clt-ssl-protocol: tlsv1.2
```

```
fds-ssl-protocol : tlsv1.2
fmtr-log : info
linkd-log : info
max-av-ips-version : 20
max-work : 1
push-override:
push-override-to-client:
send_report : enable
send_setup : disable
server-override:
system-support-fct : emergency
system-support-fdc :
system-support-fgt :
system-support-fml :
system-support-fsa :
system-support-fts :
umsvc-log : info
unreg-dev-option : add-service
update-schedule:
    time: 00:10
wanip-query-mode : disable
```

fmupdate fwm-setting

Use this command to view firmware management settings.

Syntax

```
get fmupdate fwm-setting
```

Example

This example shows the output for `get fmupdate fwm-setting`:

```
auto-scan-fgt-disk : enable
check-fgt-disk : enable
fds-failover-fmg : enable
fds-image-timeout : 1800
immx-source : fmg
log : fwm_dm
multiple-steps-interval : 60
```

fmupdate multilayer

Use this command to view multilayer mode configuration.

Syntax

```
get fmupdate multilayer
```

fmupdate publicnetwork

Use this command to view public network configuration.

Syntax

```
get fmupdate publicnetwork
```

fmupdate server-access-priorities

Use this command to view server access priorities.

Syntax

```
get fmupdate server-access-priorities
```

Example

This example shows the output for `get fmupdate server-access-priorities`:

```
access-public : disable
av-ips : disable
private-server:
web-spam : enable
```

fmupdate server-override-status

Use this command to view server override status configuration.

Syntax

```
get fmupdate server-override status
```

fmupdate service

Use this command to view update manager service configuration.

Syntax

```
get fmupdate service
```

Example

This example shows the output for `get fmupdate service`:

```
avips : enable
query-antispam : enable
query-antivirus : disable
query-filequery : disable
query-iot : disable
query-outbreak-prevention: disable
query-webfilter : enable
webfilter-https-traversal: disable
```

fmupdate web-spam

Use these commands to view web spam configuration.

Syntax

```
get fmupdate web-spam fgd-setting
get fmupdate web-spam web-proxy
```

Example

This example shows the output for `get fmupdate web-spam web-proxy`:

```
ip : 0.0.0.0
ip6 : ::
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

system admin

Use these commands to view admin configuration.

Syntax

```
get system admin group [group name]
get system admin ldap [server entry name]
get system admin profile [profile ID]
get system admin radius [server entry name]
get system admin setting
get system admin tacacs [server entry name]
get system admin user [username]
```

Example

This example shows the output for `get system admin setting`:

```
access-banner : disable
admin-https-redirect: enable
admin-login-max : 256
admin_server_cert : server.crt
allow_register : disable
auth-addr : (null)
auth-port : 443
auto-update : enable
banner-message : (null)
central-ftgd-local-cat-id: disable
chassis-mgmt : disable
chassis-update-interval: 15
device_sync_status : enable
gui-theme : blue
http_port : 80
https_port : 443
idle_timeout : 900
idle_timeout_api : 900
idle_timeout_gui : 900
install-ifpolicy-only: disable
mgmt-addr : (null)
mgmt-fqdn : (null)
objects-force-deletion: enable
offline_mode : disable
register_passwd : *
sdwan-monitor-history: disable
sdwan-skip-unmapped-input-device: disable
shell-access : disable
show-add-multiple : disable
show-adom-devman : enable
show-checkbox-in-table: disable
show-device-import-export: disable
show-fct-manager : disable
show-hostname : disable
show_automatic_script: disable
show_grouping_script: enable
show_schedule_script: disable
show_tcl_script : disable
unreg_dev_opt : add_allow_service
webadmin_language : auto_detect
```

system alert-console

Use this command to view alert console information.

Syntax

```
get system alert-console
```

Example

This example shows the output for `get system alert-console`:

```
period : 7
severity-level : emergency
```

system alertemail

Use this command to view alert email configuration.

Syntax

```
get system alertemail
```

Example

This example shows the output for `get system alertemail`:

```
authentication : enable
fromaddress : (null)
fromname : (null)
smtppassword : *
smtpport : 25
smtpserver : (null)
smtpuser : (null)
```

system auto-delete

Use this command to view automatic deletion policies for logs, reports, DLP files, and quarantined files.

Syntax

```
get system auto-delete
```

system backup

Use the following commands to view backups:

Syntax

```
get system backup all-settings
get system backup status
```

Example

This example shows the output for `get system backup status`:

```
All-Settings Backup
  Last Backup: Tue Sep 29 08:03:35 2020
  Next Backup: N/A
```

system certificate

Use these commands to view certificate configuration.

Syntax

```
get system certificate ca [certificate name]
get system certificate crl [crl name]
get system certificate local [certificate name]
get system certificate oftp [certificate name]
get system certificate remote [certificate name]
get system certificate ssh [certificate name]
```

Example

This example shows the output for `get system certificate local Fortinet_Local`:

```
name : Fortinet_Local
password : *
comment : Default local certificate
private-key :
certificate :
  Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN =
    FMG-VM0A11000137, emailAddress = support@fortinet.com
  Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
    Authority, CN = support, emailAddress = support@fortinet.com
  Valid from: 2011-01-07 26:58:75 GMT
  Valid to: 2031-02-21 31:88:05 GMT
  Fingerprint: 0A:--:--:--:--:--:--:--:--:--:--:--:--:0B
  Root CA: No
  Version: 3
```

```
Serial Num:
  89
Extensions:
  Name: X509v3 Basic Constraints
  Critical: no
  Content:
  CA:FALSE
csr :
```

system connector

Use this command to view FSSO connector refresh intervals, in seconds.

Syntax

```
get system connector
```

Example

This example shows the output for `get system connector`:

```
fsso-refresh-interval: 180
fsso-sess-timeout : 300
px-refresh-interval : 300
px-svr-timeout : 900
```

system dm

Use this command to view device manager information on your FortiManager unit.

Syntax

```
get system dm
```

Example

This example shows the output for `get system dm`:

```
concurrent-install-image-limit: 500
concurrent-install-limit: 480
concurrent-install-script-limit: 480
conf-merge-after-script: disable
discover-timeout : 6
dpm-logsize : 10000
fgfm-sock-timeout : 360
fgfm_keepalive_itvl : 120
force-remote-diff : disable
```

```
fortiap-refresh-cnt : 500
fortiap-refresh-itvl: 10
fortiext-refresh-cnt: 50
install-image-timeout: 3600
install-tunnel-retry-itvl: 60
max-revs : 100
nr-retry : 1
retry : enable
retry-intvl : 15
rollback-allow-reboot: disable
script-logsize : 100
skip-tunnel-fcp-req : enable
verify-install : disable
```

system dns

Use this command to view DNS configuration.

Syntax

```
get system dns
```

Example

This example shows the output for `get system dns`:

```
primary : 111.11.111.11
secondary : 111.11.111.12
ip6-primary : ::
ip6-secondary : ::
```

system docker

Use this command to view Docker and management extension statuses.

Syntax

```
get system docker
```

Example

This example shows the output for `get system docker`:

```
status : disable
cpu : 50
mem : 50
default-address-pool_base : 172.17.0.0 255.255.0.0
```

```
default-address-pool_size : 24
docker-user-login-max: 32
```

system fips

Use this command to view FIPS configuration.

Syntax

```
get system fips
```

system fortiview

Use this command to view Fortiview configuration.

Syntax

```
get system fortiview auto-cache
get system fortiview setting
```

Example

This example shows the output for `get system fortiview auto-cache`:

```
aggressive-fortiview: disable
interval : 168
status : enable
```

system global

Use this command to view global system settings.

Syntax

```
get system global
```

Example

This example shows the output for `get system global`:

```
admin-lockout-duration: 60
admin-lockout-threshold: 3
```

```
adom-mode : normal
adom-rev-auto-delete: by-revisions
adom-rev-max-backup-revisions: 5
adom-rev-max-revisions: 120
adom-status : disable
clone-name-option : default
clt-cert-req : disable
console-output : standard
country-flag : enable
create-revision : disable
daylightsavetime : enable
default-disk-quota : 1000
detect-unregistered-log-device: enable
device-view-mode : regular
dh-params : 2048
disable-module : fortirecorder siem soc ai
enc-algorithm : high
faz-status : disable
fgfm-local-cert : (null)
fgfm-ssl-protocol : tls1.2
ha-member-auto-grouping: enable
hostname : FMG-VM64
import-ignore-addr-cmt: disable
language : english
latitude : (null)
ldap-cache-timeout : 86400
ldapconntimeout : 60000
log-checksum : none
log-forward-cache-size : 0
longitude : (null)
max-running-reports : 1
multiple-steps-upgrade-in-autolink : disable
object-revision-db-max: 100000
object-revision-mandatory-note: enable
object-revision-object-max: 100
object-revision-status: enable
oftp-ssl-protocol : tls1.2
partial-install : disable
partial-install-rev : disable
perform-improve-by-ha: disable
policy-object-icon : disable
policy-object-in-dual-pane: disable
pre-login-banner : disable
private-data-encryption : disable
remoteauthtimeout : 10
search-all-adoms : disable
ssl-low-encryption : disable
ssl-protocol : tls1.3 tls1.2
ssl-static-key-ciphers: enable
task-list-size : 2000
timezone : (GMT-8:00) Pacific Time (US & Canada).
tunnel-mtu : 1500
usg : disable
vdom-mirror : disable
webservice-proto : tls1.3 tls1.2
workspace-mode : disabled
```

system ha

Use this command to view HA configuration.

Syntax

```
get system ha
```

Example

This example shows the output for `get system ha`:

```
clusterid : 1
file-quota : 4096
hb-interval : 10
hb-lost-threshold : 30
mode : standalone
password : *
peer:
```

system ha-scheduled-check

Use this command to view HA integrity check configuration.

Syntax

```
get system ha-scheduled-check
```

Example

This example shows the output for `get system ha-scheduled-check`:

```
status : disable
time : (null)
```

system ha-status

Use this command to view additional HA configuration.

Syntax

```
get system ha-status
```

Example

This example shows the output for `get system ha-status`:

```
Cluster-ID : 1
Debug : off
File-Quota : 4096
HA Health Status : OK
HA Role : Primary
FMG-HA Status : Never Synchronized State
Model : FortiManager-VM64
HB-Interval : 10
HB-Lost-Threshold : 30
HA Primary Uptime : Wed Jul 7 06:33:35 2021
HA Primary state change timestamp :
HB-Lost-Threshold : 30
Primary : FMG-VM64, FMG-VM0000000000,
System Usage stats :
  FMG-VM0000000000(updated 0 seconds ago):
    average-cpu-user/nice/system/idle=0.05%/0.00%/0.00%/99.95%, memory=14.56%
```

system interface

Use this command to view interface configuration.

Syntax

```
get system interface [interface name]
```

Example

This example shows the output for `get system interface`:

```
== [ port1 ]
name: port1 status: enable ip: 172.172.172.222 255.255.0.0 speed: auto
== [ port2 ]
name: port2 status: enable ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port3 ]
name: port3 status: enable ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port4 ]
name: port4 status: enable ip: 1.1.1.1 255.255.255.255 speed: auto
```

This example shows the output for `get system interface port1`:

```
name : port1
status : enable
ip : 172.172.172.222 255.255.255.0
allowaccess : ping https ssh snmp soc-fabric http webservice
serviceaccess :
speed : auto
description : (null)
alias : (null)
mtu : 1500
```

```
ipv6:
  ip6-address: ::/0 ip6-allowaccess:
```

system locallog

Use these commands to view local log configuration.

Syntax

```
get system locallog disk filter
get system locallog disk setting
get system locallog [fortianalyzer | fortianalyzer2 | fortianalyzer3] filter
get system locallog [fortianalyzer | fortianalyzer2 | fortianalyzer3] setting
get system locallog memory filter
get system locallog memory setting
get system locallog [syslogd | syslogd2 | syslogd3] filter
get system locallog [syslogd | syslogd2 | syslogd3] setting
```

Examples

This example shows the output for `get system locallog disk setting`:

```
status : enable
severity : information
upload : disable
server-type : FTP
max-log-file-size : 100
roll-schedule : none
diskfull : overwrite
log-disk-full-percentage: 80
```

This example shows the output for `get system locallog syslogd3 filter`:

```
event : enable
devcfg : enable
devops : enable
diskquota : enable
dm : enable
docker : enable
dvm : enable
ediscovery : enable
epmgr : enable
eventmgmt : enable
faz : enable
fazsys : enable
fgd : enable
fgfm : enable
fmgws : enable
fmlmgr : enable
fmwmgr : enable
fortiview : enable
glbcfg : enable
ha : enable
```

```
hcache : enable
incident: enable
iolog : enable
logd : enable
logdb : enable
logdev : enable
logfile : enable
logging : enable
lrmgr : enable
objcfg : enable
report : enable
rev : enable
rtmon : enable
scfw : enable
scply : enable
scrmgr : enable
scvpn : enable
system : enable
webport : enable
```

system log

Use these commands to view log configuration.

Syntax

```
get system log alert
get system log device-disable
get system log interface-stats
get system log ioc
get system log mail-domain <id>
get system log ratelimit
get system log settings
```

Example

This example shows the output for `get system log settings`:

```
FAC-custom-field1 : (null)
FAZ-custom-field1 : (null)
FCH-custom-field1 : (null)
FCT-custom-field1 : (null)
FDD-custom-field1 : (null)
FGT-custom-field1 : (null)
FMG-custom-field1 : (null)
FML-custom-field1 : (null)
FPX-custom-field1 : (null)
FSA-custom-field1 : (null)
FWB-custom-field1 : (null)
browse-max-logfiles : 10000
dns-resolve-dstip : disable
download-max-logs : 100000
```

```
ha-auto-migrate : disable
import-max-logfiles : 10000
log-file-archive-name: basic
rolling-regular:
sync-search-timeout : 60
```

system log fetch

Use these commands to view log fetching configuration.

Syntax

```
get system log-fetch client-profile [id]
get system log-fetch server-settings
```

Example

This example shows the output for `get system log-fetch server-settings`:

```
max-conn-per-session: 3
max-sessions : 1
session-timeout : 10
```

system loglimits

Use this command to view log limits on your FortiManager unit.

Syntax

```
get system loglimits
```

Example

This example shows the output for `get system loglimits`:

```
GB/day : 50
Peak Log Rate : 2100
Sustained Log Rate : 1400
```

Where:

GB/day	Number of gigabytes used per day.
Peak Log Rate	Peak time log rate.
Sustained Log Rate	Average log rate.

system mail

Use this command to view alert email configuration.

Syntax

```
get system mail [mail service id]
```

Example

This example shows the output for an alert email named `Test`:

```
id : Test
auth : disable
auth-type : psk
passwd : *
port : 25
secure-option : default
server : mailServer
user : mailperson@mailServer.com
```

system metadata

Use this command to view metadata settings.

Syntax

```
get system metadata admins [fieldname]
```

Example

This example shows the output for `get system metadata admins 'Contact Email'`:

```
fieldname : Contact Email
fieldlength : 50
importance : optional
status : enabled
```

system ntp

Use this command to view NTP configuration.

Syntax

```
get system ntp
```

Example

This example shows the output for `get system ntp`:

```
ntpserver:
  == [ 1 ]
  id: 1
  status : enable
  sync_interval : 60
```

system password-policy

Use this command to view the system password policy.

Syntax

```
get system password-policy
```

Example

This example shows the output for `get system password-policy`:

```
status : enable
minimum-length : 11
must-contain : upper-case-letter lower-case-letter number non-alphanumeric
change-4-characters : disable
expire : 30
```

system performance

Use this command to view performance statistics on your FortiManager unit.

Syntax

```
get system performance
```

Example

This example shows the output for `get system performance`:

```
CPU:
```

```
Used: 4.89%
Used(Excluded NICE): 4.89%
    %used %user %nice %sys %idle %iowait %irq %softirq
CPU0 4.89 2.85 0.00 2.04 95.11 0.00 0.00 0.00
Memory:
Total: 4,134,728 KB
Used: 2,011,824 KB 48.7%
Hard Disk:
Total: 82,434,456 KB
Used: 44,018,112 KB 53.4%
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
        6.9 5.5 1.4 193.4 195.4 0.0 5.1 0.7 0.5 108708.57
Flash Disk:
Total: 499,656 KB
Used: 113,504 KB 22.7%
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
        0.0 0.0 0.0 0.0 0.0 0.0 1.4 0.6 0.0 108708.62
```

system report

Use this command to view report configuration.

Syntax

```
get system report auto-cache
get system report est-browse-time
get system report group [group id]
get system report setting
```

Example

This example shows the output for `get system report setting`:

```
aggregate-report : disable
ldap-cache-timeout : 60
max-table-rows : 10000
report-priority : auto
template-auto-install: default
week-start : sun
```

system route

Use this command to view IPv4 routing table configuration.

Syntax

```
get system route [seq_num]
```

Example

This example shows the output for `get system route 66`:

```
seq_num : 66
device  : port5
dst     : 0.0.0.0 0.0.0.0
gateway : 10.111.1.16
```

system route6

Use this command to view IPv6 routing table configuration.

Syntax

```
get system route6 [seq_num]
```

system saml

Use this command to view SAML configuration.

Syntax

```
get system saml
```

Example

This example shows the output for `get system saml`:

```
status : enable
role   : SP
cert   : Fortinet_Local2
server-address : 172.27.2.225
login-auto-redirect : enable
entity-id : http://172.27.2.225/metadata/
acs-url   : https://172.27.2.225/saml/?acs
sls-url   : https://172.27.2.225/saml/?sls
idp-entity-id : http://http://172.27.2.224/saml-idp/sg45/metadata/
idp-single-sign-on-url: https://http://172.27.2.224/saml-idp/sg45/login/
idp-single-logout-url: https://http://172.27.2.224/saml-idp/sg45/logout/
idp-cert  : Remote_Cert_1
default-profile : Restricted_User
forticloud-sso : disable
user-auto-create : disable
```

system sniffer

Use this command to view the packet sniffer configuration.

Syntax

```
get system sniffer
```

system snmp

Use these commands to view SNMP configuration.

Syntax

```
get system snmp community [community ID]
get system snmp sysinfo
get system snmp user [SNMP user name]
```

Example

This example shows the output for `get system snmp sysinfo`:

```
contact_info : (null)
description  : Test FMG
engine-id    : (null)
location     : (null)
status       : enable
trap-cpu-high-exclude-nice-threshold: 80
trap-high-cpu-threshold: 80
trap-low-memory-threshold: 80
```

system soc-fabric

Use this command to view the SOC Fabric configuration.

Syntax

```
get system soc-fabric
```

Example

This example shows the output for `get system soc-fabric`:

```
status : disable
```

system sql

Use this command to view SQL configuration.

Syntax

```
get system sql
```

Example

This example shows the output for `get system sql`:

```
custom-index:
prompt-sql-upgrade : enable
status : local
text-search-index : disable
ts-index-field:
  == [ FGT-app-ctrl ]
  category: FGT-app-ctrl value:
    user,group,srcip,dstip,dstport,service,app,action,hostname
  == [ FGT-attack ]
  category: FGT-attack value: severity,srcip,dstip,action,user,attack
  == [ FGT-content ]
  category: FGT-content value: from,to,subject,action,srcip,dstip,hostname,status
  == [ FGT-dlp ]
  category: FGT-dlp value: user,srcip,service,action,filename
  == [ FGT-emailfilter ]
  category: FGT-emailfilter value: user,srcip,from,to,subject
  == [ FGT-event ]
  category: FGT-event value: subtype,ui,action,msg
  == [ FGT-traffic ]
  category: FGT-traffic value: user,srcip,dstip,service,app,utmaction
  == [ FGT-virus ]
  category: FGT-virus value: service,srcip,dstip,action,filename,virus,user
  == [ FGT-voip ]
  category: FGT-voip value: action,user,src,dst,from,to
  == [ FGT-webfilter ]
  category: FGT-webfilter value: user,srcip,dstip,service,action,catdesc,hostname
  == [ FGT-netscan ]
  category: FGT-netscan value: user,dstip,vuln,severity,os
  == [ FGT-fct-event ]
  category: FGT-fct-event value: (null)
  == [ FGT-fct-traffic ]
  category: FGT-fct-traffic value: (null)
  == [ FGT-fct-netscan ]
  category: FGT-fct-netscan value: (null)
  == [ FGT-waf ]
  category: FGT-waf value: user,srcip,dstip,service,action
  == [ FGT-gtp ]
  category: FGT-gtp value: msisd,from,to,status
  == [ FGT-dns ]
  category: FGT-dns value: (null)
  == [ FGT-ssh ]
  category: FGT-ssh value: (null)
```

```

== [ FML-emailfilter ]
category: FML-emailfilter value: client_name,dst_ip,from,to,subject
== [ FML-event ]
category: FML-event value: subtype,msg
== [ FML-history ]
category: FML-history value: classifier,disposition,from,to,client_
      name,direction,domain,virus
== [ FML-virus ]
category: FML-virus value: src,msg,from,to
== [ FWB-attack ]
category: FWB-attack value: http_host,http_url,src,dst,msg,action
== [ FWB-event ]
category: FWB-event value: ui,action,msg
== [ FWB-traffic ]
category: FWB-traffic value: src,dst,service,http_method,msg
background-rebuild : enable
compress-table-min-age : 7
database-type : postgres
device-count-high : disable
event-table-partition-time: 0
fct-table-partition-time: 360
rebuild-event : enable
rebuild-event-start-time: 00:00 2000/01/01
start-time : 00:00 2000/01/01
traffic-table-partition-time: 0
utm-table-partition-time: 0

```

system status

Use this command to view the status of your FortiManager unit.

Syntax

```
get system status
```

Example

This example shows the output for `get system status`:

```

Platform Type : FMG-VM64
Platform Full Name : FortiManager-VM64
Version : v6.0.1-build0150 180606 (GA)
Serial Number : F-----7
BIOS version : 04000002
Hostname : FMG-VM64
Max Number of Admin Domains : 1000000000
Max Number of Device Groups : 1000000000
Admin Domain Configuration : Enabled
HA Mode : Stand Alone
Branch Point : 0150
Release Version Information : GA
Current Time : Tue Sep 29 08:09:05 PDT 2020

```

```
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 36.62GB, Total 78.62GB
File System : Ext4
License Status : Valid
```

system syslog

Use this command to view syslog information.

Syntax

```
get system syslog [syslog server name]
```

Example

This example shows the output for an syslog server named Test:

```
name : Test
ip : 10.10.10.1
port : 514
```

system workflow

Use this command to view workflow approval matrix information.

Syntax

```
get system workflow approval-matrix [adom]
```

show

The `show` commands display a part of your unit's configuration in the form of the commands that are required to achieve that configuration from the firmware's default state.



Although not explicitly shown in this section, for all `config` commands, there are related `show` commands that display that part of the configuration. The `show` commands use the same syntax as their related `config` command.



CLI commands and variables are case sensitive.

Unlike the `get` command, `show` does not display settings that are in their default state.

Example

```
FMG-VM64 # show sys glob
config system global
    set adom-status enable
    set create-revision enable
    set detect-unregistered-log-device disable
    set device-view-mode tree
    set hostname "FMG-VM64"
end
```

Appendix A - CLI Error Codes

Some FortiManager CLI commands issue numerical error codes. The following table lists the error codes and descriptions.

Error Code	Description
0	Success
1	Function called with illegal parameters
2	Unknown protocol
3	Failed to connect host
4	Memory failure
5	Session failure
6	Authentication failure
7	Generic file transfer failure
8	Failed to access local file
9	Failed to access remote file
10	Failed to read local file
11	Failed to write local file
12	Failed to read remote file
13	Failed to write remote file
14	Local directory failure
15	Remote directory failure



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.