



FortiManager v4.0 MR3 Patch Release 8 CLI Reference



FortiManager v4.0 MR3 Patch Release 8 CLI Reference

November 25, 2013

02-438-167076-20131125

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. 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 guarantees. 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.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log	11
Introduction.....	12
About the FortiManager system	12
Web-based Manager	13
FortiManager system product life cycle	13
What's New in FortiManager v4.0 MR3	14
Using the Command Line Interface	21
CLI command syntax.....	21
Connecting to the CLI.....	22
Connecting to the FortiManager console	22
Setting administrative access on an interface	23
Connecting to the FortiManager CLI using SSH	24
Connecting to the FortiManager CLI using the Web-based Manager.....	24
CLI objects.....	24
CLI command branches	25
config branch	25
get branch.....	27
show branch	28
execute branch	29
diagnose branch	29
Example command sequences.....	29
CLI basics	30
Command help	31
Command completion	31
Recalling commands	31
Editing commands	31
Line continuation.....	32
Command abbreviation	32
Environment variables.....	32
Encrypted password support	32
Entering spaces in strings.....	33
Entering quotation marks in strings	33
Entering a question mark (?) in a string	33
International characters	33
Special characters	33
IP address formats.....	33
Editing the configuration file	34
Changing the baud rate	34

Administrative Domains.....	35
ADOMs overview	35
Configuring ADOMs.....	36
Concurrent ADOM access	37
fmsystem.....	38
admin ldap	38
admin profile	40
admin radius	43
admin setting	44
admin tacacs	48
admin user	49
alert-console	54
alert-event	54
alertemail.....	57
backup all-settings	58
certificate ca	59
certificate local.....	60
dm	61
dns	63
fips	63
global	64
ha	66
General FortiManager HA configuration steps	68
interface	69
locallog disk setting	70
locallog filter.....	73
locallog fortianalyzer setting	76
locallog memory setting.....	76
locallog syslogd (syslogd2, syslogd3) setting.....	77
log fortianalyzer.....	79
log setting	80
mail	81
metadata.....	82
ntp.....	82
password-policy	83
route.....	84
snmp community	85
snmp sysinfo.....	88
snmp user	89
syslog.....	90

fmupdate	92
analyzer virusreport	92
av-ips advanced-log	93
av-ips fct server-override	93
av-ips fgt server-override	94
av-ips push-override	95
av-ips push-override-to-client	96
av-ips update-schedule	97
av-ips web-proxy	98
custom-url-list	99
deployment	99
device-version	100
disk-quota	101
fct-services	101
multilayer	102
publicnetwork	102
server-access-priorities	102
config private-server	103
server-override-status	104
service	104
support-pre-fgt43	105
web-spam fct server-override	105
web-spam fgd-log	106
web-spam fgd-setting	107
web-spam fgt server-override	107
web-spam poll-frequency	108
web-spam web-proxy	108
fmclient	110
ad_grouping_setting	110
ad_ou_grouping	110
client_license	111
cluster secondary	112
cluster setting	112
communication_setting	113
discovery	114
emailalert	114
enterprise_license	115
group_admin	116
ldap_users	117
ldapsetting	118

license_key	118
location_aware.....	119
lockdown	120
systemsetting.....	120
webfilter_profile.....	121
fcdevice	123
group.....	123
ungroup.....	125
unit	126
fcpolicy	127
antileak option	127
antileak sensword	128
antispam bannedword	129
antispam blackwhitelist	129
antispam option	130
antivirus scheduledscan	131
antivirus setting email	132
antivirus setting realtime	133
antivirus setting scheduledscan	134
firewall address	136
firewall addrgrp	137
firewall apppolicy	138
firewall option.....	139
firewall pingserver	142
firewall policy	142
firewall protocol	144
firewall protocolgrp	145
firewall schedule recurring	145
firewall schedulegrp	146
firewall service	147
firewall trustedip address.....	148
firewall zone	149
log setting	150
system locationaware	152
system settings.....	152
system trustedfortimanager.....	155
system wan_optimization	156
vpn download	156
vpn option	157
vpn security_policy	158

webfilter option	158
webfilter profile	160
execute	161
add-vm-license	162
backup	162
bootimage	163
certificate ca	163
certificate local	163
certificate local generate	164
chassis	165
console baudrate	165
date	166
device	167
devicelog clear	167
dmserver delrev	167
dmserver revlist	167
dmserver showconfig	168
dmserver showdev	168
dmserver showrev	168
fcdevice addtomanaged	168
fcdevice find-unit	169
fcdevice search	169
fcpolicy apply_to_members	169
fcpolicy deploy	170
fcpolicy grant unlicensed	170
fcpolicy group	170
fcpolicy retrieve	171
fcpolicy revoke unit	171
fcpolicy unit	171
fgfm reclaim-dev-tunnel	172
fgt-cli-access	172
fmclient apply-lockdown	172
fmclient client_license list	173
fmclient client_license list_device	173
fmclient cluster	174
fmclient enterprise_license download	174
fmclient enterprise_license list	174
fmclient group refresh	175
fmclient group rename	175
fmclient license_key deploy	175

fmclient license_key list	175
fmclient optimize-fcm-database	176
fmclient package delete	176
fmclient package deploy	176
fmclient package download	176
fmclient package list	177
fmclient refresh_ou	177
fmclient sync-ldap	177
fmclient sync_ou_group	177
fmpolicy copy-global-object	178
fmpolicy install-config	178
fmpolicy print-device-database	179
fmpolicy print-global-database	179
fmpolicy print-global-object	179
fmscript clean-sched	179
fmscript delete	180
fmscript import	180
fmscript list	181
fmscript run	181
fmscript showlog	182
fmupdate {ftp scp tftp} import	183
fmupdate {ftp scp tftp} export	183
format disk	184
ping	185
raid	185
reboot	186
reset	186
restore	186
shutdown	187
ssh	188
time	188
top	188
traceroute	189
diagnose	190
cdb check	190
debug application	191
debug cli	194
debug crashlog	194
debug disable	194
debug dpm	194

debug enable	195
debug info	195
debug sysinfo	195
debug timestamp	195
debug vminfo	196
dvm adom	196
dvm check-integrity	196
dvm debug	197
dvm device	197
dvm device-tree-update	197
dvm group	197
dvm lock	197
dvm proc	198
dvm task	198
dvm transaction-flag	198
fgfm	199
fmclient cache	199
fmclient data	200
fmclient eventlog	201
fmclient log	201
fmclient performance	202
fmnetwork arp	202
fmnetwork interface	202
fmnetwork netstat	203
fmsystem admin-session	204
fmsystem disk	204
fmsystem export	205
fmsystem flash	205
fmsystem fsck	205
fmsystem logtoconsole	206
fmsystem ntp	206
fmsystem print	206
fmsystem process	207
fmsystem raid	208
fmsystem route	208
fmsystem server	208
fmupdate	209
fwmanager	213
ha	214
hardware	214

rtm.....	215
sniffer	215
test application	220
test deploymanager	221
test policy-check	221
test search	221
test sftp	222
test sysalert.....	222
get	223
fcdevice temp	223
fcdevice unlicensed	224
fmclient status.....	224
fmsystem status.....	225
fmsystem performance	225
show	226
Index	227

Change Log

Date	Change Description
2012-04-11	Initial release.
2012-06-27	Change Log added.
2012-08-08	Added integer value for the set autosync-interval command. Default is 10 minutes. Updated Table 3 Administrative Domains/Network Devices per FortiManager model.
2012-10-01	Updated document template.
2012-12-04	Minor update.
2013-02-21	Updated for FortiManager v4.0 MR3 Patch Release 7.
2013-11-25	Updated for FortiManager v4.0 MR3 Patch Release 8.

Introduction

FortiManager centralized management appliances deliver the essential tools needed to effectively manage your Fortinet-based security infrastructure.

Using the FortiManager system, you can:

- configure multiple FortiGate units (including FortiGate, FortiWiFi, FortiGate One, and FortiGate VM), FortiCarrier units, FortiMail units, FortiSwitch units, and FortiClient endpoint security agents,
- segregate management of large deployments easily and securely by grouping devices and agents into geographic or functional administrative domains (ADOMs),
- configure and manage VPN policies,
- monitor the status of these units,
- view device logs,
- update the antivirus and attack signatures,
- provide web filtering and email filtering service to the licensed devices as a local FortiGuard Distribution Network (FDN) server, and
- update the firmware images of the devices.

The FortiManager system scales to manage up to 10000 devices and virtual domains (VDOMS), and up to 120000 FortiClient agents from a single FortiManager interface. It is designed for medium to large enterprises and managed security service providers. FortiManager system architecture emphasizes reliability, scalability, ease of use, and easy integration with third-party systems.

This chapter contains following topics:

- [About the FortiManager system](#)
- [Web-based Manager](#)
- [FortiManager system product life cycle](#)

About the FortiManager system

The FortiManager system is a security-hardened appliance with simplified installation, and improved system reliability and security. You can install a second peer FortiManager system for database backups.

The FortiManager system manages communication between the managed devices and the FortiManager Web-based Manager.

The FortiManager system stores and manages all managed devices' configurations.

It can also act as a local FDN server for the managed devices to download virus and attack signatures, and to use the web filtering and email filtering service. This will significantly reduce network delay and usage, compared with the managed devices' connection to an FDN server over the Internet.

Web-based Manager

You can use the FortiManager Web-based Manager to configure the managed devices and to view the device configuration, device status, system health, real time logs, and historical logs. The FortiManager Web-based Manager supports role-based administration. Permissions and device access can be set individually for each manager account added to the FortiManager Web-based Manager.

Administrators with read and write access can view the configuration, health status, and logs, and can change the configurations of the devices assigned to them. The FortiManager Web-based Manager also allows these users to remotely upgrade device firmware, and virus and attack definitions.

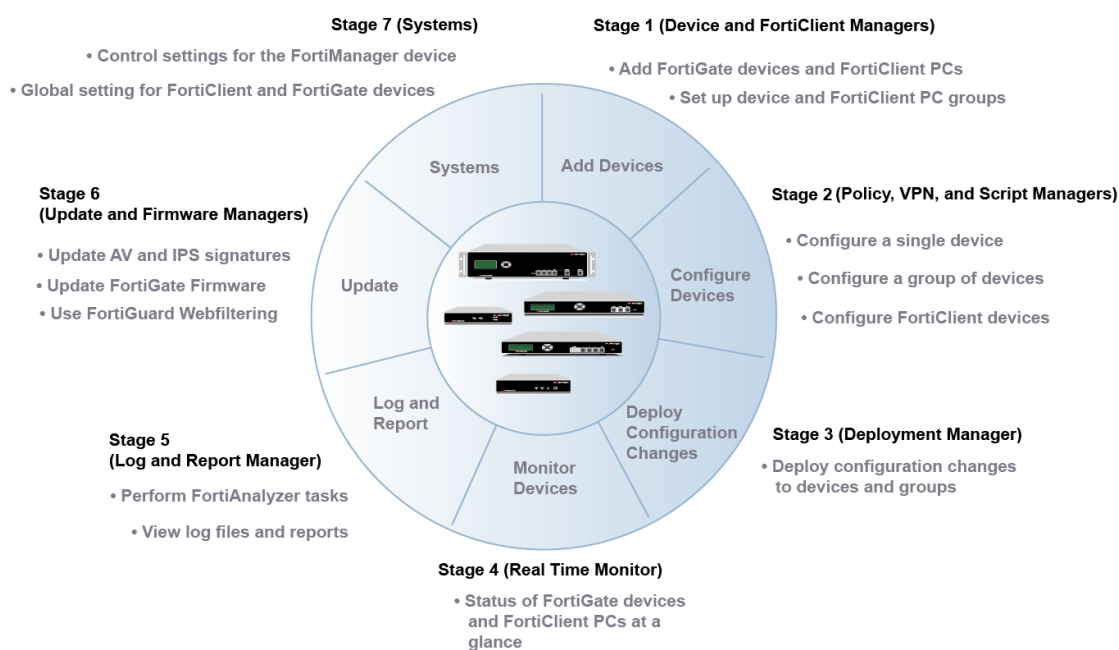
Administrators with read only access can view the configuration, device status, system health, real time logs, and historical logs of the devices assigned to them.

FortiManager system product life cycle

The FortiManager system allows you to manage devices through their entire product life cycle:

Deployment	Complete device configuration after initial installation.
Monitoring	Real-time monitoring of device status and health.
Maintenance	Continuous, incremental configuration and updates.
Updates	Updates of virus definitions, attack definitions, web filtering service, email filtering service, and firmware images.

Figure 1: FortiManager System product life cycle



What's New in FortiManager v4.0 MR3

The tables below list commands which have changed in this v4.0 MR3 release.

Command	Change
<code>config fmsystem global</code>	Added new variables: <ul style="list-style-type: none">• <code>enc-algorithm</code>• <code>language</code>• <code>admintimeout</code>• <code>remoteauthtimeout</code>• <code>ldapconntimeout</code>• <code>max-concurrent-users</code>• <code>webservice-support-ssl3</code>• <code>workspace</code>
<code>config fmsystem interface</code>	Added new variables: <ul style="list-style-type: none">• <code>description</code>• <code>alias</code>
<code>config fmsystem snmp sysinfo</code>	Added new variables: <ul style="list-style-type: none">• <code>engine-id</code>• <code>trap-high-cpu-threshold</code>• <code>trap-low-memory-thresholds</code>
<code>config fmsystem snmp user</code>	Added command and related variables.
<code>config fmsystem ha</code>	Added a new variable: <ul style="list-style-type: none">• <code>peer status</code>
<code>config fmsystem ntp</code>	Added ntp server information: <ul style="list-style-type: none">• <code>ntpv3</code>• <code>authentication</code>• <code>key</code>• <code>key-id</code>
<code>config fmsystem locallog fortianalyzer setting</code>	Added new variable: <ul style="list-style-type: none">• <code>diskfull</code>

Command	Change
config fmsystem admin profile	<p>Added new variables:</p> <ul style="list-style-type: none"> • scope • admin-setting • global-policy-packages • global-objects • profile-perm • device-manager • device-config • config-retrieve • term-access • adom-policy-package • adom-policy-object • forticonsole • consistency-check • network • admin • system • devices • alerts • dlp • reports • logs • quar • net-monitor • vuln-mgmt <p>Removed variables:</p> <ul style="list-style-type: none"> • device-summary • group-op • script-database • fwimage-database • fgd-center • all devcfg variables • script-management • service-usage • firmware-management • security-console • domain-install • global-storage • web-portal • gms-retrieve

Command	Change
config fmsystem admin ldap	Added new variables: <ul style="list-style-type: none"> • secure
config fmsystem admin user	Added variables: <ul style="list-style-type: none"> • password-expire • force-password-change • last-name • first-name • email-address • phone-number • mobile-number • pager-number • hidden • dashboard-tab tabid • dashboard-tabs name • dashboard moduleid • dashboard name • dashboard column • dashboard refresh-interval • dashboard status • dashboard tabid • dashboard widget-type • dashboard log-rate-type • dashboard log-rate-topn • dashboard log-rate-period • dashboard res-view-type • dashboard res-period • dashboard num-entries

Command	Change
<code>config fmsystem admin setting</code>	<p>Added variables:</p> <ul style="list-style-type: none"> • <code>chassis-mgmt</code> • <code>chassis-update-interval</code> • <code>access-banner</code> • <code>banner-message</code> • <code>install-ifpolicy-only</code> • <code>show-global-policy-settings</code> • <code>show-global-object-settings</code> • <code>show-adom-ipv6-settings</code> • <code>show-adom-dynamic-objects</code> • <code>show-adom-dos-policies</code> • <code>show-adom-sniffer-policies</code> • <code>show-adom-central-nat-policies</code> • <code>show-adom-taskmon-button</code> • <code>show-adom-terminal-button</code> • <code>show-adom-policy-consistency-button</code> • <code>show-adom-forticonsole-button</code> • <code>show-adom-rtmlog</code> • <code>show-adom-vpnman</code> • <code>show-adom-devman</code> • <code>show-adom-web-portal</code> • <code>show-fortimail-settings</code> • <code>show-foc-settings</code> • <code>show-fcm-settings</code> • <code>show-fsw-settings</code> • <code>show-device-import-export</code> <p>Removed variables:</p> <ul style="list-style-type: none"> • <code>device-locks</code>
<code>config fmsystem password-policy</code>	Added command and related variables.
<code>config fmsystem log rolling</code>	Removed command.
<code>config fmsystem dm</code>	Added command and related variables.
<code>config fmupdate av-ips fgt</code>	Added server list id variable.
<code>config fmupdate av-ips fct</code>	Added server list id variable.
<code>config fmupdate web-spam fgt</code>	Removed command.

Command	Change
<code>config fmupdate service</code>	<p>Added variable:</p> <ul style="list-style-type: none"> • <code>use-cert</code> <p>Removed variable:</p> <ul style="list-style-type: none"> • <code>web-spam</code>
<code>config fmupdate service-access-priorities</code>	<p>Added variables:</p> <ul style="list-style-type: none"> • <code>private-server id</code> • <code>private-server ip</code> • <code>private-server time_zone</code> <p>Removed variable:</p> <ul style="list-style-type: none"> • <code>web-spam</code> • <code>lookup_default_server</code>
<code>config fmupdate custom-url-list</code>	Removed command.
<code>config fmupdate server-override-status</code>	Added command and related variables.
<code>config fmupdate multilayer</code>	Added command and related variables.
<code>config fmupdate support-pre-fgt43</code>	Added command and related variables.
<code>config fmclient ad_grouping_setting</code>	Added command and related variables.
<code>config fmclient ad_ou_grouping</code>	Added command and related variables.
<code>config fmclient location-aware</code>	Added command and related variables.
<code>config fcdevice group</code>	<p>Variable units changed.</p> <p>Added variable:</p> <ul style="list-style-type: none"> • <code>groupid</code>
<code>config fcpolicy system locationaware</code>	Added command.
<code>diagnose cdb check</code>	Added command and related variables.
<code>diagnose debug application</code>	<p>Added variables:</p> <ul style="list-style-type: none"> • <code>fgdsvr</code> • <code>fgdupd</code> • <code>sqlrptcached</code> <p>Variable removed:</p> <ul style="list-style-type: none"> • <code>vm-fdsclient</code>
<code>diagnose fmsystem export</code>	<p>Added variable:</p> <ul style="list-style-type: none"> • <code>upgradelog</code>
<code>diagnose fmsystem raid</code>	Added command and related variables.

Command	Change
diagnose fwmanager	Added variables: <ul style="list-style-type: none"> • set-devsched • set-grpsched • getall-schedule • reset-schedule-database
diagnose hardware	Added command and related variables.
diagnose test deploymanager	Added variable: <ul style="list-style-type: none"> • reloadconf
diagnose dvm	Added variable: <ul style="list-style-type: none"> • device-tree-update
diagnose rtm	Added variables: <ul style="list-style-type: none"> • snmp-community-name get • snmp-community-name set
execute devicelog clear	Added command.
execute fcpolicy deploy	Variable units changed.
execute sql-local	Added commands and related variables.
execute sql-query-dataset	Added command and related variables.
execute sql-query-generic	Added command.
execute reset-sqllog-transfer	Added command.
execute sql-report	Added command and related variables.
execute log_aggregation	Added command.
execute fcpolicy retrieve unit	Variable units changed.
execute fcpolicy unit	Variable units changed.
execute fcpolicy revoke	Variable units changed.
execute fcpolicy grant	Variable units changed.
execute fcpolicy install-config	Added command.
execute fcpolicy print-global-onject	Added command.
execute fmclient apply-lockdown	Variables' units changed.
execute fcdevice find-unit	Added command.
execute fmupdate scp	Added command.

Command	Change
<code>execute fmscript clean-sched</code>	Added command.
<code>execute format</code>	<p>Added variables:</p> <ul style="list-style-type: none"> • <code>disk-ext4</code> • <code>disk_partition_2-ext4</code> • <code>disk_partition_3-ext4</code> <p>If the FortiManager has RAID configured, the 'disk-ext4 is replaced with the value for the RAID level.</p>

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.

For example:

```
execute restore image ftp <filepath>
```

You enter:

```
execute restore image ftp myfile.bak
```

`<xxx_ipv4>` indicates a dotted decimal IPv4 address.

`<xxx_v4mask>` indicates a dotted decimal IPv4 network mask.

`<xxx_ipv4mask>` indicates a dotted decimal IPv4 address followed by a dotted decimal IPv4 network mask.

- 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 keyword or variable is optional.

For example:

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

To show the settings for all interfaces, you can enter `show fmsystem interface`. To show the settings for the Port1 interface, you can enter `show fmsystem 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 ssh}
```

You can enter any of the following:

```
set allowaccess ping
```

```
set allowaccess https ping
```

```
set allowaccess ssh
set allowaccess https ssh
set allowaccess https ping ssh
```

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 or SSH to connect to the FortiManager CLI.

- [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 Web-based Manager](#)

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 the FortiManager unit is powered on.
3. Start HyperTerminal, enter a name for the connection, and select *OK*.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the FortiManager console port.
5. Select *OK*.
6. Select the following port settings and select *OK*.

Bits per second	115200
Data bits	8

Parity	None
Stop bits	1
Flow control	None

7. Press `Enter` to connect to the FortiManager CLI.
A prompt similar to the following appears (shown for the FMG-400C):
FMG400C login:
8. Type a valid administrator name and press `Enter`.
9. Type the password for this administrator and press `Enter`.
A prompt similar to the following appears (shown for the FMG-400C):
FMG400C #
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 SSH access. If you want to use the Web-based Manager, you need HTTPS access.

To use the Web-based Manager 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 fmsystem 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 fmsystem 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 fmsystem interface <interface_name>

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

Connecting to the FortiManager CLI using SSH

Secure Shell (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.



A maximum of 5 SSH connections can be open at the same time.

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. Type a valid administrator name and press `Enter`.
4. Type 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 Web-based Manager

The Web-based Manager also provides a CLI console window.

To connect to the CLI using the Web-based Manager:

1. Connect to the Web-based Manager and log in.
For information about how to do this, see the [FortiManager Administration Guide](#).
2. Go to *System Settings > General > Dashboard*.
3. In *System Information* section, select *Connect to CLI Console*.
The Admin Console window opens. If asked, accept the application's certificate.
4. When you are finished using the console, select *Disconnect* and then select *Close*.

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.

Table 1: CLI objects

fmsystem	Configures options related to the overall operation of the FortiManager unit, such as interfaces, virtual domains, and administrators. See “ fmsystem ” on page 38 .
fmupdate	Configures settings related to FortiGuard service updates and the FortiManager unit's built-in FDS. See “ fmupdate ” on page 92 .

Table 1: CLI objects (continued)

fmclient	Configures the FortiManager settings used to manage clustering, discovering and adding FortiClient agents, licenses, client lockdown, and web filtering for managed FortiClient agents. See “fmclient” on page 110 .
fcdevice	Configures FortiClient agents and client groups. See “fcdevice” on page 123 .
fcpolicy	Configures the settings of FortiClient agents or client groups. See “fcpolicy” on page 127 .

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. See also [“Example command sequences” on page 29](#).

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 fmsystem 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	<p>Add an entry to the FortiManager configuration or edit an existing entry. For example in the <code>config system admin shell</code>:</p> <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	<p>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.</p> <p>The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.</p>
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	<p>Remove all entries configured in the current shell. For example in the <code>config user local shell</code>:</p> <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 <code>config</code> command while editing a table entry. An example of this is the command to add host definitions to an SNMP community.
end	<p>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.</p> <p>The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.</p>
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	<p>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 fmsystem admin user shell</code>.</p> <ul style="list-style-type: none"> • Type <code>edit User1</code> and press <code>Enter</code>. • Use the <code>set</code> commands to configure the values for the new admin account. • Type <code>next</code> to save the configuration for User1 without leaving the <code>config fmsystem admin user shell</code>. • Continue using the <code>edit</code>, <code>set</code>, and <code>next</code> commands to continue adding admin user accounts. • type <code>end</code> and press <code>Enter</code> to save the last configuration and leave the shell.
set	<p>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>.</p> <p>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.</p>
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.

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.

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

Example

When you type `get` in the `config fmsystem 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
description      : (null)
password         : *
profileid        : Super_User
trusthost1       : 0.0.0.0 0.0.0.0
trusthost2       : 0.0.0.0 0.0.0.0
trusthost3       : 127.0.0.1 255.255.255.255
```

Example

You want to confirm the IP address and network mask of the `port1` interface from the root prompt.

At the `#` prompt, type:

```
get fmsystem interface port1
```

The screen displays:

```
name             : port1
status           : up
ip               : 172.20.120.160 255.255.255.0
allowaccess       : ping https ssh
```

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

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 fmsystem interface
edit "port1"
set ip 172.20.120.160 255.255.255.0
set allowaccess ping https ssh
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 fmsystem dns
```

The screen displays:

```
config fmsystem dns
  set primary 65.39.139.53
  set secondary 65.39.139.63
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.

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

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 technical 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 fmsystem 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. Type `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`.

7. If you want to leave the `config system dns` shell without saving your changes, type `abort` and press `Enter`.

8. To save your changes and exit the `dns` sub-shell, type `end` and press `Enter`.

9. To confirm your changes have taken effect after leaving the `dns` sub-shell, type `get fmsystem dns` and press `Enter`.

CLI basics

This section includes:

- [Command help](#)
- [Command completion](#)
- [Recalling commands](#)
- [Editing commands](#)
- [Line continuation](#)
- [Command abbreviation](#)
- [Environment variables](#)
- [Encrypted password support](#)
- [Entering spaces in strings](#)
- [Entering quotation marks in strings](#)
- [Entering a question mark \(?\) in a string](#)
- [International characters](#)
- [Special characters](#)
- [IP address formats](#)
- [Editing the configuration file](#)
- [Changing the baud rate](#)

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.
- Type 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.
- Type 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 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 the Backspace and Delete keys and the control keys listed in [Table 2](#) to edit the command.

Table 2: Control keys for editing commands

Function	Key combination
Beginning of line	Ctrl+A
End of line	Ctrl+E
Back one character	Ctrl+B
Forward one character	Ctrl+F
Delete current character	Ctrl+D
Previous command	Ctrl+P
Next command	Ctrl+N
Abort the command	Ctrl+C
If used at the root prompt, exit the CLI	Ctrl+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 unambiguous 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 IP 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 fmsystem admin user user1
config fmsystem admin user
    edit "user1"
        set password ENC UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1
        rVJmMFc9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxskRcU3E9Xq
        Oit82PgScwzGzGuJ5a9f
        set profileid "Standard_User"
    next
end
```

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

```
config system admin
```

and press Enter.

Type:

```
edit user1
```

and press Enter.

Type:

```
set password ENC UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMF
c9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxskRcU3E9XqOit82PgScwz
GzGuJ5a9f
```

and press **Enter**.

Type:

```
end
```

and 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.

IP address formats

You can enter an IP 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 IP address is displayed in the configuration file in dotted decimal format.

Editing the configuration file

You can change the FortiManager configuration by backing up the configuration file to a TFTP server. Then you can make changes to the file and restore it to the FortiManager unit.

1. Use the `execute backup all-settings` command to back up the configuration file to a TFTP server. For example,

```
execute backup all-settings 10.10.0.1 mybackup.cfg myid mypass
```

2. Edit the configuration file using a text editor.

Related commands are listed together in the configuration file. For instance, all the system commands are grouped together. You can edit the configuration by adding, changing or deleting the CLI commands in the configuration file.

The first line of the configuration file contains information about the firmware version and FortiManager model. Do not edit this line. If you change this information the FortiManager unit will reject the configuration file when you attempt to restore it.

3. Use the `execute restore all-settings` command to copy the edited configuration file back to the FortiManager unit. For example,

```
execute restore all-settings 10.10.0.1 mybackup.cfg myid mypass
```

The FortiManager unit receives the configuration file and checks to make sure the firmware version and model information is correct. If it is, the FortiManager unit loads the configuration file and checks each command for errors. If the FortiManager unit finds an error, an error message is displayed after the command and the command is rejected. Then the FortiManager unit restarts and loads the new configuration.

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.

Administrative Domains

This chapter provides information about the Administrative Domain (ADOM) functionality introduced in FortiManager v4.0.

This chapter includes the following sections:

- [ADOMs overview](#)
- [Configuring ADOMs](#)

ADOMs overview

FortiManager can manage a large number of Fortinet devices. Administrative domains (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 36](#).

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

Table 3: Number of Administrative Domains/Network Devices per FortiManager model

FortiManager Model	Administrative Domain/Network Devices
FMG-200D	30/30
FMG-400C	300/300
FMG-1000C	800/800
FMG-3000C	5000/5000
FMG-5001A	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.

Within the CLI, you can enable ADOMs and set the administrator ADOM. To configure the ADOMs, you must use the Web-based Manager.

To enable or disable ADOMs:

Enter the following CLI command:

```
config fmsystem 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 a reduced operation mode and more complicated management scenarios. It is recommended only for advanced users.

To change administrative domain device modes:

Enter the following CLI command:

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

To assign an administrator to an ADOM:

Enter the following CLI command:

```
config fmsystem admin user
    edit 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 or 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.



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:

```
config fmsystem global
    set workspace enable
end
```

To disable ADOM locking and enable concurrent ADOM access:

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

fmsystem

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

This chapter contains following sections:

admin ldap	dm	log fortianalyzer
admin profile	dns	log setting
admin radius	fips	mail
admin setting	global	metadata
admin tacacs	ha	ntp
admin user	interface	password-policy
alert-console	locallog disk setting	route
alert-event	locallog filter	snmp community
alertemail	locallog fortianalyzer setting	snmp sysinfo
backup all-settings	locallog memory setting	snmp user
certificate ca	locallog syslogd (syslogd2, syslogd3) setting	syslog
certificate local		

For more information about configuring ADOMs, see “Administrative Domains” on page 35.

admin ldap

Use this command to add, edit, and delete LDAP users.

Syntax

```
config fmsystem admin ldap
  edit name {LDAP server entry name}
    set server {name_str | ip_str}
    set cnid <string>
    set dn <string>
    set port <integer>
    set type {anonymous | regular | simple}
    set username <string>
    set password <string>
    set group <string>
    set filter <query_string>
    set secure {disable | ldaps | starttls}
```

end

Variable	Description
server {name_str ip_str}	Enter the LDAP server domain name or IP address.
cnid <string>	Enter common name identifier.
dn <string>	Enter the distinguished name.
port <integer>	Enter the port number for LDAP server communication. Default: 389
type {anonymous regular simple}	Set a binding type: <ul style="list-style-type: none">anonymous: Bind using anonymous user searchregular: Bind using username/password and then searchsimple: Simple password authentication without search Default: simple
username <string>	Enter a username. This keyword appears only when type is set to regular.
password <string>	Enter a password for the username above. This keyword appears only when type is set to regular.
group <string>	Enter an authorization group. The authentication user must be a member of this group (full DN) on the server.
filter <query_string>	Enter content for group searching. For example: (&(objectcategory=group) (member=*)) (&(objectclass=groupofnames) (member=*)) (&(objectclass=groupofuniquenames) (uniquemember=*)) (&(objectclass=posixgroup) (memberuid=*))
secure {disable ldaps starttls}	Set the SSL connection type: <ul style="list-style-type: none">disable: no SSLldaps: use LDAPSstarttls: use STARTLS

Example

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

```
config fmsystem 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
```

Related topics

- [admin profile](#)

admin profile

Use this command to configure access profiles. In a newly-created access profile, no access is enabled.

Syntax

```
config fmsystem admin profile
edit <profile_name>
    set description <text>
    set scope <adom | global>
    set system-setting {none | read-write}
    set admin-setting {none | read | read-write}
    set adom-switch {none | read | read-write}
    set global-policy-packages {none | read | read-write}
    set global-objects {none | read | read-write}
    set profile-perm {none | read | read-write}
    set read-passwd {none | read | read-write}
    set device-manager {none | read | read-write}
    set device-config {none | read | read-write}
    set device-op {none | read | read-write}
    set deploy-management {none | read | read-write}
    set config-retrieve {none | read | read-write}
    set term-access {none | read | read-write}
    set adom-policy-packages {none | read | read-write}
    set adom-policy-objects {none | read | read-write}
    set vpn-manager {none | read | read-write}
    set realtime-monitor {none | read | read-write}
    set fct-manager {none | read | read-write}
    set forticonsole {none | read | read-write}
    set consistency-check {none | read | read-write}
    set faz-management {none | read | read-write}
    set network {none | read | read-write}
    set admin {none | read | read-write}
    set system {none | read | read-write}
    set devices {none | read | read-write}
    set alerts {none | read | read-write}
    set dlp {none | read | read-write}
    set reports {none | read | read-write}
    set logs {none | read | read-write}
    set quar {none | read | read-write}
    set net-monitor {none | read | read-write}
    set vuln-mgmt {none | read | read-write}
```

end

Variable	Description
<profile_name>	Edit the access profile. Enter a new name to create a new profile. The pre-defined access profiles are Super_User, Standard_User and Restricted_User.
description <text>	Enter a description for this access profile. Enclose the description in quotes if it contains spaces.
scope <adom global>	Set the scope for this access profile to either ADOM or Global. Default: global
system-setting {none read-write}	Set the level of access to system settings for this profile.
admin-setting {none read read-write}	Set the administration settings for this profile.
adom-switch {none read read-write}	Set the administrator domain for this profile.
global-policy-packages {none read read-write}	Set the global policy packages for this profile.
global-objects {none read read-write}	Set the global objects for this profile.
profile-perm {none read read-write}	Set the profile permissions.
read-passwd {none read read-write}	Add the capability to view the authentication password in clear text to this profile.
device-manager {none read read-write}	Enter the level of access to device manager settings for this profile.
device-config {none read read-write}	Enter the level of access to device configuration settings for this profile.
device-op {none read read-write}	Add the capability to add, delete, and edit devices to this profile.
deploy-management {none read read-write}	Enter the level of access to the deployment management configuration settings for this profile.
config-retrieve {none read read-write}	Set the configuration retrieve settings for this profile.
term-access {none read read-write}	Set the terminal access for this profile.
adom-policy-packages {none read read-write}	Enter the level of access to ADOM policy packages for this profile.
adom-policy-objects {none read read-write}	Enter the level of access to ADOM policy objects for this profile.

Variable	Description
vpn-manager {none read read-write}	Enter the level of access to VPN console configuration settings for this profile.
realtime-monitor {none read read-write}	Enter the level of access to the Real-Time monitor configuration settings for this profile.
fct-manager {none read read-write}	Enter the level of access to the FortiClient manager configuration settings for this profile.
forticonsole {none read read-write}	Enable or disable the FortiConsole for this profile.
consistency-check {none read read-write}	Enable or disable consistency check for this profile.
faz-management {none read read-write}	Enter the level of access to FortiAnalyzer configuration management settings for this profile.
network {none read read-write}	Enable or disable access permission.
admin {none read read-write}	Enable or disable access permission.
system {none read read-write}	Enable or disable access permission.
devices {none read read-write}	Enable or disable access permission.
alerts {none read read-write}	Enable or disable access permission.
dlp {none read read-write}	Enable or disable access permission.
reports {none read read-write}	Enable or disable access permission.
logs {none read read-write}	Enable or disable access permission.
quar {none read read-write}	Enable or disable access permission.
net-monitor {none read read-write}	Enable or disable access permission.
vuln-mgmt {none read read-write}	Enable or disable access permission.

Related topics

- [admin radius](#)

admin radius

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

Syntax

```
config fmsystem admin radius
  edit <server>
    set auth-type <auth_prot_type>
    set nas-ip <ip>
    set port <integer>
    set secret <passwd>
    set secondary-secret <passwd>
    set server <string>
    set secondary-server <string>
  end
```

Variable	Description
auth-type <auth_prot_type>	Enter the authentication protocol the RADIUS server will use. <ul style="list-style-type: none">• any — use any supported authentication protocol• mschap2• chap• pap
nas-ip <ip>	Enter the NAS IP address.
port <integer>	Enter the RADIUS server port number. Default: 1812
secret <passwd>	Enter the password to access the RADIUS server.
secondary-secret <passwd>	Enter the password to access the RADIUS secondary-server.
server <string>	Enter the RADIUS server DNS resolvable domain name or IP address.
secondary-server <string>	Enter the RADIUS secondary-server DNS resolvable domain name or IP address.

Example

This example shows how to add the RADIUS server RAD1 at the IP address 206.205.204.203 and set the shared secret as R1a2D3i4U5s.

```
config fmsystem admin radius
  edit RAD1
    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 fmsystem admin setting
  set access-banner
  set admin_server_cert <admin_server_cert>
  set allow_register {enable | disable}
  set autosync {enable | disable}
  set autosync_interval <integer>
  set banner-message <string>
  set chassis-mgmt
  set chassis-update-interval
  set demo-mode {enable | disable}
  set device_sync_status {enable | disable}
  set http_port <integer>
  set https_port <integer>
  set idle_timeout <integer>
  set install-ifpolicy-only {enable | disable}
  set mgmt-addr <string>
  set offline_mode {enable | disable}
  set register_passwd <password>
  set show-add-multiple {enable | disable}
  set show-adom-central-nat-policies {enable | disable}
  set show-adom-devman {enable | disable}
  set show-adom-dos-policies {enable | disable}
  set show-adom-dynamic-objects {enable | disable}
  set show-adom-forticonsole-button {enable | disable}
  set show-adom-icap-policies {enable | disable}
  set show-adom-implicit-policy {enable | disable}
  set show-adom-ipv6-settings {enable | disable}
  set show-adom-policy-consistency-button {enable | disable}
  set show-adom-rtmlog {enable | disable}
  set show-adom-sniffer-policies {enable | disable}
  set show-adom-taskmon-button {enable | disable}
  set show-adom-terminal-button {enable | disable}
  set show-adom-voip-policies {enable | disable}
  set show-adom-vpnman {enable | disable}
  set show-adom-web-portal {enable | disable}
  set show-device-import-export {enable | disable}
  set show-fcm-settings {enable | disable}
  set show-foc-settings {enable | disable}
  set show-fortimail-settings {enable | disable}
  set show-fsw-settings {enable | disable}
  set show-global-object-settings {enable | disable}
  set show-global-policy-settings {enable | disable}
```

```

set unreg_dev_opt {add_allow_service | add_no_service | ignore}
set webadmin_language {auto_detect | english | japanese |
    simplified_chinese | traditional_chinese}
end

```

Variable	Description
access-banner	Enable or disable the access banner. Default: disable
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 an unregistered device to be registered. Default: disable
autosync {enable disable}	Set the automatic synchronization of device configurations. Default: disable
autosync_interval <integer>	Enter the time in minutes after the last device configuration to synchronize the device configuration. (5, 10, 15, 20, 25, 30 minutes). Default: 10
banner-message <string>	Enable the banner messages. Maximum of 255 characters.
chassis-mgmt	Enable or disable chassis management. Default: disable
chassis-update-interval	Set the chassis background update interval (4 - 1440 minutes). Default: 15
demo-mode {enable disable}	Enable demo mode. Default: disable
device_sync_status {enable disable}	Enable or disable device synchronization status indication. Default: enable
http_port <integer>	Enter the HTTP port number for web administration. Default: 80
https_port <integer>	Enter the HTTPS port number for web administration. Default: 443
idle_timeout <integer>	Enter the idle timeout value. The range is from 1 to 480 minutes. Default: 5
install-ifpolicy-only {enable disable}	Enable to allow only the interface policy to be installed. Default: disable

Variable	Description
mgmt-addr <string>	GQDN/IP of FortiManager used by FGFM.
offline_mode {enable disable}	Enable offline mode to shut down the protocol used to communicate with managed devices. Default: disable
register_passwd <password>	Enter the password to use when registering a device.
show-add-multiple {enable disable}	Show the add multiple button.
show-adom-central-nat-policies {enable disable}	Show ADOM central NAT policy settings on the Web-based Manager. Default: disable
show-adom-devman {enable disable}	Show ADOM device manager tools on the Web-based Manager. Default: disable
show-adom-dos-policies {enable disable}	Show ADOM DOS policy settings on the Web-based Manager. Default: disable
show-adom-dynamic-objects {enable disable}	Show ADOM dynamic object settings on the Web-based Manager. Default: enable
show-adom-forticonsole-button {enable disable}	Show ADOM banner button FortiConsole on the Web-based Manager. Default: enable
show-adom-icap-policies {enable disable}	Show the ADOMICAP policy settings in the Web-based Manager.
show-adom-implicit-policy {enable disable}	Show the ADOM implicit policy settings in the Web-based Manager.
show-adom-ipv6-settings {enable disable}	Show ADOM IPv6 settings in the Web-based Manager. Default: disable
show-adom-policy-consistency-button {enable disable}	Show ADOM banner button Policy Consistency in the Web-based Manager. Default: disable
show-adom-rtmlog {enable disable}	Show ADOM RTM device log in the Web-based Manager. Default: disable
show-adom-sniffer-policies {enable disable}	Show ADOM sniffer policy settings in the Web-based Manager. Default: disable

Variable	Description
<code>show-adom-taskmon-button</code> {enable disable}	Show ADOM banner button Task Monitor in the Web-based Manager. Default: enable
<code>show-adom-terminal-button</code> {enable disable}	Show ADOM banner button Terminal in the Web-based Manager. Default: enable
<code>show-adom-voip-policies</code> {enable disable}	Show ADOM VoIP policy settings in the Web-based Manager.
<code>show-adom-vpnman</code> {enable disable}	Show ADOM VPN manager in the Web-based Manager. Default: enable
<code>show-adom-web-portal</code> {enable disable}	Show ADOM web portal settings in the Web-based Manager. Default: disable
<code>show-device-import-export</code> {enable disable}	Enable import/export of ADOM, device, and group lists.
<code>show-fcm-settings</code> {enable disable}	Show FortiClient Manager settings in the Web-based Manager. Default: disable
<code>show-foc-settings</code> {enable disable}	Show FortiCarrier settings in the Web-based Manager. Default: disable
<code>show-fortimail-settings</code> {enable disable}	Show FortiMail settings in the Web-based Manager. Default: disable
<code>show-fsw-settings</code> {enable disable}	Show FortiSwitch settings in the Web-based Manager. Default: disable
<code>show-global-object-settings</code> {enable disable}	Show global object settings in the Web-based Manager. Default: enable
<code>show-global-policy-settings</code> {enable disable}	Show global policy settings in the Web-based Manager. Default: enable

Variable	Description
unreg_dev_opt {add_allow_service add_no_service ignore}	<p>Select action to take when an unregistered device connects to FortiManager.</p> <ul style="list-style-type: none"> add_allow_service: Add unregistered devices and allow service requests. add_no_service: Add unregistered devices and deny service requests. ignore: Ignore unregistered devices. <p>Default: add_allow_service</p>
webadmin_language {auto_detect english japanese simplified_chinese traditional_chinese}	<p>Enter the language to be used for web administration.</p> <p>Default: auto_detect</p>

admin tacacs

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

Syntax

```
config fmsystem admin tacacs
  edit <name_str>
    set authen-type <auth_prot_type>
    set key <passw>
    set port <integer>
    set server <string>
  end
```

Variable	Description
authen-type <auth_prot_type>	<p>Choose which authentication type to use.</p> <p>Default: auto</p>
key <passw>	Key to access the server.
port <integer>	Port number of the TACACS+ server.
server <string>	The server domain name or IP

Example

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

```
config fmsystem 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. For information about ADOMs, see "Administrative Domains" on page 35.



You can create meta-data fields for administrator accounts. These objects must be created using the FortiManager Web-based Manager. 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 v4.0 Administration Guide*.

Syntax

```
config fmsystem admin user
  edit <name_str>
    set password <password>
    set trusthost1 <ip_mask>
    set trusthost2 <ip_mask>
    set trusthost3 <ip_mask>
    set profileid <profile-name>
    set adom <adom_name(s)>
    set restrict-access {enable | disable}
    set description <string>
    set user_type <local | radius | ldap | tacacs-plus>
    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 wildcard <enable | disable>
    set radius-accprofile-override <enable | disable>
    set radius-adom-override <enable | disable>
    set radius-group-match <string>
    set last-name <string>
    set first-name <string>
    set email-address <string>
    set phone-number <string>
    set mobile-number <string>
    set pager-number <string>
  end
  config meta-data
    edit <fieldname>
      set fieldlength
```

```

        set fieldvalue <string>
        set importance
        set status
    end
end
config dashboard
    edit
        set moduleid
        set name <string>
        set column <column_pos>
        set refresh-interval <integer>
        set status {close | open}
        set tabid <integer>
        set widget-type <string>
        set num-entries <integer>
        set log-rate-type {device | log}
        set log-rate-topn <integer>
        set log-rate-period {1hour | 3min | 6hours}
        set res-view-type {history | real-time}
        set res-period {10min | day | hour}
    end
end
config restrict-dev
    edit <string>
end
end

```

Variable	Description
password <password>	Enter a password for the administrator account. For improved security, the password should be at least 6 characters long. This keyword is available only if <code>user_type</code> is <code>local</code> .
trusthost1 <ip_mask> trusthost2 <ip_mask> trusthost3 <ip_mask>	<p>Optionally, type the trusted host IP address and network mask from which the administrator can log in to the FortiManager system. You can specify up to three trusted hosts.</p> <p>Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see "Using trusted hosts".</p> <p>Default: 0.0.0.0, 255.255.255.255, 255.255.255</p>
profileid <profile-name>	<p>Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiManager features.</p> <p>Default: Restricted_User</p>
adom <adom_name(s)>	<p>Enter the name(s) of the ADOM(s) the administrator belongs to. Any configuration of ADOMs takes place via the FortiManager Web-based Manager. For more information, see "Administrative Domains" on page 35.</p>

Variable	Description
<code>restrict-access {enable disable}</code>	Enable or disable restricted access to the dev-vdom. Default: disable
<code>description <string></code>	Enter a description for this administrator account. When using spaces, enclose description in quotes.
<code>user_type <local radius ldap tacacs-plus></code>	Enter <code>local</code> if the FortiManager system verifies the administrator's password. Enter <code>radius</code> if a RADIUS server verifies the administrator's password. Default: local
<code>ldap-server <string></code>	Enter the LDAP server name if the user type is set to LDAP.
<code>radius_server <string></code>	Enter the RADIUS server name if the user type is set to RADIUS.
<code>tacacs-plus-server <string></code>	Enter the TACACS+ server name if the user type is set to TACACS+.
<code>ssh-public-key1 <key-type> <key-value></code>	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.
<code>ssh-public-key2 <key-type>, <key-value></code>	
<code>ssh-public-key3 <key-type> <key-value></code>	
<code>wildcard <enable disable></code>	Enable or disable wildcard remote authentication
<code>radius-accprofile-override <enable disable></code>	Allow access profile to be overridden from RADIUS.
<code>radius-adom-override <enable disable></code>	Allow ADOM to be overridden from RADIUS
<code>radius-group-match <string></code>	Only admin that belong to this group are allowed to login.
<code>last-name <string></code>	Administrators last name.
<code>first-name <string></code>	Administrators first name.
<code>email-address <string></code>	Administrators email address.
<code>phone-number <string></code>	Administrators phone number.
<code>mobile-number <string></code>	Administrators mobile phone number.
<code>pager-number <string></code>	Administrators pager number.
Variable for <code>config meta-data</code> subcommand: Note: This subcommand can only change the value of an existing field. To create a new metadata field, use the <code>config metadata</code> command.	

Variable	Description
fieldname	The label/name of the field. Read-only. Default: 50
fieldlength	The maximum number of characters allowed for this field. Read-only.
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.
importance	Indicates whether the field is compulsory (<code>required</code>) or optional (<code>optional</code>). Read-only. Default: optional
status	For display only. Value cannot be changed. Default: enable
Variable for <code>config dashboard-tabs</code> subcommand:	
tabid <integer>	Tab ID.
name <string>	Tab name.
Variable for <code>config dashboard</code> subcommand:	
moduleid	Widget ID.
name <string>	Widget name.
column <column_pos>	Widget's column ID. Default: 0
refresh-interval <integer>	Widget's refresh interval. Default: 300
status {close open}	Widget's opened/closed status. Default: open
tabid <integer>	ID of the tab where the widget is displayed. Default: 0
widget-type <string>	Widget type.
num-entries <integer>	Number of entries. Default: 10
log-rate-type {device log}	Log receive monitor widget's statistics breakdown options. Default: log
log-rate-topn <integer>	Log receive monitor widget's number of top items to display. Default: 5

Variable	Description
<code>log-rate-period {1hour 3min 6hours}</code>	Log receive monitor widget's data period. Default: 2 min
<code>res-view-type {history real-time}</code>	Widget's data view type. Default: history
<code>res-period {10min day hour}</code>	Widget's data period. Default: 10 min
Variable for <code>config restrict-dev-vdom</code> subcommand:	
<code>dev-vdom <string></code>	Enter device or VDOM to edit.

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 IP address if you define only one trusted host IP address with a network mask 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 Web-based Manager 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 IP address.

```
config fmsystem 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 Web-based Manager.

Syntax

```
config fmsystem alert-console
  set period <integer>
  set severity-level {information | notify | warning | error |
    critical | alert | emergency}
end
```

Variable	Description
period <integer>	Enter the number of days to keep the alert console information on the dashboard in days between 1 and 7. Default: 7
severity-level {information notify warning error critical alert emergency}	Enter the severity level to display on the alert console on the dashboard.

Example

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

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

Related topics

- `alertemail`

alert-event

Use `alert-event` commands to configure the FortiManager unit to monitor logs for log messages with certain severity levels, or information within the logs. If the message appears in the logs, the FortiManager unit sends an email or SNMP trap to a predefined recipient(s) of the log message encountered. Alert event messages provide immediate notification of issues occurring on the FortiManager unit.

When configuring an alert email, you must configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server and must look up this name on your DNS server. name

Syntax

```
config fmsystem alert-event
edit <name_string>
config alert-destination
edit destination_id <integer>
set type {mail | snmp | syslog}
set from <email_addr>
set to <email_addr>
set smtp-name <server_name>
set snmp-name <server_name>
set syslog-name <server_name>
end
set enable-generic-text {enable | disable}
set enable-severity-filter {enable | disable}
set event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}
set generic-text <string>
set num-events {1 | 5 | 10 | 50 | 100}
set severity-filter {high | low | medium | medium-high |
medium-low}
set severity-level-comp {>= | = | <=}
set severity-level-logs {no-check | information | notify |
warning | error | critical | alert | emergency}
end
```

Variable	Description
<name_string>	Enter a name for the alert event.
destination_id <integer>	Enter the table sequence number, beginning at 1.
type {mail snmp syslog}	Select the alert event message method of delivery. Default: mail
from <email_addr>	Enter the email address of the sender of the message. This is available when the type is set to mail.
to <email_addr>	Enter the recipient of the alert message. This is available when the type is set to mail.
smtp-name <server_name>	Enter the name of the mail server. This is available when the type is set to mail.
snmp-name <server_name>	Enter the snmp server name. This is available when the type is set to snmp.
syslog-name <server_name>	Enter the syslog server name or IP address. This is available when the type is set to syslog.
enable-generic-text {enable disable}	Enable the text alert option. Default: disable
enable-severity-filter {enable disable}	Enable the severity filter option. Default: disable

Variable	Description
event-time-period {0.5 1 3 6 12 24 72 168}	The period of time in hours during which if the threshold number is exceeded, the event will be reported.
generic-text <string>	Enter the text the alert looks for in the log messages.
num-events {1 5 10 50 100}	Set the number of events that must occur in the given interval before it is reported.
severity-filter {high low medium medium-high medium-low}	Set the alert severity indicator for the alert message the FortiManager unit sends to the recipient.
severity-level-comp {>= = <=}	Set the severity level in relation to the log level. Log messages are monitored based on the log level. For example, alerts may be monitored if the messages are greater than, and equal to (>=) the Warning log level.
severity-level-logs {no-check information notify warning error critical alert emergency}	Set the log level the FortiManager looks for when monitoring for alert messages.

Example

In the following example, the alert message is set to send an email to the administrator when 5 warning log messages appear over the span of three hours.

```
config fmsystem alert-event
  edit warning
    config alert-destination
      edit 1
        set type mail
        set from fmgr@example.com
        set to admin@example.com
        set smtp-name mail.example.com
      end
      set enable-severity-filter enable
      set event-time-period 3
      set severity-level-log warning
      set severity-level-comp =
      set severity-filter medium
    end
  end
```

Related topics

- [alert-console](#)
- [alertemail](#)

alertemail

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

All variables are required if authentication is enabled.

Syntax

```
config fmsystem alertemail
    set authentication {enable | disable}
    set fromaddress <email-addr_str>
    set fromname <name_str>
    set smtppassword <pass_str>
    set smtpport <port_int>
    set smtpserver {<ipv4>|<fqdn_str>}
    set smtpuser <username_str>
end
```

Variable	Description
authentication {enable disable}	Enable or disable alert email authentication. Default: enable
fromaddress <email-addr_str>	The email address the alertmessage is from. This is a required variable.
fromname <name_str>	The SMTP name associated with the email address. To enter a name that includes spaces, enclose the whole name in quotes.
smtppassword <pass_str>	Set the SMTP server password.
smtpport <port_int>	The SMTP server port. Default: 25
smtpserver {<ipv4> <fqdn_str>}	The SMTP server address. Enter either a DNS resolvable host name or an IP address.
smtpuser <username_str>	Set the SMTP server username.

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 IP address of 192.168.10.10.

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

backup all-settings

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

Syntax

```
config fmsystem backup all-settings
  set status {enable | disable}
  set server {<ipv4>|<fqdn_str>}
  set user <username_str>
  set passwd <pass_str>
  set directory <dir_str>
  set week_days {monday tuesday wednesday thursday friday saturday
    sunday}
  set time <hh:mm:ss>
  set protocol {ftp | sftp}
  set crptpasswd <pass_str>
end
```

Variable	Description
status {enable disable}	Enable or disable scheduled backups. Default: disable
server {<ipv4> <fqdn_str>}	Enter the IP address or DNS resolvable host name of the backup server.
user <username_str>	Enter the user account name for the backup server.
passwd <pass_str>	Enter the password for the backup server.
directory <dir_str>	Enter the name of the directory on the backup server in which to save the backup file.
week_days {monday tuesday wednesday thursday friday saturday sunday}	Enter days of the week on which to perform backups. You may enter multiple days.
time <hh:mm:ss>	Enter time of day to perform the backup. Time is required in the form <hh:mm:ss>.
protocol {ftp sftp}	Enter the transfer protocol. Default: sftp
crptpasswd <pass_str>	Optional password to protect backup content

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 fmsystem 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 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 `fmsystem certificate local` command to install the signed local certificate.
4. Use the `fmsystem 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 fmsystem certificate ca
  edit <ca_name>
    set ca <cert>
    set comment <string>
  end
```

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

```
get fmsystem certificate ca <ca_name>
```

Variable	Description
<code>edit <ca_name></code>	Enter a name for the CA certificate.
<code>ca <cert></code>	Enter or retrieve the CA certificate in PEM format.
<code>comment <string></code>	Optionally, enter a descriptive comment.

certificate local

Use this command to install local 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 `fmsystem certificate local` command to install the signed local certificate.
- 4. Use the `fmsystem 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 fmsystem certificate local
  edit <cert_name>
    set password <cert_password>
    set comment <comment_text>
    set private-key <prkey>
    set certificate <cert_PEM>
    set csr <csr_PEM>
  end
```

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

```
get fmsystem certificate local [cert_name]
```

Variable	Description
<code>edit <cert_name></code>	Enter the local certificate name.
<code>password <cert_password></code>	Enter the local certificate password.
<code>comment <comment_text></code>	Enter any relevant information about the certificate.
<code>certificate <cert_PEM></code>	Enter the signed local certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
<code>private-key <prkey></code>	The private key in PEM format.
<code>csr <csr_PEM></code>	The CSR in PEM format.

Use this command to configure Deployment Manager settings.

Syntax

```
config fmsystem dm
    set concurrent-install-limit <installs_int>
    set concurrent-install-script-limit <scripts_int>
    set discover-timeout <integer>
    set dpm-logsize <kbytes_int>
    set fgfm-sock-timeout <sec_int>
    set fgfm_keepalive_itvl <sec_int>
    set force-remote-diff {enable | disable}
    set max-revs <revs_int>
    set nr-retry <retries_int>
    set retry {enable | disable}
    set retry-intvl <sec_int>
    set rollback-allow-reboot {enable | disable}
    set script-logsize <integer>
    set verify-install {enable | disable}
end
```

Variable	Description
concurrent-install-limit <installs_int>	The maximum number of concurrent installs. The range can be from 5 to 100. Default: 60
concurrent-install-script-limit <scripts_int>	The maximum number of concurrent install scripts. The range can be from 5 to 100. Default: 60
discover-timeout <integer>	Check connection timeout when discovering a device. The range can be from 3 to 15. Default: 6
dpm-logsize <kbytes_int>	The maximum DPM log size per device in kB. The range can be from 1 to 10000K. Default: 10000
fgfm-sock-timeout <sec_int>	The maximum FortiManager/FortiGate communication socket idle time. The interval can be from 90 to 1800 seconds. Default: 360
fgfm_keepalive_itvl <sec_int>	The interval at which the FortiManager will send a keepalive signal to a FortiGate unit to keep the FortiManager/FortiGate communication protocol active. The interval can be from 30 to 600 seconds. Default: 120

Variable	Description
<code>force-remote-diff</code> <code>{enable disable}</code>	Enable to always use remote diff when installing. Default: disable
<code>max-revs <revs_int></code>	The maximum number of revisions saved. Valid numbers are from 1 to 250. Default: 100
<code>nr-retry <retries_int></code>	The number of times the FortiManager unit will retry. Default: 1
<code>retry {enable disable}</code>	Enable or disable configuration installation retries. Default: enable
<code>retry-intvl <sec_int></code>	The interval between attempting another configuration installation following a failed attempt. Default: 15
<code>rollback-allow-reboot</code> <code>{enable disable}</code>	Enable to allow a FortiGate unit to reboot when installing a script or configuration. Default: disable
<code>script-logsize <integer></code>	Enter the maximum script log size per device (1-10000Kb). Default: 100
<code>verify-install {enable disable}</code>	Enable to verify install against remote configuration. Default: enable

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 fmsystem dm
  set retry enable
  set nr-retry 5
  set retry-intvl 30
end
```

dns

Use this command to set the DNS server addresses. Several FortiManager functions, including sending alert email, use DNS.

Syntax

```
config fmsystem dns
    set primary <ipv4>
    set secondary <ipv4>
end
```

Variable	Description
primary <ipv4>	Enter the primary DNS server IP address. Default: 65.39.139.53
secondary <ipv4>	Enter the secondary DNS IP server address. Default: 65.39.139.63

Example

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

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

fips

Use this command to set the FIPS status.

Syntax

```
config fmsystem fips
    set
end
```

global

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

Syntax

```
config fmsystem global
    set admin-lockout-duration <integer>
    set admin-lockout-threshold <integer>
    set admintimeout <integer>
    set adom-mode {advanced | normal}
    set adom-status {enable | disable}
    set backup-compression
    set backup-managed
    set console-output {more | standard}
    set daylightsavetime {enable | disable}
    set dh-params
    set enc-algorithm {default | high | low}
    set hostname <string>
    set language {english | japanese | simch | trach}
    set lcdpin <pin_int>
    set ldapconntimeout <integer>
    set max-concurrent-users <integer>
    set remoteauthtimeout <integer>
    set ssl-low-encryption {enable | disable}
    set swapmem {enable | disable}
    set timezone <timezone_int>
    set webservice-support-ssl3 {enable | disable}
    set workspace {enable | disable}
end
```

Variable	Description
admin-lockout-duration <integer>	Set the lockout duration (seconds) for FortiManager administration. Default: 60
admin-lockout-threshold <integer>	Set the lockout threshold for FortiManager administration (1 to 10). Default: 3
admintimeout <integer>	Set the administrator idle timeout (in minutes). Default: 5
adom-mode {advanced normal}	Set the ADOM mode.
adom-status {enable disable}	Enable or disable administrative domains (ADOMs). Default: disable

Variable	Description
<code>backup-compression</code>	Set the backup compression speed. Default: normal
<code>backup-managed</code>	Enable or disable backup management. Default: disable
<code>console-output {more standard}</code>	Select how the output is displayed on the console. Select <code>more</code> to pause the output at each full screen until keypress. Select <code>standard</code> for continuous output without pauses. Default: standard
<code>daylightsavetime {enable disable}</code>	Enable or disable daylight saving time. If you enable daylight saving time, the FortiManager unit automatically adjusts the system time when daylight saving time begins or ends. Default: enable
<code>dh-params</code>	DH parameters.
<code>enc-algorithm {default high low}</code>	Set SSL communication encryption algorithms. Default: default
<code>hostname <string></code>	FortiManager host name.
<code>language {english japanese simch trach}</code>	Web interface language. Select from English, Japanese, Simplified Chinese, or Traditional Chinese. Default: English
<code>lcdpin <pin_int></code>	Set the 6 digit PIN administrators must enter to use the LCD panel.
<code>ldapconntimeout <integer></code>	LDAP connection timeout (in milliseconds). Default: 60000
<code>max-concurrent-users <integer></code>	Maximum number of concurrent administrators. Default: 20
<code>remoteauthtimeout <integer></code>	Remote authentication (RADIUS/LDAP) timeout (in seconds). Default: 10
<code>ssl-low-encryption {enable disable}</code>	Enable or disable low-grade (40-bit) encryption. Default: enable
<code>swapmem {enable disable}</code>	Enable or disable virtual memory. Default: enable
<code>timezone <timezone_int></code>	The time zone for the FortiManager unit. Default: (GMT-8)Pacific Time (US & Canada)

Variable	Description
<code>webservice-support-ssl3 {enable disable}</code>	Enable or disable SSLv3 protocol support for web service TLS/SSL connections.
<code>workspace {enable disable}</code>	Enable or disable Workspace (ADOM locking).

Example

The following command turns on daylight saving time, sets the FortiManager unit name to FMG3k, sets the LCD password to 123856, and chooses the Eastern time zone for US & Canada.

```
config fmsystem global
    set daylightsavetime enable
    set hostname FMG3k
    set lcdpin 123856
    set timezone 12
end
```

ha

Use the `config fmsystem 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 six FortiManager units of the same FortiManager model. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to five 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).

Administrators connect to the primary unit Web-Based Manager or CLI to perform FortiManager operations. The primary unit also interacts with managed FortiGate devices, FortiMail devices, FortiClient applications, 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 IP 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.

To configure a cluster, use the `config fmsystem ha` command to set the HA operation mode (mode) to `ha` and set the local IP1 (`local-ip1`), peer IP1 (`peer-ip1`) and the first synchronization interface (also called synchronization port) (`synchport1`) of both FortiManager units in the cluster. The local IP1 IP address of both FortiManager units must match the peer IP1 IP address of the other FortiManager unit. Both units should also have the same first synchronization interface.

Syntax

```
config fmsystem ha
    set clusterid <clusert_ID_int>
    set hb-interval <time_interval_int>
    set hb-lost-threshold <lost_heartbeats_int>
    set mode {master | slave | standalone}
    set password <password_str>
    config peer
        edit <peer_id_int>
            set ip <peer_ip_ipv4>
            set serial-number <peer_serial_str>
            set status <peer_status>
        end
    end
end
```

Variable	Description
clusterid <clusert_ID_int>	A number between 0 and 64 that identifies the HA cluster. All members of the HA cluster must have the same <code>clusterid</code> . If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different group ID.
hb-interval <time_interval_int>	<p>The time in seconds that a cluster unit waits between sending heartbeat packets. 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. The default heartbeat interval is 5 seconds.</p> <p>The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds.</p>
hb-lost-threshold <lost_heartbeats_int>	<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. The default failover threshold is 3. The failover threshold range is 1 to 255.</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>

Variable	Description
mode {master slave standalone}	Select master to configure the FortiManager unit to be the primary unit in a cluster. Select slave to configure the FortiManager unit to be a backup unit in a cluster. Select standalone to stop operating in HA mode.
password <password_str>	A group password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.
config peer	Add peers to the HA configuration of the FortiManager unit. You add all of the backup units as peers to the primary unit (up to 5). For each backup unit you add the primary unit.
edit <peer_id_int>	Add a peer and add the peer's IP address and serial number.
ip <peer_ip_ipv4>	Enter the IP address of the peer FortiManager unit.
serial-number <peer_serial_str>	Enter the serial number of the peer FortiManager unit.
status <peer_status>	Enter the status of the peer FortiManager unit.

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 fmsystem ha
    set mode master
    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 fmsystem ha
  set mode slave
  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.

interface

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

Syntax

```
config fmsystem interface
  edit <port_str>
    set status {up | down}
    set ip <ipv4_mask>
    set allowaccess {http https ping snmp ssh telnet webservice}
    set serviceaccess {fclupdates fgtupdates}
    set speed {1000full 100full 100half 10full 10half auto}
    set description <string>
    set alias <string>
  end
```

Variable	Description
<port_str>	<port_str> can be set to a port number such as port1, port2, port3, or port4. Different FortiManager models have different numbers of ports.
status {up down}	Start or stop the interface. If the interface is stopped it does not accept or send packets. If you stop a physical interface, VLAN interfaces associated with it also stop. Default: up
ip <ipv4_mask>	Enter the interface IP address and network mask. The IP address cannot be on the same subnet as any other interface.

Variable	Description
<code>allowaccess {http https ping snmp ssh telnet webservice}</code>	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.
<code>serviceaccess {fclupdates fgtupdates}</code>	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.
<code>speed {1000full 100full 100half 10full 10half auto}</code>	Enter the speed and duplexing the network port uses. Enter <code>auto</code> to automatically negotiate the fastest common speed. Default: <code>auto</code>
<code>description <string></code>	Enter a description of the interface.
<code>alias <string></code>	Enter an alias for the interface.

Example

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

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

locallog disk setting

Use this command to configure the FortiAnalyzer 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 fmsystem locallog disk setting
  set status {enable | disable}
  set severity {alert | critical | debug | emergency | error |
    information | notification | warning}
  set max-log-file-size <size_int>
  set roll-schedule {none | daily | weekly}
  set roll-day <string>
  set roll-time <hh:mm>
  set diskfull {nolog | overwrite}
```

```

set log-disk-full-percentage
set upload {disable | enable}
set uploadip <ipv4>
set server-type {faz | ftp | scp | sftp}
set uploadport <port_int>
set uploaduser <user_str>
set uploadpass <passwd_str>
set uploadaddr <dir_str>
set uploadtype <event>
set uploadzip {disable | enable}
set uploadsched {disable | enable}
set upload-time <hh:mm>
set upload-delete-files {disable | enable}
end

```

Variable	Description																
status {enable disable}	Enter enable to begin logging. Default: disable																
severity {alert critical debug emergency error information notification warning}	Select the logging severity level. The FortiManager unit logs all messages at and above the logging severity level you select. For example, if you select <code>critical</code> , the unit logs <code>critical</code> , <code>alert</code> and <code>emergency</code> level messages. Default: alert The logging levels in descending order are: <table> <tr> <td>emergency</td><td>The unit is unusable.</td></tr> <tr> <td>alert</td><td>Immediate action is required.</td></tr> <tr> <td>critical</td><td>Functionality is affected.</td></tr> <tr> <td>error</td><td>Functionality is probably affected.</td></tr> <tr> <td>warning</td><td>Functionality might be affected.</td></tr> <tr> <td>notification</td><td>Information about normal events.</td></tr> <tr> <td>information</td><td>General information about unit operations.</td></tr> <tr> <td>debug</td><td>Information used for diagnosis or debugging.</td></tr> </table>	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.	debug	Information used for diagnosis or debugging.
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.																
debug	Information used for diagnosis or debugging.																
max-log-file-size <size_int>	Enter the size at which the log is rolled. The range is from 1 to 1024 megabytes. Default: 100																
roll-schedule {none daily weekly}	Enter the period for the scheduled rolling of a log file. If <code>roll-schedule</code> is <code>none</code> , the log rolls when <code>max-log-file-size</code> is reached. Default: none																
roll-day <string>	Enter the day for the scheduled rolling of a log file.																

Variable	Description
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: overwrite
log-disk-full-percentage	Enter the percentage at which the log disk will be considered full.
upload {disable enable}	Enable to permit uploading of logs. Default: disable
uploadip <ipv4>	Enter IP address of the destination server. Default: 0.0.0.0
server-type {fz ftp scp sftp}	Enter the type the server to use to store the logs.
uploadport <port_int>	Enter the port to use when communicating with the destination server. Default: 21
uploaduser <user_str>	Enter the user account on the destination server.
uploadpass <passwd_str>	Enter the password of the user account on the destination server.
uploadaddr <dir_str>	Enter the destination directory on the remote server.
uploadtype <event>	Enter to upload the event log files. Default: event
uploadzip {disable enable}	Enable to compress uploaded log files. Default: disable
uploadsched {disable enable}	Enable to schedule log uploads.
upload-time <hh:mm>	Enter to configure when to schedule an upload.
upload-delete-files {disable enable}	Enable to delete 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 fmsystem 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 fmsystem locallog [memory| disk | fortianalyzer | syslogd |
  syslogd2 | syslogd3] filter
  set devcfg {disable | enable}
  set dm {disable | enable}
  set dvm {disable | enable}
  set epmgr {disable | enable}
  set event {disable | enable}
  set fctmgr {disable | enable}
  set fgd {disable | enable}
  set fgfm {disable | enable}
  set fmlmgr {disable | enable}
  set fmwmgr {disable | enable}
  set glbcfg {disable | enable}
  set ha {disable | enable}
  set iolog {disable | enable}
  set lrmgr {disable | enable}
  set objcft {disable | enable}
  set rev {disable | enable}
  set rtmon {disable | enable}
  set scfw {disable | enable}
  set scply {disable | enable}
```

```

set scrmgr {disable | enable}
set scvpn {disable | enable}
set system {disable | enable}
set webport {disable | enable}
end

```

Variable	Description
devcfg {disable enable}	Enable to log device configuration messages. Default: disable
dm {disable enable}	Enable to log deployment manager messages. Default: disable
dvm {disable enable}	Default: disable
epmgr {disable enable}	Enable to log endpoint manager messages. Default: disable
event {disable enable}	Enable to configure log filter messages. Default: disable
fctmgr {disable enable}	Enable to log FortiClient manager messages. Default: disable
fgd {disable enable}	Enable to log FortiGuard service messages. Default: disable
fgfm {disable enable}	Enable to log FortiGate/FortiManager communication protocol messages. Default: disable
fmlmgr {disable enable}	Enable to log FortiMail manager messages. Default: disable
fmwmgr {disable enable}	Enable to log firmware manager messages. Default: disable
glbcfg {disable enable}	Enable to log global database messages. Default: disable
ha {disable enable}	Enable to log high availability activity messages. Default: disable
iolog {disable enable}	Enable input/output log activity messages. Default: disable
lrmgr {disable enable}	Enable to log and report manager messages. Default: disable

Variable	Description
<code>objcft {disable enable}</code>	Enable to log object configuration. Default: disable
<code>rev {disable enable}</code>	Enable to log revision history messages. Default: disable
<code>rtmon {disable enable}</code>	Enable to log real-time monitor messages. Default: disable
<code>scfw {disable enable}</code>	Enable to log firewall objects messages. Default: disable
<code>scply {disable enable}</code>	Enable to log policy console messages. Default: disable
<code>scrmgr {disable enable}</code>	Enable to log script manager messages. Default: disable
<code>scvpn {disable enable}</code>	Enable to log VPN console messages. Default: disable
<code>system {disable enable}</code>	Enable to log system manager messages. Default: disable
<code>webport {disable enable}</code>	Enable to log web portal messages. Default: disable

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

locallog fortianalyzer setting

Use this command to enable or disable, and select the severity threshold of, remote logging to the FortiAnalyzer unit entered in `fmsystem log fortianalyzer`. Refer to `fmsystemlocallog filter` on page 73.

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 fmsystem locallog fortianalyzer setting
    set severity {emergency | alert | critical | error | warning |
        notification | information | debug}
    set status {disable | enable}
end
```

Variable	Description
<code>severity {emergency alert critical error warning notification information debug}</code>	Enter the severity threshold that a log message must meet or exceed to be logged to the FortiAnalyzer unit. For details on severity levels, see “severity {alert critical debug emergency error information notification warning}” on page 71. Default: alert
<code>status {disable enable}</code>	Enable or disable remote logging to the FortiAnalyzer unit. Default: disable

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 fmsystem locallog fortianalyzer setting
    set status enable
    set severity information
end
```

locallog memory setting

Use this command to configure memory settings for local logging purposes. Refer to `fmsystemlocallog filter` on page 73.

Syntax

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

end

Variable	Description
<code>diskfull {nolog overwrite}</code>	Enter action to take when the disk is full: <ul style="list-style-type: none">• <code>nolog</code> — stop logging• <code>overwrite</code> — overwrites oldest log entries Default: <code>overwrite</code>
<code>severity {emergency alert critical error warning notification information debug}</code>	Enter to configure the severity level to log files. See “ <code>severity {alert critical debug emergency error information notification warning}</code> ” on page 71 for more information on the severity levels. Default: <code>alert</code>
<code>status <disable enable></code>	Enable or disable the memory buffer log. Default: <code>disable</code>

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 fmsystem 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 syslogd servers, `syslogd`, `syslogd2` and `syslogd3`.

Syntax

```
config fmsystem locallog {syslogd | syslogd2 | syslogd3} setting
    set csv {disable | enable}
    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 port <port_int>
    set server <address_ipv4>
    set severity {emergency | alert | critical | error | warning |
        notification | information | debug}
    set status {enable | disable}
```

end

Variable	Description
<code>csv {disable enable}</code>	<p>Enable to produce the log in comma separated value (CSV) format. If you do not enable CSV format the FortiManager unit produces space separated log files.</p> <p>Default: disable</p>
<code>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}</code>	<p>Enter the facility type. <code>facility</code> identifies the source of the log message to syslog. Change <code>facility</code> to distinguish log messages from different FortiManager units so you can determine the source of the log messages. Available facility types are:</p> <ul style="list-style-type: none">• <code>alert</code> — log alert• <code>audit</code> — log audit• <code>auth</code> — security/authorization messages• <code>authpriv</code> — security/authorization messages (private)• <code>clock</code> — clock daemon• <code>cron</code> — cron daemon performing scheduled commands• <code>daemon</code> — system daemons running background system processes• <code>ftp</code> — File Transfer Protocol (FTP) daemon• <code>kernel</code> — kernel messages• <code>local0</code> – <code>local7</code> — reserved for local use• <code>lpr</code> — line printer subsystem• <code>mail</code> — email system• <code>news</code> — network news subsystem• <code>ntp</code> — Network Time Protocol (NTP) daemon• <code>syslog</code> — messages generated internally by the syslog daemon <p>Default: local 7</p>
<code>port <port_int></code>	<p>Enter the port number for communication with the syslog server.</p> <p>Default: 514</p>
<code>server <address_ipv4></code>	<p>Enter the IP address of the syslog server that stores the logs.</p>

Variable	Description	
severity {emergency alert critical error warning notification information debug}	Select the logging severity level. The FortiManager unit logs all messages at and above the logging severity level you select. For example, if you select <code>critical</code> , the unit logs <code>critical</code> , <code>alert</code> and <code>emergency</code> level messages. Default: <code>alert</code> The logging levels in descending order are:	
	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.
	debug	Information used for diagnosis or debugging.
status {enable disable}	Enter <code>enable</code> to begin logging. Default: <code>disable</code>	

Example

In this example, the logs are uploaded to a syslog server at IP address `10.10.10.8`. The FortiManager unit is identified as facility `local0`.

```

config fmsystem locallog syslogd setting
    set facility local0
    set server 10.10.10.8
    set status enable
    set severity information
end

```

log fortianalyzer

Use this command to configure a connection with the FortiAnalyzer unit which will be used as the FortiManager's remote log server. You must configure the FortiAnalyzer unit to accept web

service connections. Refer to [fmsystemlocallog filter](#) on page 73 for details of the filters.

Syntax

```
config fmsystem log fortianalyzer
  set status {disable | enable}
  set ip <ipv4>
  set secure_connection {disable | enable}
  set localid <string>
  set psk <passwd>
  set username <username_str>
  set passwd <pass_str>
  set auto_install {enable | disable}
end
```

Variable	Description
status {disable enable}	Enable or disable to configure the connection to the FortiAnalyzer unit. Default: disable
ip <ipv4>	Enter the IP address of the FortiAnalyzer unit.
secure_connection {disable enable}	Enable or disable secure connection with the FortiAnalyzer unit.
localid <string>	Enter the local ID.
psk <passwd>	Enter the preshared key with the FortiAnalyzer unit.
username <username_str>	Enter the FortiAnalyzer administrator login that the FortiManager unit will use to administer the FortiAnalyzer unit.
passwd <pass_str>	Enter the FortiAnalyzer administrator password for the account specified in username.
auto_install {enable disable}	Enable to automatically update the FortiAnalyzer settings as they are changed on the FortiManager unit. Default: disable

Example

You can configure a secure tunnel for logs and other communications with the FortiAnalyzer unit.

```
config fmsystem log fortianalyzer
  set status enable
  set ip 192.168.1.100
  set username admin
  set passwd wert5W34bNg
end
```

log setting

Use this command to configure settings for logs.

Syntax

```
config fmsystem log setting
  set compression <int>
  set level {emerg | alert | crit | error | warn | notice | info |
            debug}
  set rotatesize <int>
end
```

Variable	Description
compression <int>	Enter to select a compression level for log files in the range of 0-10. When at zero, the compression level is disabled. Default: 6
level {emerg alert crit error warn notice info debug}	Enter the required log level. Default: alert
rotatesize <int>	Enter a number (in bytes) to configure the rotate size of the log file. Default: 10 000 000

Example

This example configures log settings for an average level of compression in the log files, to log all events of warning level and higher and to rotate the logs when they reach a size of 500 000 bytes.

```
config fmsystem log settings
  set compression 6
  set level warn
  set rotatesize 500 000
  set toconsole enable
end
```

mail

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

Syntax

```
config fmsystem mail
  edit <server>
    set auth {enable | disable}
    set passwd <passwd>
    set user <string>
```

end

Variable	Description
<server>	Enter the name of the mail server.
auth {enable disable}	Enable or disable authentication.
passwd <passwd>	Enter the SMTP account password value.
user <string>	Enter the SMTP account user name.

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 fmsystem admin user` to add data to the metadata fields.

Syntax

```
config fmsystem metadata admins
edit <name_str>
    set field_length {20 | 50 | 255}
    set importance {optional | required}
    set status {enable | disable}
end
```

Variable	Description
<name_str>	Enter the name of the new data field.
field_length {20 50 255}	Select the maximum number of characters allowed in this field: 20, 50, or 255. Default: 50
importance {optional required}	Select if this field is required or optional when entering standard information. Default: optional
status {enable disable}	Enable or disable the metadata. Default: disable

ntp

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

Syntax

```
config fmsystem ntp
  set status {enable | disable}
  set sync_interval <min_str>
  config ntpserver
    edit <id>
      set ntpv3 {disable | enable}
      set server {<ipv4> | <fqdn_str>}
      set authentication {disable | enable}
      set key <passwd>
      set key-id <integer>
    end
  end
end
```

Variable	Description
status {enable disable}	Enable or disable NTP time setting. Default: disable
sync_interval <min_str>	Enter time, in minutes, how often the FortiManager unit synchronizes its time with the NTP server. Default: 60
Variable for config ntpserver subcommand:	
ntpv3 {disable enable}	Enable or disable NTPV3. Default: disable
server {<ipv4> <fqdn_str>}	Enter the IP address or fully qualified domain name of the NTP server.
authentication {disable enable}	Enable or disable MD5 authentication. Default: disable
key <passwd>	The authentication key.
key-id <integer>	The key ID for authentication. Default: 0

password-policy

Use this command to configure access password policies.

Syntax

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

```

    set expire <integer>
end

```

Variable	Description
status {disable enable}	Enable or disable the password policy. Default: enable
minimum-length <integer>	Set the password's minimum length. Must contain between 8 and 256 characters. 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 {disable enable}	Enable or disable changing at least 4 characters for a new password. Default: disable
expire <integer>	Set the number of days after which admin users' password will expire; 0 means never. Default: 0

Related topics

- [admin profile](#)

route

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

Syntax

```

config fmsystem route
  edit <seq_int>
    set device <port_str>
    set dst <dst_ipv4mask>
    set gateway <gateway_ipv4>
  end
end

```

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_str>	Enter the port used for this route.
dst <dst_ipv4mask>	Enter the IP address and mask for the destination network.
gateway <gateway_ipv4>	Enter the default gateway IP address for this network.

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 IP address and interface that connects it to the FortiManager unit.

For more information on SNMP traps and variables see the [FortiManager Administration Guide](#), or the [Fortinet Knowledge Base](#) online.



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 FortiManager unit as well.

Syntax

```
config fmsystem snmp community
  edit <index_number>
    set events <events_list>
    set name <community_name>
    set query-v1-port <port_number>
    set query-v1-status {enable | disable}
    set query-v2c-port <port_number>
    set query-v2c-status {enable | disable}
    set status {enable | disable}
    set trap-v1-rport <port_number>
    set trap-v1-status {enable | disable}
    set trap-v2c-rport <port_number>
    set trap-v2c-status {enable | disable}
  config hosts
```

```

edit <host_number>
    set interface <if_name>
    set ip <address_ipv4>
end
end

```

Variable	Description
edit <index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.
events <events_list>	<p>Enable the events for which the FortiManager unit should send traps to the SNMP managers in this community.</p> <ul style="list-style-type: none"> 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 HA master. intf_ip_chg: An interface IP address has changed. mem_low: The available memory is low. sys_reboot: The FortiManager unit has rebooted. <p>Default: All events enabled</p>
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 SNMP v2c trap packets to the SNMP manager, and is also present in query packets from, the SNMP manager.</p>
query-v1-port <port_number>	<p>Enter the SNMP v1 query port number used when SNMP managers query the FortiManager unit.</p> <p>Default: 161</p>
query-v1-status {enable disable}	<p>Enable or disable SNMP v1 queries for this SNMP community.</p> <p>Default: enable</p>
query-v2c-port <port_number>	<p>Enter the SNMP v2c query port number used when SNMP managers query the FortiManager unit.</p> <p>SNMP v2c queries will include the name of the community.</p> <p>Default: 161</p>
query-v2c-status {enable disable}	<p>Enable or disable SNMP v2c queries for this SNMP community.</p> <p>Default: enable</p>
status {enable disable}	<p>Enable or disable this SNMP community.</p> <p>Default: enable</p>

Variable	Description
trap-v1-rport <port_number>	Enter the SNMP v1 remote port number used for sending traps to the SNMP managers. Default: 162
trap-v1-status {enable disable}	Enable or disable SNMP v1 traps for this SNMP community. Default: enable
trap-v2c-rport <port_number>	Enter the SNMP v2c remote port number used for sending traps to the SNMP managers. Default: 162
trap-v2c-status {enable disable}	Enable or disable SNMP v2c traps for this SNMP community. SNMP v2c traps sent out to SNMP managers include the community name. Default: enable
Hosts Variables	
edit <host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <if_name>	Enter the name of the FortiManager unit that connects to the SNMP manager.
ip <address_ipv4>	Enter the IP address of the SNMP manager. Default: 0.0.0.0

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 IP address is 192.168.20.34 and it connects to the FortiManager unit internal interface.

```

config fmsystem 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
  end
end

```

Related topics

- [snmp sysinfo](#)
- [snmp user](#)

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 [FortiManager Administration Guide](#), or the [Fortinet Knowledge Base](#) online.

Syntax

```
config fmsystem snmp sysinfo
    set contact-info <info_str>
    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>
end
```

Variable	Description
contact-info <info_str>	Add the contact information for the person responsible for this FortiManager unit. The contact information can be up to 35 characters long.
description <description>	Add a name or description of the FortiManager unit. The description can be up to 35 characters long.
engine-id <string>	Local SNMP engine ID string (maximum 24 characters).
location <location>	Describe the physical location of the FortiManager unit. The system location description can be up to 35 characters long.
status {enable disable}	Enable or disable the FortiManager SNMP agent. Default: disable
trap-high-cpu-threshold <percentage>	CPU usage when trap is set. Default: 80
trap-low-memory-threshold <percentage>	Memory usage when trap is set. 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

```

Related topics

- [snmp community](#)
- [snmp user](#)

snmp user

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

For more information on SNMP traps and variables, see the [FortiManager v4.0 Administration Guide](#), or the [Fortinet Knowledge Base](#) online.

Syntax

```

config fmsystem snmp user
    edit <name>
        set auth-proto < >
        set events <events_list>
        set auth-pwd < >
        set notify-hosts <ip>
        set priv-proto < >
        set priv-pwd < >
        set queries {enable | disable}
        set query-port <port_number>
        set security-level <level>
    end
end

```

Variable	Description
<name>	
auth-proto < >	Authentication protocol. Default: sha
auth-pwd < >	Password for the authentication protocol.

Variable	Description
events <events_list>	<p>Enable the events for which the FortiManager unit should send traps to the SNMP managers in this community.</p> <ul style="list-style-type: none"> 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 HA master. intf_ip_chg: An interface IP address has changed. mem_low: The available memory is low. sys_reboot: The FortiManager unit has rebooted. <p>Default: All events enabled</p>
notify-hosts <ip>	Hosts to send notifications (traps) to.
priv-protocol < >	<p>Privacy (encryption) protocol.</p> <p>Default: aes</p>
priv-pwd < >	Password for the privacy (encryption) protocol.
queries {enable disable}	<p>Enable or disable queries for this user.</p> <p>Default: enable</p>
query-port <port_number>	<p>SNMPv3 query port.</p> <p>Default: 161</p>
security-level <level>	<p>Security level for message authentication and encryption.</p> <ul style="list-style-type: none"> auth-no-priv: message with authentication but no privacy (encryption) auth-priv: message with authentication and privacy (encryption) no-auth-no-priv: message with no authentication and no privacy (encryption). <p>Default: no-auth-no-priv</p>

syslog

Use this command to configure Syslog servers.

Syntax

```
config fmsystem snmp user
edit <name>
set ip <string>
set port <integer>
end
```

end

Variable	Description
ip <string>	Syslog server IP address or hostname.
port <integer>	Syslog server port.

fmupdate

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

This chapter contains following sections:

analyzer virusreport	deployment	support-pre-fgt43
av-ips advanced-log	device-version	web-spam fct server-override
av-ips fct server-override	disk-quota	web-spam fgd-log
av-ips fgt server-override	fct-services	web-spam fgd-setting
av-ips push-override	multilayer	web-spam fgt server-override
av-ips push-override-to-client	publicnetwork	web-spam poll-frequency
av-ips update-schedule	server-access-priorities	web-spam web-proxy
av-ips web-proxy	server-override-status	
custom-url-list	service	

analyzer virusreport

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

Syntax

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

Variable	Description
status {enable disable}	Enable or disable sending virus detection notification to Fortinet. Default: enable

Example

This example enables virus detection notifications to Fortinet.

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

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 FortiGuard Distribution Network (FDN).

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 or disable logging of FortiGuard Antivirus and IPS service updates of FortiGate devices. Default: disable
log-server {enable disable}	Enable or disable logging of update packages received by the built-in FDS server. Default: disable

Example

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

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

av-ips fct server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard Antivirus updates for FortiClient from the FDN.

Syntax

```
config fmupdate av-ips fct server-override
    set status {enable | disable}
    config servlist
        edit <id>
            set ip <xxx.xxx.xxx.xxx>
            set port <port_int>
        end
    end
```

end

Variable	Description
status {enable disable}	Enable or disable the override. Default: disable
Variable for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <xxx.xxx.xxx.xxx>	Enter the IP address of the override server address. Default: 0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDN. Default: 443

Example

You could configure the FortiManager unit's built-in FDS to use a specific FDN server and a different port when retrieving FortiGuard Antivirus updates for FortiClient from the FDN.

```
config fmupdate av-ips fct server-override
  set status enable
  config servlist
    edit 1
      set ip 192.168.25.152
      set port 80
    end
  end
end
```

av-ips fgt server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard Antivirus and IPS updates for FortiGate units from the FDN.

Syntax

```
config fmupdate av-ips fgt server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <xxx.xxx.xxx.xxx>
      set port <port_int>
    end
  end
```

end

Variable	Description
status {enable disable}	Enable or disable the override. Default: disable
Variable for config servlist subcommand:	
<id>	Override server ID (1-10)
ip <xxx.xxx.xxx.xxx>	Enter the IP address of the override server address. Default: 0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDN. Default: 443

Example

You could configure the FortiManager unit's built-in FDS to use a specific FDN server and a different port when retrieving FortiGuard Antivirus and IPS updates for FortiGate units from the FDN.

```
config fmupdate av-ips fgt server-override
  set status enable
  config servlist
    edit 1
      set ip 172.27.152.144
      set port 8890
    end
  end
end
```

av-ips push-override

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDN 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 av-ips push-override
  set ip <recipientaddress_ipv4>
  set port <recipientport_int>
  set status {enable | disable}
```

end

Variable	Description
ip <recipientaddress_ipv4>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiManager unit. Default: 0.0.0.0
port <recipientport_int>	Enter the receiving port number on the NAT device. Default: 9443
status {enable disable}	Enable or 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 FDN, you could also notify the FDN 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 av-ips push-override
  set status enable
  set ip 172.16.124.135
  set port 9000
end
```

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

av-ips 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 FDN 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 av-ips push-override-to-client
  set status {enable | disable}
  config <announce-ip>
    edit <id>
      set ip <xxx.xxx.xxx.xxx>
      set port <recipientport_int>
    end
```

end

Variable	Description
status {enable disable}	Enable or disable the push updates. Default: disable
<announce-ip>	Config the IP information of the device.
<id>	Edit the announce IP ID.
ip <xxx.xxx.xxx.xxx>	Enter the announce IP address. Default: 0.0.0.0
port <recipientport_int>	Enter the announce IP port. Default: 9443

av-ips update-schedule

Use this command to configure the built-in FDS to retrieve FortiGuard Antivirus and IPS updates at a specified day and time.

Syntax

```
config fmupdate av-ips update-schedule
  set frequency {every | daily | weekly}
  set status {enable | disable}
  set time <hh:mm>
end
```

Variable	Description
frequency {every daily weekly}	Enter to configure the frequency of the updates. Default: every
status {enable disable}	Enable or disable regularly scheduled updates. Default: enable
time <hh:mm>	Enter to configure the time or interval when the update will begin. For example, if you want to schedule an update every day at 6:00 PM, enter 18:00. The time period format is the 24-hour clock: hh=0-23, mm=0-59. If the minute is 60, the updates will begin at a random minute within the hour. If the frequency is every, the time is interpreted as an hour and minute interval, rather than a time of day. Default: 01:60

Example

You could schedule the built-in FDS to request the latest FortiGuard Antivirus and IPS updates every five hours, at a random minute within the hour.

```
config fmupdate av-ips udpate-schedule
  set status enable
  set frequency every
  set time 05:60
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 ip <proxy_ipv4>
  set mode {proxy | tunnel}
  set password <passwd_str>
  set port <port_int>
  set status {enable | disable}
  set username <username_str>
end
```

Variable	Description
ip <proxy_ipv4>	Enter the IP address of the web proxy. Default: 0.0.0.0
mode {proxy tunnel}	Enter the web proxy mode.
password <passwd_str>	If the web proxy requires authentication, enter the password for the user name.
port <port_int>	Enter the port number of the web proxy. Default: 80
status {enable disable}	Enable or disable connections through the web proxy. Default: disable
username <username_str>	If the web proxy requires authentication, enter the user name.

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 ip 10.10.30.1
```

```

set port 8890
set username avipsupdater
set password cvhk3rf3u9jvsYU
end

```

custom-url-list

Use this command to configure the URL list.

Syntax

```

config fmupdate custom-url-list
set db_selection <both | custom-url | fortiguard-db>
end

```

Variable	Description
db_selection <both custom-url fortiguard-db>	<p>Manage the URL database.</p> <ul style="list-style-type: none"> both: support both custom-url and FortiGuard database custom-url: customer imported URL list fortiguard-db: Fortinet's FortiGuard database. <p>Default: 0.0.0.0</p>

deployment

Use this command to configure the deployment mode and set the delay time to deploy packages to devices.

Syntax

```

config fmupdate deployment
set delaytime <integer>
set mode {auto | delay | manual}
end

```

Variable	Description
delaytime <integer>	<p>Enter the delay time you want to use in the delay mode deployment.</p> <p>Default: 60</p>
mode {auto delay manual}	<p>Set the mode of deployment.</p> <ul style="list-style-type: none"> auto: the FMG is used as a relay device only. Packages will be deployed as soon as they are ready. delay: updates the device from the FMG after the time set in delaytime. manual: deploy the packages manually. <p>Default: auto</p>

Example

Following example shows the packages will be deployed after 5 minutes.

```
config fmupdate deployment
  set delaytime 5
  set mode delay
end
```

device-version

Use this command to configure the correct firmware version of the device or devices connected or will be connecting to the FortiManager unit. You should verify what firmware version is currently running on the device before using this command.

Syntax

```
config fmupdate device-version
  set faz <firmware_version>
  set fct <firmware_version>
  set fgt <firmware_version>
  set fml <firmware_version>
  set fsw <firmware_version>
end
```

Variable	Description
faz <firmware_version>	Enter the correct firmware version that is currently running for FortiAnalyzers.
fct <firmware_version>	Enter the correct firmware version that is currently running for FortiClients.
fgt <firmware_version>	Enter the correct firmware version that is currently running for FortiGate units.
fml <firmware_version>	Enter the correct firmware version that is currently running for the FortiMail units.
fsw <firmware_version>	Enter the correct firmware version that is currently running for the FortiSwitch units.

Example

In the following example, the FortiGate units, including FortiClient agents, are configured with the new firmware version 4.0.

```
config fmupdate device-version
  set fct 4.0
  set fgt 4.0
end
```

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
```

Use `value` to set the size of the Upgrade Manager disk quota in MB. The default size is 10 GB. 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 <port_int>
end
```

Variable	Description
<code>status {enable disable}</code>	Enable or disable built-in FDS service to FortiClient installations. Default: enable
<code>port <port_int></code>	Enter the port number on which the built-in FDS should provide updates to FortiClient installations. 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
```

multilayer

Syntax

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

Variable	Description
webspam-rating {disable enable}	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 {disable enable}	Enable or disable the public network. Default: enable

Example

The following example shows how to enable public network.

```
config fmupdate publicnetwork
    (publicnetwork) # set status enable
end
```

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.



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 {disable | enable}
  set av-ips {disable | enable}
  set web-spam {disable | enable}
end
```

Variable	Description
access-public {disable enable}	Disable to prevent FortiManager default connectivity to public FDS and FortiGuard servers. Default: enable
av-ips {disable enable}	Enable to allow the FortiGate unit to get antivirus updates from other FortiManager units or private FDS servers. Default: disable
web-spam {disable enable}	Enable or disable private server in web-spam.

config private-server

Use this command to configure multiple FortiManager units and private servers.

Syntax

```
config fmupdate server-access-priorities
  config private-server
    edit <id>
      set ip <xxx.xxx.xxx.xxx>
      set time_zone <integer>
    end
  end
end
```

Variable	Description
<id>	Enter a number to identify the FortiManager unit or private server.
ip <xxx.xxx.xxx.xxx>	Enter the IP address of the FortiManager unit or private server.
time_zone <integer>	Enter the correct time zone of the private server. Using -24 indicates that the server is using the local time zone.

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

```

server-override-status

Syntax

```

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

```

Variable	Description
mode {loose strict}	<p>Set the server override mode.</p> <ul style="list-style-type: none"> • loose: allow access other servers • strict: access override server only). <p>Default: loose</p>

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 use-cert {BIOS | FortiGuard}
    set web-spam {disable | enable}
end

```

Variable	Description
avips {enable disable}	<p>Enable the built-in FDS to provide FortiGuard Antivirus and IPS updates.</p> <p>Default: disable</p>

Variable	Description
use-cert {BIOS FortiGuard}	Choose local certificate. <ul style="list-style-type: none"> BIOS: Use default certificate in BIOS. FortiGuard: Use default certificate as FortiGuard. Default: BIOS
web-spam {disable enable}	Enable or disable private server in web-spam.

Example

```
config fmupdate service
    set avips enable
end
```

support-pre-fgt43

Use this command to support FortiOS v4.0 MR2 and older devices for updates.

Syntax

```
config fmupdate support-pre-fgt43
    set status {enable | disable}
end
```

Variable	Description
status {enable disable}	Enable or disable support for FortiOS v4.0 MR2 and older devices for update.

web-spam fct server-override

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

Syntax

```
config fmupdate web-spam fct server-override
    set status {enable | disable}
    config servlist
        edit <id>
            set ip <xxx.xxx.xxx.xxx>
            set port <port_int>
        end
    end
```

end

Variable	Description
status {enable disable}	Enable or disable the override. Default: disable
Variable for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <xxx.xxx.xxx.xxx>	Enter the IP address of the override server address. Default: 0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDN. Default: 443

web-spam fgd-log

Use this command to configure the FortiGuard web-spam log settings.

Syntax

```
config fmupdate web-spam fgd-log
  set spamlog {all | disable | nospam}
  set status {disable | enable}
  set urllog {all | disable | miss}
end
```

Variable	Description
spamlog {all disable nospam}	Configure the anti spam log settings. <ul style="list-style-type: none">all: Log all Spam lookupsdisable: Disable Spam lognospam: Log Non-spam events.
status {disable enable}	Enable or disable the FGD server event log status.
urllog {all disable miss}	Configure the web filter log setting. <ul style="list-style-type: none">all: Log all URL lookupsdisable: Disable URL logmiss: Log URL rating misses.

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-preload {disable | enable}
  set av-cache <integer>
  set av-preload {disable | enable}
  set update-interval <integer>
  set wf-cache <integer>
  set wf-preload {disable | enable}
end
```

Variable	Description
as-cache <integer>	Set the antispam service maximum memory usage (100 to 4000MB).
as-preload {disable enable}	Enable or disable preloading the antispam database into memory.
av-cache <integer>	Set the web filter service maximum memory usage (100 to 500MB).
av-preload {disable enable}	Enable or disable preloading the antivirus database into memory.
update-interval <integer>	Set the FortiGuard database update wait time if there are not enough delta files (2 to 24 hours).
wf-cache <integer>	Set the web filter service maximum memory usage (100 to 4000MB).
wf-preload {disable enable}	Enable or disable preloading the web filter database into memory.

web-spam fgt server-override

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

Syntax

```
config fmupdate web-spam fgt server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <xxx.xxx.xxx.xxx>
      set port <port_int>
    end
  end
```

end

Variable	Description
status {enable disable}	Enable or disable the override. Default: disable
Variable for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <xxx.xxx.xxx.xxx>	Enter the IP address of the override server address. Default: 0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDN. Default: 443

web-spam poll-frequency

Use this command to configure the web-spam poll frequency.

Syntax

```
config fmupdate web-spam poll-frequency
  set time <hh:mm>
end
```

Variable	Description
time <hh:mm>	Enter the poll frequency time interval

web-spam web-proxy

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

Syntax

```
config fmupdate web-spam web-proxy
  set ip <proxy_ipv4>
  set mode {proxy | tunnel}
  set password <passwd>
  set port <integer>
  set status {disable | enable}
  set username <string>
```

end

Variable	Description
ip <proxy_ipv4>	Enter the IP address of the web proxy. Default: 0.0.0.0
mode {proxy tunnel}	Enter the web proxy mode.
password <passwd>	If the web proxy requires authentication, enter the password for the user name.
port <integer>	Enter the port number of the web proxy. Default: 80
status {disable enable}	Enable or disable connections through the web proxy. Default: disable
username <string>	If the web proxy requires authentication, enter the user name.

fmclient

Use `fmclient` commands to configure the FortiManager settings used to manage FortiClient software, licenses and web filtering for managed FortiClient agents.

This chapter contains following sections:

<code>ad_grouping_setting</code>	<code>discovery</code>	<code>license_key</code>
<code>ad_ou_grouping</code>	<code>emailalert</code>	<code>location_aware</code>
<code>client_license</code>	<code>enterprise_license</code>	<code>lockdown</code>
<code>cluster secondary</code>	<code>group_admin</code>	<code>systemsetting</code>
<code>cluster setting</code>	<code>ldap_users</code>	<code>webfilter_profile</code>
<code>communication_setting</code>	<code>ldapsetting</code>	

ad_grouping_setting

Syntax

```
config fmclient ad_grouping_setting interval <integer>
end
```

Variable	Description
<code>interval <integer></code>	The interval in which FCM synchronizes with the AD server (minutes). Default: 10

ad_ou_grouping

Syntax

```
config fmclient ad_ou_grouping
edit <name>
    set description <string>
    set ldapname <string>
    set rootou <string>
    set domain <string>
    set md5 <string>
end
```

Variable	Description
<code><name></code>	Enter a name for this OU grouping.
<code>description <string></code>	AD OU Grouping description.

Variable	Description
ldapname <string>	LDAP server name.
rootou <string>	Root OU. An LDAP server must be selected before the Root OU can be set.
domain <string>	Domain Name. This command is hidden.
md5 <string>	MD5. This command is hidden.

client_license

Use this command to create enterprise client licenses. You must first purchase an enterprise license and download it using the [enterprise_license](#) command.

Syntax

```
config fmclient client_license
edit <name>
    set description <string>
    set emailaddress <string>
    set expiry <date>
    set groupid <integer>
    set seats <integer>
    set status {enable | disable}
    set username <string>
end
```

Variable	Description
<name>	Enter a name for this client license.
description <string>	Optionally, enter a description.
emailaddress <string>	Enter the email address for the contact person.
expiry <date>	Set the license expiry date in the format yyyy-mm-dd hh:mm:ss. You can omit the time portion, which defaults to 00:00:00.
groupid <integer>	Enter the group id number. To find the number, enter this keyword followed by a ?.
seats <integer>	Set the maximum number of seats for this client license. The total seat count of all licenses can exceed the seat count of the enterprise license, but the number of managed clients cannot. Default: 0
status {enable disable}	Enable or disable this license. Default: disable
username <string>	Enter the user name for the license key.

cluster secondary

Use this command to add FortiManager units to your FortiClient Manager cluster as secondary units. For more information about FortiClient Manager clustering, see “[cluster setting](#)” on page 112.

After you enable the unit as a secondary cluster member, you need to restart the unit.

Syntax

```
config fmclient cluster secondary
edit <sec_fmgr_serno>
    set enable {enable | disable}
end
```

Variable	Description
<sec_fmgr_serno>	The serial number of the secondary FortiManager unit.
enable {enable disable}	Enable or disable this unit as a secondary cluster member. Default: disable

cluster setting

Use this command to enable FortiClient Manager clustering and to configure this FortiManager unit as a primary or secondary unit.

You can combine two or more FortiManager units into a FortiClient Manager cluster to manage a large number of FortiClient agents. One FortiManager unit is designated as the primary unit and all other units are secondary. The primary unit co-ordinates sharing of information amongst all units in the cluster. A managed FortiClient agent can log into any one of the units and receive its configuration information from that unit. Similarly, the administrator can log into any one of the units and modify the configuration of a FortiClient agent, even if that agent is connected to a different FortiManager unit.

Configure only one FortiManager unit in the cluster as the primary unit. On that primary unit, use the `cluster secondary` command to register each secondary unit.

Syntax

```
config fmclient cluster setting
set cluster_enable {enable | disable}
set cluster_role {primary | secondary}
end
```

Variable	Description
cluster_enable {enable disable}	Enable or disable clustering. Default: enable

Variable	Description
<code>cluster_role {primary secondary}</code>	Select whether this FortiManager unit is a primary or secondary FortiClient Manager. This is available only when <code>cluster_enable</code> is set to <code>enable</code> . Default: <code>primary</code>
<code>primary_ip <ip4></code>	Enter the IP address of the primary FortiManager unit. This is available only if <code>cluster_role</code> is <code>secondary</code> . Default: <code>0.0.0.0</code>

communication_setting

Use this command to configure settings for message communication between the FortiManager unit and FortiClient agents.

Syntax

```
config fmclient communication_setting
    set action_queue_interval <q1,q2,q3,q4>
    set action_queue_length <q1,q2,q3,q4>
    set disable_auto_vaccum {yes | no}
    set min_message_interval <seconds>
end
```

Variable	Description
<code>action_queue_interval <q1,q2,q3,q4></code>	Set sending interval in seconds of each message queue. <ul style="list-style-type: none"> q1 — Deploy/retrieve messages q2 — Lockdown/License key messages q3 — Patch update messages q4 — AV update messages Default: <code>60, 60, 120, 180</code>
<code>action_queue_length <q1,q2,q3,q4></code>	Set length of each message queue. <ul style="list-style-type: none"> q1 — Deploy/retrieve messages q2 — Lockdown/License key messages q3 — Patch update messages q4 — AV update messages Default: <code>300, 1500, 60, 60</code>

Variable	Description
<code>disable_auto_vaccum {yes no}</code>	By default, the FortiManager database performs periodic cleanup operations to maintain performance. You can disable this feature. Default: no
<code>min_message_interval <seconds></code>	Minimum interval, in seconds, allowed for two continuous messages. Default: 0

discovery

Use this command to enable or disable FortiClient discovery on FortiManager ports. You can also choose ports to accept unicast requests that FortiClient agents send to the FortiManager unit.

Syntax

```
config fmclient discovery
    set accept_ports {port1 port2...portn}
    set newclient_action {add-to-temp | auto-pop}
end
```

Variable	Description
<code>accept_ports {port1 port2...portn}</code>	Enter FortiManager ports that will accept requests for management from FortiClient agents. Separate port names with spaces.
<code>newclient_action {add-to-temp auto-pop}</code>	Select <code>add-to-temp</code> to add new discovered FortiClient agents to temporary clients list, and <code>auto-pop</code> to display the discovered FortiClient agents in the managed clients list. Default: auto-pop

emailalert

Use this command to configure the sending of email alerts for FortiClient Manager management alerts and events.

Syntax

```
config fmclient emailalert
    set admin_email <email_addr>
    set enable_email_alert {enable | disable}
    set fromaddr <from_addr>
    set password <string>
    set port <port_num>
    set secure_connection {None | TLS}
    set send_alert {enable | disable}
    set send_customer {enable | disable}
```

```

set send_event {enable | disable}
set smtpserver <mail_server>
set use_auth {enable | disable}
set username <string>
end

```

Variable	Description
admin_email <email_addr>	Enter the email address of the person who will receive alerts.
enable_email_alert {enable disable}	Enable sending of alert email. Default: disable
fromaddr <from_addr>	Enter the from address to provide in alert email messages.
password <string>	If use_auth is enable, enter the sender email account password.
port <port_num>	Enter the port number that the mail server uses. Default: 25
secure_connection {None TLS}	Select secure TLS connection or non-secured connection. Default: None
send_alert {enable disable}	Enable sending management alerts.
send_customer {enable disable}	Enable sending management customers.
send_event {enable disable}	Enable sending management events. Default: disable
smtpserver <mail_server>	Enter the SMTP mail server IP address or fully qualified domain name.
use_auth {enable disable}	Set to enable if the mail server requires authentication. Default: disable
username <string>	If use_auth is enable, enter the sender email account user name.

enterprise_license

Use this command to configure the validation type for enterprise licensing.

Syntax

```

config fmclient enterprise_license
set accept_blank {disable | enable}
set auto_add2managed {disable | enable}
set companion_key <string>
set deploy_key <string>
set disp_flag <integer>
set expiry <string>

```

```

set external_url <url>
set license_key <string>
set model {redistribute | standard | volume}
set seats <integer>
set validation_type {internal | external}
end

```

Variable	Description
accept_blank {disable enable}	Accept a blank license.
auto_add2managed {disable enable}	Add the free FortiClient to managed automatically.
companion_key <string>	This is a hidden command.
deploy_key <string>	This is a hidden command.
disp_flag <integer>	This is a hidden command.
expiry <string>	This is a hidden command.
external_url <url>	If validation_type is external, enter the validation facility URL.
license_key <string>	This is a hidden command.
model {redistribute standard volume}	Set the type of license model.
seats <integer>	This is a hidden command.
validation_type {internal external}	Set validation type for client license key: <ul style="list-style-type: none"> internal: Validate on FortiManager unit. external: Validate through external facility. Default: internal

group_admin

Use this command to configure FortiClient group administrators.

Syntax

```

config fmclient group_admin
edit <name>
    set group group1[,group2][,groupn]
    set option {none | access_ungroup}
end

```

Variable	Description
<name>	Enter the name of the administrator. The administrator must not have the Super_User administrative profile.

group group1[,group2][,groupn]	Enter the names of one or more client groups. Separate group names with commas.
option {none access_ungroup}	Set option to access_ungroup to enable this group administrator to configure ungrouped clients. Otherwise, set option to none. Default: none

ldap_users

Use this command to associate users in the LDAP database with web filter profiles.

Before using this command, you must first configure access to the LDAP server in the `ldapsetting` command and then run the `fmclient sync-ldap` command to retrieve user and group information.

Syntax

```
config fmclient ldap_users
edit <dn>
    set domain
    set ldap-server
    set name
    set type
    set webfilter-profile <profile_name>
end
```

Variable	Description
edit <dn>	Enter the distinguished name (DN) for this LDAP user.
domain	Domain Name.
ldap-server	Enter the LDAP server name if the user type is set to LDAP.
name	Enter the CN name.
type	Enter the user type.
webfilter-profile <profile_name>	Enter the web filter profile for this user. The profile must be configured in <code>webfilter_profile</code> .

The `get` form of the command returns the web filter profile setting and other information about the user. For example:

```
FMG3000 # get fmclient ldap_users
CN=Guest,CN=Users,DC=office,DC=example,

dn                : CN=Guest,CN=Users,DC=office,DC=example,DC=com
domain            : office.example.com
ldap-server       : OurWindowsAD
name              : Guest
type              : user
webfilter-profile : Adult
```

ldapsetting

Use this command to configure access to LDAP servers for per-user web filtering on a Windows AD network. After you configure the LDAP server settings, run the `fmclient sync-ldap` command to retrieve user and group information.

Syntax

```
config fmclient ldapsetting
  edit <srvname>
    set base_dn <basedn>
    set bind_dn <binddn>
    set ldap_host <hostaddr>
    set ldap_port <portno>
    set password <pwd_str>
  end
```

Variable	Description
edit <srvname>	Enter a name for this LDAP server.
base_dn <basedn>	Enter the base distinguished name for the LDAP server. (Maximum 255 characters)
bind_dn <binddn>	Enter the bind distinguished name for the LDAP server. (Maximum 255 characters)
ldap_host <hostaddr>	Enter the IP address or host name of the LDAP server.
ldap_port <portno>	Enter the port number for the LDAP server. Default: 389
password <pwd_str>	Enter the password for authenticated access to the LDAP server.

license_key

Use this command to assign license keys to client groups. The new key takes effect when you deploy the revised configuration.

Syntax

```
config fmclient license_key
  edit <lic_key>
    set comment <comment_str>
    set groups <grp1_id grp1_id>
  end
```

Variable	Description
<lic_key>	Enter the license key.

Variable	Description
comment <comment_str>	Optionally enter a description or comment.
groups <grp1_id grp2_id>	Enter the IDs of client groups licensed with this key. To list client group IDs and names, enter set groups ?

location_aware

Syntax

```

config fmclient location_aware
  edit <name>
    set criteria_gateway_mac <string>
    set criteria_match {all | any | exact}
    set criteria_ping_server <string>
    set description <string>
    set firewall_action {allow | normal}
    set firewall_profile {business | custom | home}
    set firewall_trusted_ip_status {disable | enable}
    set webfilter_behavior {allow | block}
    set webfilter_profile-name {Adult | Child | Default}
    set webfilter_status {disable | enable}
  end
end

```

Variable	Description
<name>	
criteria_gateway_mac <string>	Gateway MAC address.
criteria_match {all any exact}	Criteria match. Default: all
criteria_ping_server <string>	Pingable IP address.
description <string>	Description.
firewall_action {allow normal}	Set the default firewall action for the application. Default: normal
firewall_profile {business custom home}	Firewall profile. <ul style="list-style-type: none"> Business: basic business use Custom: custom profile Home: basic home use Default: home
firewall_trusted_ip_status {disable enable}	Enable trusted IP. Default: disable

Variable	Description
<code>webfilter_behavior {allow block}</code>	Set the default behavior for unrated URLs. Default: block
<code>webfilter_profile-name {Adult Child Default}</code>	Set the web filter profile name.
<code>webfilter_status {disable enable}</code>	Enable the web filter. Default: disable

lockdown

Use this command to configure FortiClient lockdown through the FortiManager unit. With the lock-down enabled, all configuration on the managed FortiClient agents will be read-only except VPN. However, if you want to allow a FortiClient user to modify the configuration, you can send the lockdown password to the user who can then unlock the configuration. For information on FortiClient unlock feature, see [FortiClient Endpoint Security User Guide](#).

Syntax

```
config fmclient lockdown
    set password <passwd>
    set status {enable | disable}
end
```

Variable	Description
<code>password <passwd></code>	Enter the lockdown password.
<code>status {enable disable}</code>	Disable or enable lockdown setting. Default: disable

systemsetting

Use this command to configure FortiClient Manager global settings pertaining to

- dynamic grouping
- firewall and antivirus alerts
- automatic retrieval of configuration from newly-added clients

Syntax

```
config fmclient systemsetting
    set debug_timing {enable | disable}
    set grouping_skip_static {yes | no}
    set log_level <log_level>
    set monitor_event_duration <days>
    set monitor_eventlogging_duration <days>
    set retrieve_new_client_config {yes | no}
    set update_for_unmanaged {enable | disable}
```

end

Variable	Description
debug_timing {enable disable}	Enable debug timing to support performance monitoring. Default: disable
grouping_skip_static {yes no}	Select yes to skip searching members of static groups when forming dynamic groups. Default: no
log_level <log_level>	Set logging level. 0 = error, 1 = information, 2 = debug Default: 0
monitor_event_duration <days>	Enter the number of days that firewall and antivirus alerts are retained before automatic deletion. Enter 0 to keep alerts until you manually delete them. Default: 30
monitor_eventlogging_duration <days>	Enter the number of days that management event logs are retained before automatic deletion. Enter 0 to keep event logs until you manually delete them. Default: 30
retrieve_new_client_config {yes no}	Select yes to retrieve the configuration from a new client when it is added to the managed clients list. Default: no
update_for_unmanaged {enable disable}	Select to provide antivirus update services for unmanaged FortiClient installations. Default: disable

webfilter_profile

Use this command to configure web filter profiles.

Syntax

```
config fmclient webfilter-profile
  edit <wprofile_name>
    set blocked_categories {cat1,cat2,...catn}
    set blocked_classification {class1,class2, ...classn}
    set blocked_urls {url1,url2,...urln}
    set bypassed_urls {url1,url2,...urln}
    set comments <string>
```

end

Variable	Description
edit <wprofile_name>	Enter a name for this web filter profile.
blocked_categories {cat1,cat2,...catn}	Enter a comma-separated list of FortiGuard categories to block. For a list of categories, enter <code>set blocked_categories?</code>
blocked_classification {class1,class2, ...classn}	Enter a comma-separated list of FortiGuard classifications to block. For a list of classifications, enter <code>set blocked_classification?</code>
blocked_urls {url1,url2,...urln}	Enter a comma-separated list of URLs to always block, regardless of FortiGuard ratings.
bypassed_urls {url1,url2,...urln}	Enter a comma-separated list of URLs that are not subject to web filtering.
comments <string>	Optionally, enter a descriptive comment about this profile.

fcdevice

Use fcdevice commands to configure FortiClient agents and groups managed by the FortiManager unit.

This chapter contains following sections:

group	ungroup	unit
-----------------------	-------------------------	----------------------

group

Use this command to configure the group-shared FortiClient agent settings.

Syntax

```
config fcdevice group
  edit <name>
    set comment <string>
    set dns_domain <domain_name>
    set enterprise_client_license
    set fmgaddr <fmgr_ip>
    set fmg_sn <serno>
    set groupid
    set ip_address <ip>
    set member <uid>
    set order <order-int>
    set os_name <os-name>
    set parent <grp_name>
    set policy {dnsdomain | ip_address | os | windows_group}
    set type {dynamic | static}
    set windows_group <wingrpname>
  end
```

Variable	Description
<name>	Add or modify a FortiClient agent group.
comment <string>	Enter a description for this group. Enclose the description in quotes if it contains spaces.
dns_domain <domain_name>	If policy is dns_domain, enter the DNS domain name.
enterprise_client_license	Enterprise client license.
fmgaddr <fmgr_ip>	Enter the IP Address of the FortiManager server. Default: 0.0.0.0
fmg_sn <serno>	Enter the serial number of the FortiManager server.

Variable	Description
<code>groupid</code>	The group ID. Cannot be set.
<code>ip_address <ip></code>	<p>If <code>policy</code> is <code>ip_address</code>, enter one of:</p> <p>IP address, for example "192.168.1.2"</p> <p>IP address range, for example "192.168.1.2-192.168.1.5"</p> <p>Subnet address, for example "192.168.1.0/24"</p>
<code>member <uid></code>	If <code>policy</code> is <code>static</code> , enter the device names to be included in the group.
<code>order <order-int></code>	<p>Optionally, change the order number to change the relative position of the group in the Web-based Manager navigation frame. By default, a new group is listed after existing ones.</p> <p>Default: Set on creation</p>
<code>os_name <os-name></code>	If <code>policy</code> is <code>os</code> , enter the OS name.
<code>policy {dnsdomain ip_address os windows_group}</code>	<p>If <code>type</code> is <code>dynamic</code>, select criterion for group membership:</p> <ul style="list-style-type: none"> • <code>dnsdomain</code> — DNS domain • <code>ip_address</code> — IP Address • <code>os</code> — Operating system type • <code>windows_group</code> — Windows Group
<code>parent <grp_name></code>	If this is a nested group, enter the parent group name.
<code>type {dynamic static}</code>	<p>Select a group type.</p> <ul style="list-style-type: none"> • <code>static</code> - specify members by name • <code>dynamic</code> - define membership by DNS domain, IP address, OS type or Windows group. <p>Default: <code>static</code></p>
<code>windows_group <wingrpname></code>	If <code>policy</code> is <code>windows_group</code> , enter the Windows workgroup or domain name.

Related topics

- [ungroup](#)
- [unit](#)

ungroup

Use this command to obtain information about ungrouped FortiClient agents. You can also add a description for the ungrouped agents.

Syntax

```
config fcdevice ungroup
  edit <name>
    set description <string>
  end
```

Variable	Description
<name>	Modify a FortiClient PC. You can only modify description. All other keywords are read-only.
description <string>	Enter a comment of up to 255 bytes.

```
get fcdevice ungroup <name>
```

The get command retrieves information like this:

```
host_name           : fips-1
av_db_ver           : 6.467
av_engine_ver       : 2.85
description         : (null)
dns_domain          : (null)
expiry_date         : No License
ip                  : 172.20.120.54
last_connection     : 2007-03-06 20:38:47
online              : yes
os_name             : Windows 2000 Service Pack 4
sn                  : FCT9003215254778
status_av           : enable
status_firewall     : enable
status_vpn          : enable
status_wf           : enable
version             : 4.0.395
windows_group       : WORKGROUP
```

Related topics

- [group](#)
- [unit](#)

unit

Use this command to get information about an individual FortiClient agent or to add a description for a FortiClient agent.

Syntax

```
config fcdevice unit
  edit <host_name>
    set description <string>
  end
```

Variable	Description
<host_name>	Edit the agent name.
description <string>	Enter a description for this agent. Enclose the description in quotes if it contains spaces.

```
get fcdevice unit <name>
```

The get command retrieves information like this:

```
host_name           : fips-1
av_db_ver           : 6.467
av_engine_ver       : 2.85
description         : (null)
dns_domain          : (null)
expiry_date         : No License
group               :
ip                  : 172.20.120.54
last_connection     : 2012-08-14 20:38:47
online              : yes
os_name             : Windows XP Service Pack 2
sn                  : FCT9003215254778
status_av           : enable
status_firewall     : enable
status_vpn          : enable
status_wf           : enable
version             : 4.1.0143
windows_group       : TECHDOC
```

Related topics

- [group](#)
- [ungroup](#)

fcpolicy

Use `fcpolicy` commands to configure the settings of a FortiClient agent. Configuring a single FortiClient agent using the FortiClient Manager is very similar to configuring the FortiClient program on a personal computer. Using the FortiClient Manager, you can configure and manage multiple FortiClient agents without logging on to each personal computer separately. You can also install all the configuration changes at once.

Before using these commands, you first need to select a registered FortiClient agent or FortiClient agent group that you want to configure by using one of the following `execute` commands:

To select a device: `execute fcpolicy unit <host_name>`

To select a group: `execute fcpolicy group <group_name>`

This chapter contains the following sections:

antileak option	firewall addrgrp	firewall zone
antileak sensword	firewall apppolicy	log setting
antispam bannedword	firewall option	system locationaware
antispam blackwhitelist	firewall pingserver	system settings
antispam option	firewall policy	system trustedfortimanager
antivirus scheduledscan	firewall protocol	system wan_optimization
antivirus setting email	firewall protocolgrp	vpn download
antivirus setting realtime	firewall schedule recurring	vpn option
antivirus setting scheduledscan	firewall schedulegrp	vpn security_policy
firewall address	firewall service	webfilter option
	firewall trustedip address	webfilter profile

antileak option

Use this command to configure antileak options.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antileak option
    set action {block | log}
    set enable {enable | disable}
    set override {yes | no}
```

end

Variable	Description
<code>action {block log}</code>	Set action to take when leakage detected: <ul style="list-style-type: none">• <code>block</code> - block sending of email suspected of leakage• <code>log</code> - log leakage incident Default: log
<code>enable {enable disable}</code>	Enable or disable Antileak feature. Default: disable
<code>override {yes no}</code>	Enter <code>yes</code> to configure options for a unit that differ from the group configuration. Default: no

Related topics

- `antileak sensword`

antileak sensword

Use this command to configure the antileak sensitive word list.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antileak sensword
  edit <senswordid>
    set override {yes | no}
    set sensword <string>
  end
```

Variable	Description
<code>edit <senswordid></code>	Enter an integer ID to identify the entry.
<code>sensword <string></code>	Enter the sensitive word.
<code>override {yes no}</code>	Enter <code>yes</code> to configure options for a unit that differ from the group configuration. Default: no

Related topics

- `antileak option`

antispam bannedword

Use this command to configure the antispam banned word list.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antispam bannedword
  edit <bannedwordid>
    set bannedword <string>
    set override {yes | no}
  end
```

Variable	Description
bannedword <string>	Enter the sensitive word.
override {yes no}	Enter yes to configure options for a unit that differ from the group configuration. Default: no

Related topics

- `antispam blackwhitelist`
- `antispam option`

antispam blackwhitelist

Use this command to configure the antispam black/white list.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antispam blackwhitelist
  edit <bwlid>
    set emailaddress <emailaddr>
    set override {yes | no}
    set status {allow | block}
  end
```

Variable	Description
emailaddress <emailaddr>	Enter the email address.

Variable	Description
<code>override {yes no}</code>	Enter <code>yes</code> to configure options for a unit that differ from the group configuration. Default: <code>no</code>
<code>status {allow block}</code>	Enter <code>allow</code> to add to whitelist. Enter <code>block</code> to add to blacklist. Default: <code>block</code>

Related topics

- `antispam bannedword`
- `antispam option`

antispam option

Use this command to configure antispam options.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antispam option
    set antispam-port <portnum>
    set antispam-server <srv_ip>
    set antispam-using-override-server {enable | disable}
    set auto_submit {enable | disable}
    set dont_prompt {enable | disable}
    set enable_antispam {enable | disable}
    set override {yes | no}
end
```

Variable	Description
<code>antispam-port <portnum></code>	Enter the override Antispam server port number.
<code>antispam-server <srv_ip></code>	Enter the override Antispam server IP address.
<code>antispam-using-override-server {enable disable}</code>	Enable or disable use of override antispam server. Default: <code>disable</code>
<code>auto_submit {enable disable}</code>	Enable or disable auto-submission of misclassified email to Fortinet. Default: <code>disable</code>

Variable	Description
<code>dont_prompt {enable disable}</code>	Enable if you do not want users prompted to submit misclassified email to Fortinet. Default: disable
<code>enable_antisipam {enable disable}</code>	Enable or disable the antisipam feature. Default: disable
<code>override {yes no}</code>	Enter <code>yes</code> to configure options for a unit that differ from the group configuration. Default: no

Related topics

- `antisipam bannedword`
- `antisipam blackwhitelist`

antivirus scheduledscan

Use this command to configure antivirus scheduled scan.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antivirus scheduledscan
    edit <name>
        set comments <string>
        set day {sunday monday ...}
        set override {no | yes}
        set scan_level {basic | full}
        set scan_options
        set time {hh:mm}
        set type {daily | one-time | weekly}
    end
```

Variable	Description
<code>edit <name></code>	Create or edit a scheduled scan.
<code>comments <string></code>	Comments on the scheduled scan.
<code>day {sunday monday ...}</code>	For weekly scan, enter the days on which the scan runs. Default: sunday
<code>override {no yes}</code>	Select <code>yes</code> to enable modification of settings. Default: no

Variable	Description
scan_level {basic full}	Select the scan level. Default: basic
scan_options	Select scan options.
time {hh:mm}	Enter the scheduled hour and minute.
type {daily one-time weekly}	Select the scan frequency. Default: daily

antivirus setting email

Use this command to configure antivirus email scan settings.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antivirus setting email
    set action <action>
    set heuristic <disable | enable>
    set override {no | yes}
    set status {disable | enable}
    set virus-scanning {none | outlook | pop3 | smtp}
    set worm-scan <disable | enable>
end
```

Variable	Description
action <action>	Select <action> when a virus is found in email: <ul style="list-style-type: none"> • log-alert — Log the virus. Send an email alert. • strip-quarantine — Quarantine virus email attachment. Default: log-alert
heuristic <disable enable>	Disable or enable heuristic scan of email attachments. Default: disable
override {no yes}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group. Default: no
status {disable enable}	Disable or enable email scanning. Default: disable

Variable	Description
virus-scanning {none outlook pop3 smtp}	Select the protocols to scan.
worm-scan <disable enable>	Disable or enable preventing worms from spreading with emails. Default: disable

antivirus setting realtime

Use this command to configure the real-time protection settings to specify what types of files to scan and exclude and what happens when a virus is detected during real-time system monitoring.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```

config fcpolicy antivirus setting realtime
    set action {clean | deny | quarantine}
    set dont-popup-in-monitor {disable | enable}
    set dont-popup-in-scan {disable | enable}
    set exempt-files <string>
    set exempt-folders <string>
    set exempt-types <string>
    set heuristic {disable | enable}
    set heuristic-scan-action {deny | warning_only}
    set max-compress-file-size <integer>
    set override {no | yes}
    set scan-compress {no | yes}
    set scan-grayware {adware | dialer | keylogger | spyware | none}
    set scan-options <options>
    set status <rtstatus>
    set use-extended-db {disable | enable}
    set use-small-db {disable | enable}
end

```

Variable	Description
action {clean deny quarantine}	<ul style="list-style-type: none"> • clean — The FortiClient agent attempts to remove the virus from the infected file. If FortiClient cannot clean an infected file, it quarantines the file automatically. • deny — You cannot open, run or modify the file until it is cleaned. • Quarantine — Move the file to a quarantine directory. Default: deny

Variable	Description
dont-popup-in-monitor {disable enable}	Do not popup alert message box in registry monitor.
dont-popup-in-scan {disable enable}	Do not popup alert message box in real-time scan.
exempt-files <string>	Enter a comma-separated list of file names to exclude from real-time antivirus checking.
exempt-folders <string>	Enter a comma-separated list of folder names to exclude from real time antivirus checking.
exempt-types <string>	Add the file types that you do not want to scan.
heuristic {disable enable}	Disable or enable heuristic scanning. Default: disable
heuristic-scan-action {deny warning_only}	Heuristic scan action.
max-compress-file-size <integer>	Specify the file size scan limit. Default: 0
override {no yes}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group. Default: no
scan-compress {no yes}	Specify whether to scan the compressed files. Default: no
scan-grayware {adware dialer keylogger spyware none}	Specify which grayware to scan.
scan-options <options>	Enter one or more of the following options: <ul style="list-style-type: none"> network_drives — Scan network drives. reading_from_disk — Scan when reading from disk. writing_to_disk — Scan when writing to disk. none — No scan. To clear all options, enter <code>unset scan-options</code> .
status <rtstatus>	Set real-time protection status to one of: <ul style="list-style-type: none"> disable — No real time protection enable_monitor_startup — Monitor program startup list. enable_realtime_protection — Real-time protection enabled.
use-extended-db {disable enable}	Use Extended DB (Extended DB is supported by FortiClient 4.1 and later).
use-small-db {disable enable}	Use Small DB (Small DB is only supported by FortiClient 4.0).

Use this command to configure advanced antivirus scheduled scan settings.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy antivirus setting scheduledscan
    set action {clean | deny | quarantine}
    set exempt-files <string>
    set exempt-folders <string>
    set exempt-types <string>
    set heuristic {disable | enable}
    set max-compress-file-size <integer>
    set override {no | yes}
    set pause-scan-on-ups {enable | disable}
    set scan-compress {enable | disable}
    set scan-grayware {adware dialer keylogger spyware}
    set scan-on-insertion {enable | disable}
    set shellintegrate {enable | disable}
    set signature-warning {enable | disable}
end
```

Variable	Description
<code>action {clean deny quarantine}</code>	<ul style="list-style-type: none">• clean: The FortiClient agent attempts to remove the virus from the infected file. If FortiClient cannot clean an infected file, it quarantines the file automatically.• deny: You cannot open, run or modify the file until it is cleaned.• quarantine: Move the file to a quarantine directory.
<code>exempt-files <string></code>	Enter a comma-separated list of file names to exclude from real-time antivirus checking.
<code>exempt-folders <string></code>	Enter a comma-separated list of folder names to exclude from real-time antivirus checking.
<code>exempt-types <string></code>	Add the file types that you do not want to scan.
<code>heuristic {disable enable}</code>	Disable or enable heuristic scanning. Default: disable
<code>max-compress-file-size <integer></code>	Specify the file size scan limit. Default: 0
<code>override {no yes}</code>	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group. Default: no

Variable	Description
pause-scan-on-ups {enable disable}	Pause AV scanning if computer switches to battery power or UPS. Default: enable
scan-compress {enable disable}	Specify whether to scan the compressed files. Default: disable
scan-grayware {adware dialer keylogger spyware}	Specify which greyware to scan.
scan-on-insertion {enable disable}	Enable or disable scanning of removable media on insertion. Default: disable
shellintegrate {enable disable}	Enable or disable integration with Windows Explorer. Default: disable
signature-warning {enable disable}	Enable or disable notification when virus signature is out-of-date. Default: disable

firewall address

Use this command to add and edit addresses used in firewall policies.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```

config fcpolicy firewall address
  edit <name>
    set comment <string>
    set end_ip <ip>
    set fqdn <fqdn>
    set ip_address <ip>
    set ip_mask <ip&netmask>
    set override {no |yes}
    set start_ip <ip>
    set type {ip | iprange | subnet | fqdn}
  end

```

Variable	Description
edit <name>	Create or edit a firewall address.
comment <string>	Add comments for the firewall address.

Variable	Description
<code>end_ip <ip></code>	Enter the firewall address' end IP if <code>type</code> is <code>iprange</code> .
<code>fqdn <fqdn></code>	Enter the fully-qualified domain name if <code>type</code> is <code>fqdn</code> .
<code>ip_address <ip></code>	Enter the IP address. This is available when <code>type</code> is <code>ip</code> .
<code>ip_mask <ip&netmask></code>	Enter the firewall IP address and subnet mask. Format: <code>xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx</code> This is available when <code>type</code> is <code>subnet</code> .
<code>override {no yes}</code>	Select <code>yes</code> if you want this FortiClient agent uses its own firewall address instead of inheriting the address from a group in which this FortiClient agent is a member. Otherwise select <code>no</code> . Default: <code>no</code>
<code>start_ip <ip></code>	Enter the firewall address' start IP if <code>type</code> is <code>iprange</code> .
<code>type {ip iprange subnet fqdn}</code>	Select the firewall address type: <ul style="list-style-type: none"> <code>ip</code> — single IP address <code>iprange</code> — range of IP addresses <code>subnet</code> — subnet address <code>fqdn</code> — fully-qualified domain name Default: <code>ip</code>

firewall addrgrp

Use this command to configure address groups used in firewall policies.

There are three built-in address groups that correspond to the security zones in the FortiClient application: Blocked, Public, and Trusted. You can modify these address groups, but you cannot delete them.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall addrgrp
edit <name>
set comments <string>
set member <addr1 addr2 ...>
set override {no |yes}
```

end

Variable	Description
edit <name>	Create or edit a firewall address group.
comments <string>	Add comments for the firewall address
member <addr1 addr2 ...>	Select members for the group.
override {no yes}	Select yes if you want this FortiClient agent to use its own firewall address group settings instead of inheriting the settings from the group in which this FortiClient agent is a member. Otherwise select no . Default: no

firewall apppolicy

Use this command to define firewall policies that control application access to the network.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall apppolicy
  edit <app_policy_id>
    set action {allow | block}
    set comments <string>
    set destination <address_name>
    set override {no | yes}
    set protocol <protocol_name>
    set schedule <sched_name>
    set service <service_name>
    set source <address_name>
    set status {enable | disable}
  end
```

Variable	Description
edit <app_policy_id>	Enter a policy ID for this firewall application policy.
action {allow block}	Select how to respond to the application's connection attempt. Default: allow
comments <string>	Optionally enter a descriptive comment.

Variable	Description
<code>destination <address_name></code>	<p>Enter the destination address or address group to which the policy applies.</p> <p>Available addresses include Blocked, Trusted, and Public zones.</p> <p>Use the <code>firewall address</code> command to define addresses.</p>
<code>override {no yes}</code>	<p>Select <code>yes</code> if you want this FortiClient agent uses its own firewall policy settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise, select <code>no</code>.</p> <p>Default: <code>no</code></p>
<code>protocol <protocol_name></code>	<p>Select the network protocols to which this policy applies.</p> <p>Default: <code><any></code></p>
<code>schedule <sched_name></code>	<p>Select the firewall schedule that controls when the policy should be active.</p>
<code>service <service_name></code>	<p>Select the service/application to which the policy applies.</p>
<code>source <address_name></code>	<p>Enter the destination address or address group to which the policy applies.</p> <p>Available addresses include Blocked, Trusted, and Public zones.</p> <p>Use the <code>firewall address</code> command to define addresses.</p>
<code>status {enable disable}</code>	<p>Enable or disable this policy.</p> <p>Default: <code>disable</code></p>

Related topics

- `firewall address`
- `firewall addrgrp`
- `firewall protocol`
- `firewall protocolgrp`
- `firewall schedule recurring`
- `firewall service`

firewall option

Use this command to:

- `set firewall policy default action`
- `set zone security settings`
- `set whether the firewall displays blocked traffic notifications on the agent`
- `set whether FortiClient checks ping servers to determine trustworthiness of new networks`
- `enable trusted IP addresses`

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall option
    set disable-firewall-notify {yes | no}
    set enable_firewall {yes | no}
    set firewall-profile <profile_name>
    set launch-new-application {allow | follow_default}
    set override {no | yes}
    set ping-server {enable | disable}
    set ping_ttl {enable | disable}
    set public-zone-level {high | medium | low}
    set rule_order {allow | deny}
    set trusted-zone-level {high | medium | low}
    set trustip-status {enable | disable}
end
```

Variable	Description
<code>disable-firewall-notify {yes no}</code>	Enter yes to disable FortiTray notification of blocked traffic on the FortiClient agent. Default: no
<code>enable_firewall {yes no}</code>	Enable the firewall.
<code>firewall-profile <profile_name></code>	Enter the firewall profile to use: <ul style="list-style-type: none"> • <code>basic_business</code> — Allow all outgoing traffic, allow all incoming traffic from the trusted zone, and deny all incoming traffic from the public zone. • <code>basic_home</code> — Allow all outgoing traffic and deny all incoming traffic • <code>cust_profile</code> — You can configure firewall policies to control application access to the network and to control traffic between address groups. Default: <code>basic_home</code>
<code>launch-new-application {allow follow_default}</code>	Select the firewall action when an unknown application tries to communicate through the firewall: <ul style="list-style-type: none"> • <code>allow</code> — Allow the application to communicate, but raise a firewall violation alert. • <code>follow_default</code> — Follow the <code>firewall-profile</code> setting. Default: <code>follow-default</code> <p>Note: The FortiClient application can be installed with the <code>DEFAULTAPPACTION=1</code> option, which causes it to always block an unknown application and raise a firewall violation alert.</p>

Variable	Description
<code>override {no yes}</code>	Select <code>yes</code> if you want this FortiClient agent to use its own firewall option settings instead of inheriting the settings from the group in which this FortiClient agent is a member. Otherwise select <code>no</code> .
<code>ping-server {enable disable}</code>	Enable the FortiClient application to check ping servers when it is connected to a new network, such as a wireless access point. For information about defining the ping servers, see "firewall pingserver" on page 142 . Default: <code>disable</code>
<code>ping_ttl {enable disable}</code>	Ping TTL.
<code>public-zone-level {high medium low}</code>	Set the security level for the public zone. <ul style="list-style-type: none"> • <code>high</code> — Block ICMP, NetBIOS, but allow other traffic coming from this zone. • <code>medium</code> — Block ICMP and NetBIOS from this zone, but allow other traffic. Allow NetBIOS to this zone. • <code>low</code> — Allow all traffic, except where disallowed by application policies. Default: <code>high</code>
<code>rule_order {allow deny}</code>	Global firewall policy rule order.
<code>trusted-zone-level {high medium low}</code>	Set the security level for the trusted zone. <ul style="list-style-type: none"> • <code>high</code> — Block ICMP, NetBIOS, but allow other traffic coming from this zone. • <code>medium</code> — Allow all traffic to and from this zone. • <code>low</code> — Allow all traffic, except where disallowed by application policies. Default: <code>medium</code>
<code>trustip-status {enable disable}</code>	Select <code>enable</code> to exempt the addresses defined in <code>fcpolicy firewall trustedip</code> from intrusion prevention scanning. Default: <code>disable</code>

Related topics

- [firewall policy](#)
- [firewall pingserver](#)

firewall pingserver

Use this command to configure ping servers to use with the `ping-server` option in `firewall` option.

Syntax

```
config fcpolicy firewall pingserver
  edit <pingserver_name>
    set ip_fqdn <ip_fqdn>
    set override {no | yes}
  end
```

Variables	Description
<code>edit <pingserver_name></code>	Enter a name for the ping server.
<code>ip_fqdn <ip_fqdn></code>	Enter the IP address or FQDN of the ping server.
<code>override {no yes}</code>	Select <code>yes</code> if you want this FortiClient agent uses its own firewall policy settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise, select <code>no</code> . Default: <code>no</code>

Related topics

- `firewall` option, see `ping-server {enable | disable}`

firewall policy

Use this command to configure firewall policies.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: execute `fcpolicy unit <host_name>`
- to select a group: execute `fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall policy
  edit <integer>
    set action {allow | block}
    set adapters <string>
    set comments <string>
    set destination <address_name>
    set override {no | yes}
    set protocol <protocol_name>
    set schedule <sched_name>
    set service <service_name>
    set source <address_name>
    set status {enable | disable}
```

end

Variable	Description
edit <integer>	Create or edit a firewall policy by entering a policy ID.
action {allow block}	Select the response to make when the policy matches a connection attempt. Default: allow
adapters <string>	
comments <string>	Add comments for the firewall policy.
destination <address_name>	Enter the destination address or address group to which the policy applies. Available addresses include Blocked, Trusted, and Public zones. Use the <code>firewall address</code> command to define addresses.
override {no yes}	Select <code>yes</code> if you want this FortiClient agent uses its own firewall policy settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise, select <code>no</code> . Default: no
protocol <protocol_name>	Select the network protocols to which this policy applies. Default: <any>
schedule <sched_name>	Select the firewall schedule that controls when the policy should be active.
service <service_name>	Select the service/application to which the policy applies.
source <address_name>	Enter the destination address or address group to which the policy applies. Available addresses include Blocked, Trusted, and Public zones. Use the <code>firewall address</code> command to define addresses.
status {enable disable}	Enable or disable this policy. Default: disable

Related topics

- `firewall address`
- `firewall addrgrp`
- `firewall protocol`
- `firewall protocolgrp`
- `firewall schedule recurring`
- `firewall service`

firewall protocol

Use this command to define protocols for use in firewall policies.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall protocol
  edit <protocol_name>
    set comment <string>
    set destport <portnum>
    set override {no | yes}
    set srcport <portnum>
    set type {tcp | udp | tcpudp | icmp}
  end
```

Variables	Description
<code>edit <protocol_name></code>	Enter a name for the protocol.
<code>comment <string></code>	Optionally, enter a descriptive comment.
<code>destport <portnum></code>	Enter the destination port for the protocol. Default: 0
<code>override {no yes}</code>	Select <code>yes</code> if you want this FortiClient agent uses its own firewall policy settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise, select <code>no</code> . Default: no
<code>srcport <portnum></code>	Enter the source port for the protocol. Default: 0
<code>type {tcp udp tcpudp icmp}</code>	Select the type of protocol: <ul style="list-style-type: none">• TCP• UDP• TCP/UDP• ICMP Default: tcp

Related topics

- `firewall protocolgrp`
- `firewall policy`
- `firewall apppolicy`

firewall protocolgrp

Use this command to define protocol groups for use in firewall policies.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall protocol
  edit <protocol_grp_name>
    set comments <string>
    set member {prot1 prot2 ...}
    set override {no | yes}
  end
```

Variables	Description
<code>edit <protocol_grp_name></code>	Enter a name for this protocol group.
<code>comments <string></code>	Optionally, enter a descriptive comment.
<code>member {prot1 prot2 ...}</code>	Enter the names of the protocols that belong to this group. Use the <code>firewall protocol</code> command to define protocols.
<code>override {no yes}</code>	Select <code>yes</code> if you want this FortiClient agent uses its own firewall policy settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise, select <code>no</code> . Default: no

Related topics

- `firewall protocol`
- `firewall policy`
- `firewall apppolicy`

firewall schedule recurring

Use this command to configure recurring schedules used in firewall policies.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall schedule recurring
  edit <name>
    set comments <string>
    set day {friday | monday | saturday | sunday | thursday |
            tuesday | wednesday}
    set end <hh:mm>
    set override {no |yes}
    set start <hh:mm>
  end
```

Variable	Description
edit <name>	Create or modify a recurring schedule.
comments <string>	Add comments for the recurring schedule.
day {friday monday saturday sunday thursday tuesday wednesday}	Enter the start day for the schedule. Default: sunday
end <hh:mm>	Enter the end time for the schedule. Default: 00:00
override {no yes}	Select yes if you want this FortiClient agent uses its own firewall recurring schedule settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise select no . Default: no
start <hh:mm>	Enter the start time for the schedule. Default: 00:00

Related topics

- [firewall policy](#)
- [firewall apppolicy](#)

firewall schedulegrp

Use this command to configure firewall schedule groups.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall schedulegrp
  edit <name>
    set comments <string>
    set member {sched1 sched2 ...}
    set override {no | yes}
  end
```

Variable	Description
edit <name>	Create or edit a firewall schedule group.
comments <string>	Add comments for the firewall schedule group.
member {sched1 sched2 ...}	Select existing schedules as members for the group.
override {no yes}	Select yes if you want this FortiClient agent uses its own firewall schedule group settings instead of inheriting the settings from the group in which this FortiClient agent is a member. Otherwise select no . Default: no

Related topics

- `firewall schedule recurring`
- `firewall policy`
- `firewall apppolicy`

firewall service

Use this command to define applications used in application firewall policies.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall service
  edit <name>
    set checksum <integer>
    set comments <string>
    set executable <exe_name>
    set filesize <integer>
    set override {no | yes}
    set rule_order {allow | deny}
```

end

Variable	Description
edit <name>	Enter a name for this service.
checksum <integer>	Enter the CRC32 checksum of the executable file. The checksum and file size are used to uniquely identify the executable file of the firewall service. Default: 1
comments <string>	Add comments for the firewall service.
executable <exe_name>	Enter the executable file name of application. For example, the executable of Internet Explorer is iexplorer.exe. Leave <code>executable</code> empty to create a service that applies to all applications.
filesize <integer>	Enter the size of the executable file. Default: 0
override {no yes}	Select <code>yes</code> if you want this FortiClient agent uses its own firewall service settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise select <code>no</code> . Default: no
rule_order {allow deny}	The order of firewall rules for this application.

Related topics

- [firewall policy](#)
- [firewall apppolicy](#)
- [firewall protocol](#)

firewall trustedip address

Use this command to define trusted IP addresses, ranges or subnets that are exempt from intrusion detection. Use the `firewall option` command to enable trusted IPs.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall trustedip address
  edit <addr_name>
    set end_ip <ipv4>
    set ip_address <ipv4>
    set ip_mask <ipv4mask>
    set override {no | yes}
```

```

set start_ip <ipv4>
set type <addr_type>
end

```

Variable	Description
edit <addr_name>	Enter a name for the trusted address.
end_ip <ipv4>	If type is iprange, enter the range end IP address. Default: 0.0.0.0
ip_address <ipv4>	If type is ip, enter the IP address. Default: 0.0.0.0
ip_mask <ipv4mask>	If type is subnet, enter the IP address and network mask. Default: 0.0.0.0 0.0.0.0
override {no yes}	Select yes if you want this FortiClient agent uses its own firewall service settings instead of inheriting the settings from a group in which this FortiClient agent is a member. Otherwise select no. Default: no
start_ip <ipv4>	If type is iprange, enter the range start IP address. Default: 0.0.0.0
type <addr_type>	Select the trusted IP address type: <ul style="list-style-type: none"> ip — single IP address iprange — range of IP addresses subnet — subnet address Default: ip

Related topics

- `firewall option`

firewall zone

Use this command to configure the high and medium security levels for the Public and Trusted firewall zones.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy firewall zone
    set pubhigh {disable | enable}
    set pubmedium {disable | enable}
    set trusthigh {disable | enable}
    set trustmedium {disable | enable}
end
```

Variable	Description
pubhigh {disable enable}	Public Zone high level
pubmedium {disable enable}	Public Zone medium level
trusthigh {disable enable}	Trusted Zone high level
trustmedium {disable enable}	Trusted Zone medium level

Related topics

- `firewall option`

log setting

Use this command to configure logging settings for FortiClient agents.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy log setting
    set custom_field {enable | disable}
    set custom_field_name <string>
    set custom_field_value <string>
    set local_level {error | information | warning}
    set local_maxfilesize <integer>
    set override {no | yes}
    set remote_facility <facility>
    set remote_level {error | information | warning}
    set remote_logging {enable | disable}
    set remote_server <serv_addr>
    set remote_server_port <portnum>
    set remote_type {fortianalyzer | syslog}
```

end

Variable	Description
<code>custom_field {enable disable}</code>	Enable a custom log field to be included in all logs from this FortiClient agent. This field can appear in reports generated on the FortiAnalyzer unit. <code>custom_field_name</code> and <code>custom_field_value</code> define the field name and its value. Default: disable
<code>custom_field_name <string></code>	If <code>custom_field</code> is enabled, this is the name of the custom log field.
<code>custom_field_value <string></code>	If <code>custom_field</code> is enabled, this is the value of the custom log field.
<code>local_level {error information warning}</code>	Select the minimum severity of message to log locally. Default: warning
<code>local_maxfilesize <integer></code>	Set the log file maximum size (5120 - 3530944 KB). Default: 5120
<code>override {no yes}</code>	Override device group settings.
<code>remote_facility <facility></code>	Select the facility name to use on the remote log device. To list the facility names, enter <code>set remote_facility ?</code> Default: local7
<code>remote_level {error information warning}</code>	Select the minimum severity of message to log remotely. Default: warning
<code>remote_logging {enable disable}</code>	Enable or disable remote logging. Default: disable
<code>remote_server <serv_addr></code>	Enter the IP address or hostname of logging server.
<code>remote_server_port <portnum></code>	Enter the remote server port number. 0 means default. Default: 0
<code>remote_type {fortianalyzer syslog}</code>	Select the type of logging server: <ul style="list-style-type: none">• fortianalyzer• syslog Default: fortianalyzer

system locationaware

Syntax

```
config fcpolicy system locationaware
  set member <string>
  set status {disable | enable}
  set override {no | yes}
end
```

Variable	Description
member <string>	Selected location aware profile.
status {disable enable}	Enable location-aware settings. Default: disable
override {no yes}	Override device group settings.

system settings

Use this command to configure FortiClient system settings.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: execute `fcpolicy unit <host_name>`
- to select a group: execute `fcpolicy group <group_name>`

Syntax

```
config fcpolicy system settings
  set act_as {enable | disable}
  set act_av {enable | disable}
  set act_fw {enable | disable}
  set act_vpn {enable | disable}
  set act_wan {enable | disable}
  set act_wf {enable | disable}
  set conn_timeout <integer>
  set disable_pop3c {enable | disable}
  set disable_pop3s {enable | disable}
  set disable_self_test {enable | disable}
  set disable_smtp {enable | disable}
  set fortiproxy_ip <ip>
  set fortiproxy_port <integer>
  set ftpproxy {enable | disable}
  set heart_interval <integer>
  set hide_tray {disable | enable}
  set load_at_startup {enable | disable}
  set lockdown_status {enable | disable}
  set not_flash_tray {enable | disable}
```

```

set online_scep {enable | disable}
set override {yes | no}
set proxy_ip <ip>
set proxy_port <integer>
set proxy_pwd <passwd>
set proxy_type {HTTP | SOCKSV4 | SOCKSV5}
set proxy_update {enable | disable}
set proxy_user <string>
set raise_alert_to_fmg {enable | disable}
set try_public_fortiguard_network {disable | enable}
set update_server {FortiManager | public | server}
set update_server_address {ip_address | FQDN}
set update_server_port <port>
set validation_type {enterprise | standard}
set virus_submission {disable | enable}
end

```

Variable	Description
act_app {enable disable}	Enable active application detection.
act_as {enable disable}	Enable active firewall.
act_av {enable disable}	Enable active antivirus.
act_fw {enable disable}	Enable active firewall.
act_vpn {enable disable}	Enable active firewall.
act_wan {enable disable}	Enable active firewall.
act_wf {enable disable}	Enable active firewall.
conn_timeout <integer>	Enter the connection timeout time.
disable_pop3c {enable disable}	Enable disable POP3 client comforting.
disable_pop3s {enable disable}	Enable disable POP3 server comforting.
disable_self_test {enable disable}	Enable disable self test.
disable_smtp {enable disable}	Enable disable SMTP.
failover_port <integer>	Enter the failover port.
fortiproxy_ip <ip>	Enter the IP address used to test network availability.
fortiproxy_port <integer>	Enter the highest port number the proxy listen on.
ftp-proxy {enable disable}	Enable or disable ftp proxy.
heart_interval <integer>	Enter the interval of heartbeat message sent to FortiManager.
hide_tray {disable enable}	Enable to hide the tray icon.

Variable	Description
<code>load_at_startup {enable disable}</code>	Enable to load FortiClient Console at startup. Default: disable
<code>lockdown_status {enable disable}</code>	Enable to lock down FortiClient configuration. Default: disable
<code>not_flash_tray {enable disable}</code>	Enable so that the tray icon does not flash.
<code>online_scep {enable disable}</code>	Enable online SCEP.
<code>override {yes no}</code>	Select <code>yes</code> to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group. Default: no
<code>proxy_ip <ip></code>	Enter the proxy setting IP address.
<code>proxy_port <integer></code>	Enter the proxy setting port.
<code>proxy_pwd <passwd></code>	Enter the proxy password.
<code>proxy_type {HTTP SOCKSV4 SOCKSV5}</code>	Enter the proxy type.
<code>proxy_update {enable disable}</code>	Enable proxy for update.
<code>proxy_user <string></code>	Enter the proxy user name.
<code>raise_alert_to_fmg {enable disable}</code>	Enable to raise AV alerts to the FortiManager unit. Default: disable
<code>try_public_fortiguard_network {disable enable}</code>	When enabled, if the connection to customer server fails, the public FortiGuard network will be tried.
<code>update_server {FortiManager public server}</code>	Select the source for FortiClient AV/Web Filter/Antispam updates. Default: public
<code>update_server_address {ip_address FQDN}</code>	Enter the IP address or FQDN of the FDS update server. This is available when <code>update_server</code> is <code>server</code> .
<code>update_server_port <port></code>	Enter the port number for updates. This is available when <code>update_server</code> is <code>server</code> . Default: 0
<code>validation_type {enterprise standard}</code>	Enter the validation type.
<code>virus_submission {disable enable}</code>	Enable virus submission.

system trustedfortimanager

Use this command to add trusted FortiManager units through the FortiClient Manager and push them to the FortiClient agents, so that the FortiClient agents can be managed by the trusted FortiManager units.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy system trustedfortimanager
  edit <name>
    set address <ip>
    set comments <string>
    set fqdn <fqdn>
    set override {yes | no}
    set type {fqdn | ipmask | iprange | singleip}
    set subnet <ip&netmask>
    set start_ip <ip>
    set end_ip <ip>
  end
```

Variable	Description
<code>edit <name></code>	Add or edit a trusted FortiManager unit.
<code>address <ip></code>	Enter the IP address of the FortiManager unit. This appears if you select the <code>singleip</code> type.
<code>comments <string></code>	Add any notes for a trusted FortiManager unit.
<code>fqdn <fqdn></code>	Enter the FortiManager unit fully qualified domain name. This is available when <code>type</code> is <code>fqdn</code> .
<code>override {yes no}</code>	Select <code>yes</code> to enable modification of settings. Default: <code>no</code>
<code>type {fqdn ipmask iprange singleip}</code>	Select the type for the trusted FortiManager unit. Default: <code>singleip</code>
<code>subnet <ip&netmask></code>	Enter the subnet IP address and network mask on which the unit is. Format: <code>xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx</code> This is available when <code>type</code> is <code>ipmask</code> .
<code>start_ip <ip></code>	The start IP address for the range. This is available when <code>type</code> is <code>iprange</code> .
<code>end_ip <ip></code>	The end IP address for the range. This is available when <code>type</code> is <code>iprange</code> .

system wan_optimization

Use this command to configure WAN optimization settings for FortiClient agents.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy system wan_optimization
    set cache_size <integer>
    set override {yes | no}
    set protocols {http | cifs | mapi | ftp}
    set status {enable | disable}
end
```

Variable	Description
<code>cache_size <integer></code>	Set maximum disk cache size in MBytes. Range is 256 to 32768 MBytes. Entry is rounded to nearest 64MBytes (values 256, 320, 384, and so on). If your hard disk can accommodate a larger cache, better optimization performance is possible. Default: 256
<code>override {yes no}</code>	Select <code>yes</code> to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group. Default: no
<code>protocols {http cifs mapi ftp}</code>	Select the protocols to optimize: HTTP, CIFS, MAPI, or FTP.
<code>status {enable disable}</code>	Enable or disable WAN optimization. Default: disable

vpn download

Use this command to configure the FortiClient agent to download VPN configurations from a FortiGate unit running FortiOS 4.0.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy vpn download
  edit <name>
    set override {yes | no}
    set policy server <string>
    set type <automatic>
  end
```

Variable	Description
edit <name>	Create or edit a VPN.
override {yes no}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group. Default: no
policy server <string>	Enter the IP address of the VPN gateway, that is, the FortiGate unit running FortiOS 4.0 that the FortiClient agent connects to.
type <automatic>	Select the type of methods used to create VPNs. In this release, only the automatic method is supported.

vpn option

Use this command to configure VPN options.

Syntax

```
config fcpolicy vpn option
  set allow_remember_credentials {enable | disable}
  set beep {enable | disable}
  set beep_always {enable | disable}
  set beep_timeout <integer>
  set keep_running {enable | disable}
  set vpn_b4_logon {enable | disable}
end
```

Variable	Description
allow_remember_credentials {enable disable}	Enable to allow credentials to be remembered.
beep {enable disable}	Enable to cause a beep when a connection occurs.
beep_always {enable disable}	Enable continuous beeping.
beep_timeout <integer>	Enter an amount of time after which the beeping finally stops.
keep_running {enable disable}	Keep IPsec service running forever unless manually stopped.
vpn_b4_logon {enable disable}	Start VPN before logging on to Windows.

vpn security_policy

Use this command to configure a VPN security policy the FortiClient agent. The policy requires specific FortiClient security features to be active before the user can use a VPN connection.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy vpn security_policy
    set check_antispam {enable | disable}
    set check_firewall {enable | disable}
    set check_realtime_av {enable | disable}
    set check_webfilter {enable | disable}
    set override {yes | no}
end
```

Variable	Description
check_antispam {enable disable}	Enable to require that AntiSpam is enabled. Default: disable
check_firewall {enable disable}	Enable to require that Firewall is enabled. Default: disable
check_realtime_av {enable disable}	Enable to require that Real-time Protection is enabled. Default: disable
check_webfilter {enable disable}	Enable to require that Web Filter is enabled. Default: disable
override {yes no}	Select <code>yes</code> to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group. Default: no

webfilter option

The FortiManager unit can act as the local FortiGuard Web Filter and Email Filter service center. As a result, the FortiClient agents can get the web filtering and email filtering settings from the FortiManager unit instead of from the FortiGuard server through the Internet. If you have a large number of FortiClient agents, using this feature speeds up the installation of the web filter and email filter settings.

Use this command to configure the global web filtering and email filtering settings for FortiClient Manager.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: execute `fcpolicy unit <host_name>`
- to select a group: execute `fcpolicy group <group_name>`

Syntax

```
config fcpolicy webfilter option
    set override {yes | no}
    set webfilter-default-action {allow | block}
    set webfilter-dont-rate-ip {enable | disable}
    set webfilter-log-all-urls {enable | disable}
    set webfilter-port <port_num>
    set webfilter-server <fmgi_ip>
    set webfilter-status {enable | disable}
    set webfilter-using-override-server {enable | disable}
end
```

Variable	Description
<code>override {yes no}</code>	Select <code>yes</code> to enable modification of settings. Default: <code>no</code>
<code>webfilter-default-action {allow block}</code>	Select the default web filter action which applies when there is no matching rule. Default: <code>block</code>
<code>webfilter-dont-rate-ip {enable disable}</code>	Enable to filter by domain rating only. Sometimes filtering by IP address can produce false positives. Default: <code>disable</code>
<code>webfilter-log-all-urls {enable disable}</code>	Enable or disable logging of all visited URLs. Default: <code>disable</code>
<code>webfilter-port <port_num></code>	Enter the FortiManager unit's port number. This command appears if you enable <code>webfilter-status</code> . Default: <code>0</code>
<code>webfilter-server <fmgi_ip></code>	Enter the FortiManager unit's IP address. This command appears if you enable <code>webfilter-status</code> .
<code>webfilter-status {enable disable}</code>	Enable or disable the FortiClient agent to get the web filter settings from the FortiManager unit. Default: <code>disable</code>
<code>webfilter-using-override-server {enable disable}</code>	Enable or disable use of override server for web filtering service. Default: <code>disable</code>

webfilter profile

Use this command to assign web filter profiles to FortiClient agents. You can also enable per-user web filtering.

Before using this command, you must first select the FortiClient agent or FortiClient agent group that you want to configure:

- to select a device: `execute fcpolicy unit <host_name>`
- to select a group: `execute fcpolicy group <group_name>`

Syntax

```
config fcpolicy webfilter profile
    set override {yes | no}
    set peruser-status {enable | disable}
    set profile-name <name>
end
```

Variable	Description
<code>override {yes no}</code>	Select <code>yes</code> to enable modification of settings. Default: <code>no</code>
<code>peruser-status {enable disable}</code>	Enable or disable per-user web filtering. Default: <code>disable</code>
<code>profile-name <name></code>	Select the web filter profile to use. The profile must first be configured in webfilter profile .

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.

This chapter contains following sections:

add-vm-license	fcpolicy unit	fmpolicy
backup	fgfm reclaim-dev-tunnel	print-device-database
bootimage	fgt-cli-access	fmpolicy print-global-database
certificate ca	fmclient apply-lockdown	fmpolicy print-global-object
certificate local	fmclient client_license list	fmscript clean-sched
certificate local generate	fmclient client_license	fmscript delete
chassis	list_device	fmscript import
console baudrate	fmclient cluster	fmscript list
date	fmclient enterprise_license	fmscript run
device	download	fmscript showlog
device log clear	fmclient enterprise_license list	fmupdate {ftp scp tftp}
dmserver delrev	fmclient group refresh	import
dmserver revlist	fmclient group rename	fmupdate {ftp scp tftp}
dmserver showconfig	fmclient license_key deploy	export
dmserver showdev	fmclient license_key list	format disk
dmserver showrev	fmclient	ping
fcdevice addtomanaged	optimize-fcm-database	raid
fcdevice find-unit	fmclient package delete	reboot
fcdevice search	fmclient package deploy	reset
fcpolicy apply_to_members	fmclient package download	restore
fcpolicy deploy	fmclient package list	shutdown
fcpolicy grant unlicensed	fmclient refresh_ou	ssh
fcpolicy group	fmclient sync-ldap	time
fcpolicy retrieve	fmclient sync_ou_group	top
fcpolicy revoke unit	fmpolicy copy-global-object	traceroute
	fmpolicy install-config	

add-vm-license

Add a VMware license to the FortiManager.

Syntax

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

backup

Backup the FortiManager unit settings.

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 <ip> <filepath> <user> <password>
[crptpasswd]
```

Variable	Description
<ip>	Enter FTP server IP address.
<filepath>	Enter the file name for the backup and if required, enter the path to where the file will be backed up to on the backup server.
<user>	Enter username to use to log on the backup server.
<password>	Enter the password for the username on the backup server.
[crptpasswd]	Optionally, enter an encryption key (password) to encrypt data.

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

Related topics

- `restore`

bootimage

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

Syntax

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

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
```

Related topics

- [reboot](#)

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 | import} <cert_name> <tftp_ip>
```

where <cert_name> is the name of the certificate and <tftp_ip> is the IP address of the TFTP server.

Related commands

- [certificate local](#)

certificate local

Use these commands to list local certificates, and to import or export local certificates. To generate a certificate request, see [“certificate local generate” on page 164](#).

Syntax

To list the local certificates installed on the FortiManager unit:

```
execute certificate local list
```

To export or import local certificates:

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

where <cert_name> is the name of the certificate and <tftp_ip> is the IP address of the TFTP server.

Related commands

- `certificate local generate`
- `certificate ca`

certificate local generate

Use this command to generate a certificate request.

Syntax

```
execute certificate local generate <certificate-name_str> <subject>  
                                <number> [<optional_information>]
```

Variable	Description
<certificate-name_str>	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>	Enter 512, 1024, 1536 or 2048 for the size in bits of the encryption key.
<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 <code>optional_information</code> as required to further identify the unit. See “ Optional information variables ” for the list of 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 <code>organization_name_str</code> , you must first enter the <code>country_code_str</code> , <code>state_name_str</code> , and <code>city_name_str</code> . While entering optional variables, you can type? for help on the next required variable.

Optional information variables

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.
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiManager unit resides.

Variable	Description
<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 e-mail 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.

Related commands

- [certificate local](#)

chassis

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

Syntax

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

Variable	Description
<pw>	Replace the chassis password.



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

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.



You cannot change the console baud rate on the FortiManager 400 unit.

Example

Get the baudrate:

```
execute console baudrate
```

The response is like this:

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

Set the baudrate to 9600:

```
execute console baudrate 9600
```

date

Get or set the system date.

Syntax

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

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

- `mm` is the month and can be 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 2100

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

Dates entered will be validated - `mm` and `dd` require 2 digits, and `yyyy` requires 4 digits. Entering fewer digits will result in an error.

Example

This example sets the date to 17 September 2010:

```
execute date 09/17/2010
```

device

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

Syntax

```
execute device replace <name> <sn>
```

Variable	Description
<name>	The name of the device.
<sn>	The serial number of the new device.

devicelog clear

Use this command to clear a device log.

Syntax

```
execute devicelog clear <device>
```

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 <devicename>
```

Variable	Description
<devicename>	The name of the device.

dmserver showconfig

Use this command to show a specific configuration type and revision.
You cannot use this command with read-only permission.

Syntax

```
execute dmserver showconfig <devicename>
```

Variable	Description
<devicename>	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, the device name and the serial number.

Syntax

```
execute dmserver showdev
```

dmserver showrev

Use this command to display a device’s configuration revision.
You cannot use this command with read-only permission.

Syntax

```
execute dmserver showrev <devicename> <revision>
```

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

fcdevice addtomanaged

Use this command to add a FortiClient agent to the Managed Clients list from the Temporary Clients list. FortiClient Manager adds newly discovered FortiClient agents to the Temporary Clients list only if newclient_action is set to add-to-temp in fmclient discovery.

Syntax

```
execute fcdevice addtomanaged <host_name>
```

fcdevice find-unit

Use this command to find a unit.

Syntax

```
execute fcdevice find-unit <host_name | ip | uid>
```

fcdevice search

Use this command to discover FortiClient agents on the network.

Syntax

```
execute fcdevice search subnet {port1 | port2 | port3 | port4}
execute fcdevice search unicast <ip>
```

FortiClient Manager reports its search progress like this:

```
Searching...ip/mask:172.20.120.161/255.255.255.0
#####
1 FortiClient(s) found.
techdoc2 (172.20.120.54)
```

The IP/mask information is shown only for a subnet search.

fcpolicy apply_to_members

Use this command to apply group configuration to it's members.

Syntax

```
execute fcpolicy apply_to_members <module name> <include child
groups:1/0> <group name>
```

Variable	Description
<module>	Select the name from the list of available modules.
<include child groups:1/0>	Select 1 if you want to include the child groups. Select 0 is you do not want to include the child groups.
<group name>	Select the name of the group from the list.

fcpolicy deploy

Use this command to deploy the configuration changes to managed FortiClient agents and agent groups.

Syntax

```
execute fcpolicy deploy group <name>
execute fcpolicy deploy group_child <name>
execute fcpolicy deploy ungroup <host_name>
execute fcpolicy deploy unit <uid>
```

The `group` command deploys configuration changes to the specified FortiClient group.

The `group_child` command deploys configuration changes to the specified FortiClient group and its child groups.

The `ungroup` command deploys configuration changes to the specified ungrouped FortiClient agent.

The `unit` command deploys configuration changes to the specified FortiClient agent, whether it is in a group or not.

Related topics

- [fcpolicy retrieve](#)

fcpolicy grant unlicensed

Use this command to grant a license to a client that is in the Unlicensed Client list.

Syntax

```
execute fcpolicy grant unlicensed <uid>
```

where `<host_name>` is the unlicensed client's host name.

Related topics

- [fcpolicy revoke unit](#)

fcpolicy group

Use this command to select a FortiClient group for configuration.

Syntax

```
execute fcpolicy group <name>
```

If you do not specify `<group_name>`, the command reports the currently selected group.

Related topics

- [fcpolicy unit](#)

fcpolicy retrieve

Use this command to get the FortiClient configuration from the FortiClient agent and save it to the FortiManager database.

Syntax

```
execute fcpolicy retrieve group <name>
execute fcpolicy retrieve ungroup <host_name>
execute fcpolicy retrieve unit <uid>
```

The `group` command retrieves the configuration from a specified FortiClient group.

The `ungroup` command retrieves the configuration from a specified ungrouped FortiClient agent.

The `unit` command retrieves the configuration from a specified FortiClient agent, whether it is in a group or not.

Related topics

- [fcpolicy deploy](#)

fcpolicy revoke unit

Use this command to revoke a managed client's enterprise license key.

Syntax

```
execute fcpolicy revoke unit <uid>
```

Related topics

- [fcpolicy grant unlicensed](#)

fcpolicy unit

Use this command to select a FortiClient agent for configuration.

Syntax

```
execute fcpolicy unit <uid>
```

If you do not specify `<host_name>`, the command reports the currently selected FortiClient agent.

Related topics

- [fcpolicy group](#)

fgfm reclaim-dev-tunnel

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

Syntax

```
execute fgfm reclaim-dev-tunnel <devicename>
end
```

Variable	Description
<devicename>	Enter the device name.

fgt-cli-access

Connect to a CLI session on a FortiGate device attached to the FortiManager system. Disconnect using 'exit' to return to your original CLI session.

Syntax

```
execute fgt-cli-access <device_name> <username>
```

Variable	Description
<device_name>	Enter the device name from PDM, the IP address or FQDN hostname of the FortiGate device. By default it will try to match the PDM device name first.
<username>	Enter the username to use to log on the FortiGate device.

Example

This example shows how to connect to a FortiGate device called `Christmas` with an IP address of `172.20.120.151` using `admin` as the local user with no password:

```
FMG3000 # execute fgt-cli-access 172.20.120.151 admin
Christmas #
```

Related topics

- [ssh](#)

fmclient apply-lockdown

Use this command to apply FortiClient lockdown settings to all, or selected, managed FortiClient units.

Syntax

```
execute fmclient apply-lockdown all <enable|disable>
execute fmclient apply-lockdown group <name>
```

```
execute fmclient apply-lockdown unit <uid>
```

Variable	Description
all <enable disable>	Apply lockdown settings to all clients.
group <name>	Apply lockdown settings to client(s) in a group and its child group(s).
unit <uid>	Apply lockdown settings to a client.

fmclient client_license list

Use this command to list the FortiClient agent enterprise client licenses configured on the FortiManager unit.

Syntax

```
execute fmclient client_license list
```

The command output lists the following information:

- Name
- Client License
- Seats Permitted
- Seats in Use
- Expiry Date
- Group ID
- Last Update
- Status
- Comment

Related Topics

- [fmclient client_license list_device](#)

fmclient client_license list_device

Use this command to list the clients using a specified client license.

Syntax

```
execute fmclient client_license list_device <client_license_key>
```

Related Topics

- [fmclient client_license list](#)
- [fmclient enterprise_license list](#)

fmclient cluster

Use this command to control FortiClient Manager clustering.

Syntax

```
execute fmclient cluster [start | stop | status]
```

Variable	Description
start	Start clustered operation.
stop	End clustered operation.
status	Show clustering status. On primary unit, lists secondary units by serial number and IP address. On secondary unit, shows whether unit is connected to primary.

fmclient enterprise_license download

Use this command to download the FortiClient enterprise license from Customer Service & Support. You need the license key.

Syntax

```
execute fmclient enterprise_license download license_key  
<enterprise_license_key>
```

fmclient enterprise_license list

Use this command to view information about the FortiClient enterprise license configured on the FortiManager unit.

Syntax

```
execute fmclient enterprise_license list
```

The command output lists the following information:

- License Key
- Type
- Expiry Date
- Seats Permitted

fmclient group refresh

Refresh dynamic FortiClient agent group membership.

Syntax

```
execute fmclient group refresh
```

fmclient group rename

Rename a FortiClient agent group.

Syntax

```
execute fmclient group rename <group name> <new group name>
end
```

Variable	Description
<group name>	Enter the current name of the group.
<new group name>	Enter the new name of the group.

fmclient license_key deploy

Use this command to deploy license keys to FortiClient agents. You can deploy all license keys or a single license key.

Syntax

```
execute fmclient license_key deploy {all | license_key <license_key>}
```

Use the command `config fmclient license_key` to enter license keys and associate them with client groups.

fmclient license_key list

Use this command to list FortiClient license keys. You can deploy all license keys or a single license key. This command applies to standard fixed licenses, not to enterprise client licenses.

Syntax

```
execute fmclient license_key list
```

The command output lists the following information:

- License Key
- Comment
- Assigned Group(s)

fmclient optimize-fcm-database

Use this command to enable or disable FortiClient Manager database optimization.

Syntax

```
execute fmclient optimize-fcm-database {enable | disable}
```

fmclient package delete

Use this command to delete unneeded FortiClient upgrade packages.

Syntax

```
execute fmclient package delete <package_id>
```

Use the `fmclient package list` command to determine the value of `<package_id>`.

Related commands

- `fmclient package list`
- `fmclient package download`

fmclient package deploy

Use this command to deploy upgrade packages to FortiClient agents.

Syntax

```
execute fmclient package deploy all <package_version_id>
execute fmclient package deploy group <group_name>
    <package_version_id>
execute fmclient package deploy unit <host_name> <package_version_id>
```

Use the `fmclient package list` command to determine the value of `<package_version_id>`.

Use the `get` and `get` commands to obtain group names and unit host names.

Related commands

- `fmclient package list`
- `fmclient package download`

fmclient package download

Use this command to download FortiClient software upgrade packages to the FortiManager unit.

Syntax

```
execute fmclient package download <package_id>
```

Use the `fmclient package list` command to determine the value of `<package_id>`.

Related commands

- `fmclient package list`
- `fmclient package deploy`

fmclient package list

Use this command to list the FortiClient software packages available for download or deployment.

Syntax

```
execute fmclient package list
```

The command output lists the following information:

- ID
- Version
- Platform
- Date
- Status
- Description

fmclient refresh_ou

Use this command to refresh the Organizational Units (OUs) on the LDAP server.

Syntax

```
execute fmclient refresh_ou ldap_name <ldap_name>
```

fmclient sync-ldap

Use this command to synchronize the Windows AD group and user information with the LDAP server.

Syntax

```
execute fmclient sync-ldap <ldap_name>
```

fmclient sync_ou_group

Use this command to synchronize the Organizational Units (OUs) group to an ou_grouping on an Active Directory (AD) server.

Syntax

```
execute fmclient sync_ou_group ad_ou_grouping <ad_ou_grouping name>
```

Example

The following example show the command to sync an ou_group with an ou_grouping called QA_Nan on a AD server.

```
FMG3000B # execute fmclient sync_ou_group ad_ou_grouping QA_Nan
ldap host: 172.16.96.146, port: 389, base dn: dc=ad864,dc=com, bind
dn: cn=Administrator,cn=Users,dc=ad864,dc=com
synchronizing.....
```

fmpolicy copy-global-object

Use this command to set the policy to copy a global object.

Syntax

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

Variable	Description
<adom>	Enter the name of the ADOM.
<category>	Enter the name of the category in the ADOM.
<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> <devid> <revname>
end
```

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

fmpolicy print-device-database

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

Syntax

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

fmpolicy print-global-database

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

Syntax

```
execute fmpolicy print-global-database <adom_name> <ouput_filename>
```

fmpolicy print-global-object

Use this command to display the global object for an ADOM.

Syntax

```
execute fmpolicy print-global-object <adom> <category> <output>
end
```

Variable	Description
<adom>	Enter the name of the ADOM.
<category>	Enter the category of the ADOM.
<output>	Output file name.

fmscript clean-sched

Clean the script schedule table.

Syntax

```
execute fmscript clean-sched
```

fmscript delete

Delete a script.

Syntax

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

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

fmscript import

Import a script from an FTP server.

Syntax

```
execute fmscript import <ftpserver_ipv4> <filename> <username>  
                        <password> <scriptname> <scripttype> <comment> <adom_name>  
                        <os_type> <os_version> <platform> <devicename> <buildno>  
                        <hostname> <serialno>
```

Variable	Description
<ftpserver_ipv4>	The IP 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.
<adom_name>	Name of the administrative domain.
<os_type>	The operating system type, such as FortiOS. Options include any, FortiOS, FortiMail, and others.
<os_version>	The operating system version, such as FortiOS. Options include any, 300, and 400.
<platform>	The hardware platform this script can be run on. Options include any, or the model of the device such as Fortigate-60.
<devicename>	The device name to run this script on. Options include any, or the specific device name as it is displayed on the FortiManager system

Variable	Description
<buildno>	The specific build number this script can be run on. Options include any, 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 any or the specific host name.
<serialno>	The serial number of the device this script can be run on. Options include <i>any</i> or the specific serial number of the device, such as FGT5002803033042.

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.

```
FMG400A # 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
```

Related topics

- `fmscript import`
- `fmscript run`

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 <scriptid_int> <run_on> <devname> <adomname>
```

Variable	Description
<scriptid_int>	The ID number of the script to run.

Variable	Description
<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 • globaldb - on the global database
<devname>	Enter the device name to run the script on. This is required if device or devicedb were chosen for where to run the script.
<adomname>	Name of the administrative domain.

Related topics

- `fmscript import`
- `fmscript list`

fmscript showlog

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

Syntax

```
execute fmscript showlog <devicename>
```

Variable	Description
<devicename>	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.

```
FMG400A # 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
set subnet 33.33.33.0 255.255.255.0
  end
end
Running script(xml_script1) on DB success
cdb_find_entry_by_canon,52:parent=1,category=2,key=(null)
```

Related topics

- `fmscript run`

fmupdate {ftp | scp | tftp} import

You can import packages using the ftp, scp, or tftp servers.

Syntax

```
execute fmupdate {ftp | scp | tftp} import <type> <remote_file> <ip>  
                <port> <remote_path> <user> <password>
```

Variable	Description
{ftp scp tftp}	Select FTP, scp, or TFTP as the file transfer protocol to use.
<type>	Select the type of file to export or import. Options include: av-ips, fct-av, url, spam, license-fgt, license-fct, custom-url, domp
<remote_file>	Update manager packet file name on the server or host.
<ip>	Enter the FQDN or the IP Address of the server.
<port>	Enter the port to connect to on the remote SCP host.
<remote_path>	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.
<user>	Enter the user name to log into the FTP server or SCP host
<password>	Enter the password to log into the FTP server or SCP host

fmupdate {ftp | scp | tftp} export

You can export packages using the ftp, scp, or tftp servers.

Syntax

```
execute fmupdate {ftp | scp | tftp} export <type> <remote_file> <ip>  
                <port> <remote_path> <user> <password>
```

Variable	Description
{ftp scp tftp}	Select FTP, scp, or TFTP as the file transfer protocol to use.
<type>	Select the type of file to export or import. Options include: url, spam, license-package, license-info-in-xml, custom-url, domp
<remote_file>	Update manager packet file name on the server or host.
<ip>	Enter the FQDN or the IP Address of the server.
<port>	Enter the port to connect to on the remote SCP host.
<remote_path>	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.

Variable	Description
<user>	Enter the user name to log into the FTP server or SCP host
<password>	Enter the password to log into the FTP server or SCP host

format disk

Format the hard disk on the FortiManager system. If RAID is configured, change the variable disk-ext4 with <Raid Level>.

Syntax

```
execute format disk
```

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. FortiManager's IP address, and routing information will be preserved.

Variable	Description
<disk>	Format hard disk.
<disk-ext4	Format hard disk (ext4).
<disk_partition_2>	Format hard disk partition 2 (static)
<disk_partition_2-ext4	Format hard disk partition 2 (static) with ext4
<disk_partition_3>	Format hard disk partition 3 (dynamic)
<disk_partition_3-ext4	Format hard disk partition 3 (dynamic) with ext4
<disk_partition_4	Format hard disk partition 4 (misc)
<disk_partition_4-ext4	Format hard disk partition 4 (misc) with ext4

Related topics

- [restore](#)

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>	IP address of network device to contact.
<hostname>	DNS resolvable hostname of network device to contact.

Example

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

```
execute ping 192.168.1.23
```

Related topics

- `traceroute`

raid

This command allows you to add, delete and rebuild ecc.

Syntax

```
execute raid
  execute add-disk <integer>
  execute delete-disk <integer>
  execute rebuild-ecc {enable | disable}
end
```

Variable	Description
add-disk <integer>	Enables you to add a disk and giving it a number.
delete-disk <integer>	Enables you to delete the selected disk.
rebuild-ecc {enable disable}	Enables you to build the ecc table.

Example

The following example shows that disk 5 is added, disk 2 is deleted and rebuild-ecc is enabled.

```
execute raid
  execute add-disk 5
  execute delete-disk 2
  execute rebuild-ecc enable
end
```

reboot

Restart the FortiManager system.

This command will disconnect all sessions on the FortiManager system.

Syntax

```
execute reboot
```

Related topics

- `reset`
- `restore`
- `shutdown`

reset

Use this command to reset the FortiManager unit to factory defaults.

This command will disconnect all sessions and restart the FortiManager unit.

Syntax

```
execute reset all-settings
execute reset partition <partition>
```

Related topics

- `restore`
- `shutdown`

restore

Use this command to:

- restore the configuration or database from a file
- change the FortiManager unit image

This command will disconnect all sessions and restart the FortiManager unit

Syntax

```
execute restore all-settings <ip> <string> <username> <password>
    <crptpasswd> [option1+option2+...]
execute restore image {ftp | tftp} <filepath> <ip> <username>
    <password>
```

Variable	Description
all-settings	Restore all FortiManager settings from a file on a TFTP server. The new settings replace the existing settings, including administrator accounts and passwords.

Variable	Description
image	Upload a firmware image from a TFTP server to the FortiManager unit. The FortiManager unit reboots, loading the new firmware.
{ftp tftp}	Enter the type of server to retrieve the image from.
<filepath>	The file to get from the server. You can enter a path with the filename, if required.
<ip>	IP address of the server to get the file from.
<string>	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 FTP server. This option is not available for restore operations from TFTP servers.
<password>	The password for username on the FTP server. This option is not available for restore operations from TFTP servers.
<crptpasswd>	Optional password to protect backup content. Use <code>any</code> for no password.
[option1+option2+...]	Select whether to keep IP, routing, and HA info on the original unit.

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
```

shutdown

Shut down the FortiManager system.

This command will disconnect all sessions.

Syntax

```
execute shutdown
```

Related topics

- `reboot`

ssh

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

Syntax

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

<destination> - the IP or FQ DNS resolvable hostname of the system you are connecting to

<username> - the user name to use to log on to the remote system

To leave the ssh session type `exit`.

To confirm you are connected or disconnected from the ssh session, verify the command prompt has changed.

Related topics

- [fgt-cli-access](#)

time

Get or set the system time.

Syntax

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

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

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

All parts of the time are required. Single digits are allowed for each of `hh`, `mm`, and `ss`.

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
```

To exit the display, type `q`. Other interactive commands are available while running `top`. For help on them, type `h`.

Example

The execute top command displays the following information:

```
top_bin - 04:30:11 up 5 days,  1:13,  0 users,  load average: 0.46,
              0.52, 0.50
Tasks: 108 total, 2 running, 106 sleeping, 0 stopped, 0 zombie
Cpu(s): 3.4%us, 1.2%sy, 0.0%ni, 95.2%id, 0.0%wa, 0.0%hi,  0.2%si,
              0.0%st
Mem: 515376k total, 508204k used, 7172k free, 4828k buffers
Swap: 1563944k total, 4956k used, 1558988k free, 124904k cached
PID USER      PR  NI  VIRT  RES  SHR  S %CPU  %MEM    TIME+  COMMAND
189 root        20   0 136m 105m 4428 R  0.5 20.9 23:20.59 dmserver
199 root        39  19 17368 5560 2316 S  0.2  1.1  1:02.31 cpumemond
207 root        20   0 1584  508  424 S  0.2  0.1   0:00.50 webconsole
221 root        20   0 10504 4048 1864 S  0.2  0.8 11:07.38 udm_statd
2387 root        20   0 2072  920  708 R  0.2  0.2   0:00.07 top_bin
1 root         20   0 135m 105m 5168 S  0.0 21.0   0:11.94
      initXXXXXXXXXX
2 root        20   0    0    0    0 S  0.0  0.0   0:00.00 kthreadd
3 root        20   0    0    0    0 S  0.0  0.0   0:00.13 ksoftirqd/0
4 root        20   0    0    0    0 S  0.0  0.0   0:00.11 kworker/0:0
5 root        20   0    0    0    0 S  0.0  0.0   0:05.78 kworker/u:0
6 root        RT   0    0    0    0 S  0.0  0.0   0:00.00 migration/0
7 root         0 -20    0    0    0 S  0.0  0.0   0:00.00 khelper
8 root         0 -20    0    0    0 S  0.0  0.0   0:00.01 pm
9 root        20   0    0    0    0 S  0.0  0.0   0:00.68 sync_supers
10 root        20   0    0    0    0 S  0.0  0.0   0:00.01 bdi-default
11 root         0 -20    0    0    0 S  0.0  0.0   0:00.00 kintegrityd
```

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 {<ip> | <host>}
```

Variable	Description
<ip>	IP address of network device.
<host>	FQDN hostname of network device.

Example

This example shows how trace the route to a host with the IP address 192.168.1.23:

```
execute traceroute 192.168.1.23
```

diagnose

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

This chapter describes the following `diagnose` commands:

<code>cdb check</code>	<code>dvm proc</code>	<code>fmsystem ntp</code>
<code>debug application</code>	<code>dvm task</code>	<code>fmsystem print</code>
<code>debug cli</code>	<code>dvm transaction-flag</code>	<code>fmsystem process</code>
<code>debug crashlog</code>	<code>fgfm</code>	<code>fmsystem raid</code>
<code>debug disable</code>	<code>fmclient cache</code>	<code>fmsystem route</code>
<code>debug dpm</code>	<code>fmclient data</code>	<code>fmsystem server</code>
<code>debug enable</code>	<code>fmclient eventlog</code>	<code>fmupdate</code>
<code>debug info</code>	<code>fmclient log</code>	<code>fwmanager</code>
<code>debug sysinfo</code>	<code>fmclient performance</code>	<code>ha</code>
<code>debug timestamp</code>	<code>fmnetwork arp</code>	<code>hardware</code>
<code>debug vminfo</code>	<code>fmnetwork interface</code>	<code>rtm</code>
<code>dvm adom</code>	<code>fmnetwork netstat</code>	<code>sniffer</code>
<code>dvm check-integrity</code>	<code>fmsystem admin-session</code>	<code>test application</code>
<code>dvm debug</code>	<code>fmsystem disk</code>	<code>test deploymanager</code>
<code>dvm device</code>	<code>fmsystem export</code>	<code>test policy-check</code>
<code>dvm device-tree-update</code>	<code>fmsystem flash</code>	<code>test search</code>
<code>dvm group</code>	<code>fmsystem fsck</code>	<code>test sftp</code>
<code>dvm lock</code>	<code>fmsystem logtoconsole</code>	<code>test sysalert</code>

cdb check

Use this command to check the object configuration database integrity, the global policy assignment table, and repair configuration database.

Syntax

```
diagnose cdb check objcfg-integrity
diagnose cdb check policy-assignment
```

Variable	Description
<code>objcfg-integrity</code>	Check object config database integrity.
<code>policy-assignment</code>	Check the global policy assignment table.

debug application

Use this command to set the debug levels for the FortiManager applications.

Syntax

```
diagnose debug application alertmail <integer>
diagnose debug application ddmd <integer>
diagnose debug application depmanager <integer>
diagnose debug application dmapl <integer>
diagnose debug application faz-fortilogd <integer>
diagnose debug application faz-logfiled <integer>
diagnose debug application faz-oftpd <integer>
diagnose debug application fgdsrv <integer>
diagnose debug application fgdupd <integer>
diagnose debug application fgfmsd <integer>
diagnose debug application fnbam <integer>
diagnose debug application fortimanager <integer>
diagnose debug application gui <integer>
diagnose debug application ha <integer>
diagnose debug application ike <integer>
diagnose debug application localmod <integer>
diagnose debug application logd <integer>
diagnose debug application lrm <integer>
diagnose debug application ntpd <integer>
diagnose debug application ptmgr <integer>
diagnose debug application ptsessionmgr <integer>
diagnose debug application rtmd <integer>
diagnose debug application securityconsole <integer>
diagnose debug application snmpd <integer>
diagnose debug application sql_dashboard_rpt <integer>
diagnose debug application sql-integration <integer>
diagnose debug application sqlplugind <integer>
diagnose debug application sqlrptcached <integer>
diagnose debug application srchd <integer>
diagnose debug application ssh <integer>
diagnose debug application storaged <integer>
diagnose debug application uploadd <integer>
```

Variable	Description
alertmail <integer>	Set the debug level of the alert email daemon. Default: 0
ddmd <integer>	Set the debug level of the dynamic data monster. Default: 0
depmanager <integer>	Set the debug level of the deployment manager. Default: 0

Variable	Description
<code>dmapi <integer></code>	Set the debug level of the dmapi. Default: 0
<code>faz-fortilogd <integer></code>	Set the debug level of the fortilogd daemon. Default: 0
<code>faz-logfiled <integer></code>	Set the debug level of the logfiled daemon. Default: 0
<code>faz-oftpd <integer></code>	Set the debug level of the oftpd daemon. Default: 0
<code>fgdsvr <integer></code>	Set the debug level of the FortiGuard query daemon. Default: 0
<code>fgdupd <integer></code>	Set the debug level of the FortiGuard update daemon. Default: 0
<code>fgfmsd <integer></code>	Set the debug level of FGFM daemon. Default: 0
<code>fnbam <integer></code>	Set the debug level of the Fortinet authentication module. Default: 0
<code>fortimanager <integer></code>	Set the debug level of the FortiManager Web Service. Default: 0
<code>gui <integer></code>	Set the debug level of the Web-based Manager. Default: 0
<code>ha <integer></code>	Set the debug level of high availability daemon. Default: 0
<code>ike <integer></code>	Set the debug level of the IKE daemon. Default: 0
<code>localmod <integer></code>	Set the debug level of the localmod daemon. Default: 0
<code>logd <integer></code>	Set the debug level of the log daemon. Default: 0
<code>lrm <integer></code>	Set the debug level of the Log and Report Manager. Default: 0
<code>ntpd <integer></code>	Set the debug level of the Network Time Protocol (NTP) daemon. Default: 0

Variable	Description
ptmgr <integer>	Set the debug level of the Portal Manager. Default: 0
ptsessionmgr <integer>	Set the debug level of the Portal Session Manager. Default: 0
rtmd <integer>	Set the debug level of the real-time monitor. Default: 0
securityconsole <integer>	Set the debug level of the security console daemon. Default: 0
snmpd <integer>	Set the debug level of the SNMP daemon from 0-8. Default: 0
sql_dashboard_rpt <integer>	Set the debug level of the SQL dashboard report daemon. Default: 0
sql-integration <integer>	Set the debug level of SQL applications. Default: 0
sqlplugind <integer>	Set the debug level of the SQL plugin daemon. Default: 0
sqlrptcached <integer>	Set the debug level of the SQL report caching daemon. Default: 0
srchd <integer>	Set the debug level of the SRCHD. Default: 0
ssh <integer>	Set the debug level of SSH protocol transactions. Default: 0
storaged <integer>	Set the debug level of communication with java clients. Default: 0
uploadd <integer>	Set the debug level of the upload daemon. Default: 0

Example

This example shows how to set the debug level to 7 for the upload daemon:

```
diagnose debug application uploadd 7
```

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <level_int>
```

Variable	Description
<level_int>	Set the debug level of the CLI from 0-8. Default: 3

Example

This example shows how to set the CLI debug level to 5:

```
diagnose debug cli 5
```

debug crashlog

Use this command to manage crash logs.

Syntax

```
diagnose debug crashlog clear
```

Variable	Description
clear	Delete backtrace and core files.

debug disable

Use this command to disable debug mode.

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 a DPM to FortiGate communication trace.
conf-trace {enable disable status}	Enable a DPM to FortiGate configuration trace.
probe-device <ip>	Check device status.

Example

This example shows how to enable a communication trace between the DPM and a FortiGate:

```
diagnose debug dpm comm-trace enable
```

debug enable

Use this command to enable debug.

Syntax

```
diagnose debug enable
```

debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

debug sysinfo

Use this command to show system information.

Syntax

```
diagnose debug sysinfo
```

debug timestamp

Use this command to enable or disable debug timestamp.

Syntax

```
diagnose debug timestamp {enable | disable}
```

debug vminfo

Use this command to show VMware license information.

Syntax

```
diagnose debug vminfo
```

Example

Here is an example of the output from `diagnose debug vminfo`:

```
ValidLicense Type: Basic
Table size:
Maximum dev: 10
```

dvm adom

Use this command to list ADOMs.

Syntax

```
diagnose dvm adom list
```

Variable	Description
list	List ADOMs.

dvm check-integrity

Use this command to check the DVM database integrity.

Syntax

```
diagnose dvm check-integrity
```

Example

Here is an example of the output from `diagnose dvm check-integrity`:

```
[1/9] Checking object memberships      ... correct
[2/9] Checking device nodes           ... correct
[3/9] Checking device vdoms           ... correct
[4/9] Checking device ADOM memberships ... correct
[5/9] Checking devices being deleted  ... correct
[6/9] Checking groups                 ... correct
[7/9] Checking group membership       ... correct
[8/9] Checking device locks           ... correct
[9/9] Checking task database          ... correct
Checking Configuration DB ...correct
```

dvm debug

Use this command to enable or disable debug channels.

Syntax

```
diagnose dvm debug {enable | disable}
```

dvm device

Use this command to list devices or objects referencing a device.

Syntax

```
diagnose dvm device deps <device>
diagnose dvm device list
```

Variable	Description
deps <device>	List objects referencing a device.
list	List devices.

dvm device-tree-update

Use this command to enable or disable device tree automatic updates.

Syntax

```
diagnose dvm device-tree-update {enable | disable}
```

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
```

Example

Here is an example of the output from `diagnose dvm lock`:

```
DVM lock state = unlocked
Global database pending read: unlocked
Global database pending write: unlocked
Global database reserved read: unlocked
Global database reserved write: unlocked
Global database shared read: unlocked
Global database shared write: unlocked
```

dvm proc

Use this command to list DVM processes.

Syntax

```
diagnose dvm proc list
```

Variable	Description
<code>list</code>	List processes.

dvm task

Use this command to repair or reset the task database.

Syntax

```
diagnose dvm task repair
diagnose dvm task reset
```

Variable	Description
<code>repair</code>	Repair the task database while preserving existing data where possible. The FortiManager will reboot after the repairs.
<code>reset</code>	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 transaction-flag

Use this command to edit or display DVM transaction flags.

Syntax

```
diagnose dvm transaction-flag {abort | debug | none}
```

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
```

Variable	Description
install-session	Get installations session lists.
object-list	Get object lists.
session-list	Get session lists.

fmclient cache

Use this command to diagnose the FortiClient cache.

Syntax

```
diagnose fmclient cache clear
diagnose fmclient cache find <uid>
diagnose fmclient cache list
diagnose fmclient cache sync
```

Variable	Description
clear	Clear the cache.
find <uid>	Find a FortiClient in the cache using its UID.
list	List the contents of the cache.
sync	Synchronize the cache content with the database.

Example

Here is an example of the output from `diagnose fmclient cache list`:

```
Capacity:300000
Count:0
Unordered item count:0
Last sync to db:19:25:31
Last reorder time:19:25:31
```

fmclient data

Use this command to diagnose FortiClient management data.

Syntax

```
diagnose fmclient data export <ftp server> <user> <password> [remote  
path] [remote filename]  
diagnose fmclient data export_client_list <ftp server> <user>  
<password> [remote path] [remote filename]  
diagnose fmclient data import <ftp server> <user> <password>  
[remote path] [remote filename]  
diagnose fmclient data import_v3 <ftp server> <user> <password>  
[remote path] [remote filename]  
diagnose fmclient data reset  
diagnose fmclient data restore_auto_backup  
diagnose fmclient data vacuum  
diagnose fmclient data view_allow_update_fcts
```

Variable	Description
export <ftp server> <user> <password> [remote path] [remote filename]	Dump the database and export the data file.
export_client_list <ftp server> <user> <password> [remote path] [remote filename]	Export the client list to a .csv file.
import <ftp server> <user> <password> [remote path] [remote filename]	Create a database and import the data file.
import_v3 <ftp server> <user> <password> [remote path] [remote filename]	Create a database and import the v3 data file.
reset	Reset the database, then reboot the system.
restore_auto_backup	Everyday, FortiClient Manager databases are automatically backed up. Use this command to restore the latest backed up databases. The system will then reboot.
vacuum	Vacuum the database.
view_allow_update_fcts	View the allow update FortiClients.

fmclient eventlog

Use this command to switch FortiClient Manager event logging.

Syntax

```
diagnose fmclient eventlog get
diagnose fmclient eventlog set {on | off}
```

Variable	Description
get	Show the current event logging status.
set {on off}	Turn event logging on or off.

fmclient log

Use this command to diagnose the FortiClient Manager log.

Syntax

```
diagnose fmclient log export <server> <user> <password> [remote path]
                             [remote filename]
diagnose fmclient log level <integer>
diagnose fmclient log monitor
diagnose fmclient log print
```

Variable	Description
export <server> <user> <password> [remote path] [remote filename]	Export the log.
level <integer>	Get or set the log level: <ul style="list-style-type: none">• 0 - error• 1 - information• 2 - debug
monitor	Monitor the log.
print	Print the current log contents.

fmclient performance

Use this command to diagnose FortiClient cache.

Syntax

```
diagnose fmclient performance monitor
diagnose fmclient performance timing <integer>
```

Variable	Description
monitor	Monitor the statistics of processes timing. Press <code>q</code> to stop.
timing <integer>	Enable or disable CPU usage timing for processes. <ul style="list-style-type: none">• 0 - disable• 1 - enable

Example

Here is an example of enabling CPU usage timing:

```
diagnose fmclient performance timing 1
```

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
```

Variable	Description
detail <portX>	View a specific interface's details.
list	List all interface details.

Example

Here is an example of the output from `diagnose fmnetwork interface detail port1`:

```
Status: up
Speed  1000Mb/s :
Duplex  : Full
```

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
<code>list [-r]</code>	List all connections, or use -r to list only resolved IP addresses.
<code>tcp [-r]</code>	List all TCP connections, or use -r to list only resolved IP addresses.
<code>udp [-r]</code>	List all UDP connections, or use -r to list only resolved IP addresses.

Example

Here is an example of the output from `diagnose fmnetwork netstat tcp -r`:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 FMG-VM:9090            *:*                      LISTEN
tcp      0      0 *:6020                  *:*                      LISTEN
tcp      0      0 *:8900                   *:*                      LISTEN
tcp      0      0 *:8901                   *:*                      LISTEN
tcp      0      0 *:8080                   *:*                      LISTEN
tcp      0      0 *:22                     *:*                      LISTEN
tcp      0      0 *:telnet                 *:*                      LISTEN
tcp      0      0 *:8890                   *:*                      LISTEN
tcp      0      0 *:8891                   *:*                      LISTEN
tcp      0      0 *:541                    *:*                      LISTEN
```

fmsystem admin-session

Use this command to view login session information.

Syntax

```
diagnose fmsystem admin-session list
diagnose fmsystem admin-session status
```

Variable	Description
list	List login sessions.
status	Show the current session.

Example

Here is an example of the output from `diagnose fmsystem admin-session status`:

```
session_id: 31521 (seq: 4)
username: admin
admin template: admin
from: jsconsole(10.2.0.250)
profile: Super_User (type 3)
adom: root
session length: 198 (seconds)
```

fmsystem disk

Use this command to view disk diagnostic information.

Syntax

```
diagnose fmsystem disk smart
diagnose fmsystem disk status
diagnose fmsystem disk test
diagnose fmsystem disk usage
```

Variable	Description
smart	Show the disk SMART information.
status	Show the disk power status.
test	Test the disk power saving capability. This power management test will be inaccurate if there is a high system load or if there is other log disk activity. This test will take 20-50 seconds.
usage	Show the disk usage.

fmsystem export

Use this command to export logs.

Syntax

```
diagnose fmsystem export crashlog <server> <user> <password> [remote  
path] [filename]  
diagnose fmsystem export dminstallog <devid> <server> <user>  
<password> [remote path] [filename]  
diagnose fmsystem export umlog {ftp | sftp} <type> <server> <user>  
<password> [remote path] [filename]  
diagnose fmsystem export upgradelog <ftp server>
```

Variable	Description
crashlog <server> <user> <password> [remote path] [filename]	Export the crash log.
dminstallog <devid> <server> <user> <password> [remote path] [filename]	Export deployment manager install log.
umlog {ftp sftp} <type> <server> <user> <password> [remote path] [filename]	Export the update manager and firmware manager log files. The type option are: fdslinkd, fctlinkd, fgdlinkd, usvr, update, service, misc, umad, fwmlinkd
upgradelog <ftp server>	Export the upgrade error log.

fmsystem flash

Use this command to diagnose the flash memory.

Syntax

```
diagnose fmsystem flash list
```

Variable	Description
list	List flash images.

fmsystem fsck

Use this command to check and repair the filesystem.

Syntax

```
diagnose fmsystem fsck harddisk
```

Variable	Description
harddisk	Check and repair the file system, then reboot the system.

fmsystem logtoconsole

Use this command to enable or disable printing the log to the console.

Syntax

```
diagnose fmsystem logtoconsole {disable | enable}
```

fmsystem ntp

Use this command to list NTP server information.

Syntax

```
diagnose fmsystem ntp status
```

Variable	Description
status	List NTP servers' information.

fmsystem print

Use this command to print server information.

Syntax

```
diagnose fmsystem print certificate
diagnose fmsystem print cpuinfo
diagnose fmsystem print df
diagnose fmsystem print hosts
diagnose fmsystem print interface <interface>
diagnose fmsystem print loadavg
diagnose fmsystem print netstat
diagnose fmsystem print partitions
diagnose fmsystem print route
diagnose fmsystem print rtcache
diagnose fmsystem print slabinfo
diagnose fmsystem print sockets
diagnose fmsystem print uptime
```

Variable	Description
certificate	Print the IPsec certificate.
cpuinfo	Print the CPU information.
df	Print the file system disk space usage.
hosts	Print the static table lookup for host names.
interface <interface>	Print the information of the interface

Variable	Description
loadavg	Print the average load of the system.
netstat	Print the network statistics.
partitions	Print the partition information of the system.
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.

Example

Here is an example of the output from `diagnose fmsystem print df`:

```

Filesystem            1K-blocks      Used Available Use% Mounted on
none                   65536           0      65536    0% /dev/shm
none                   65536          20      65516    1% /tmp
/dev/sda1              47595      28965      16173   65% /data
/dev/sdb3              9803784    723128    8582652    8% /var
/dev/sdb2             61927420   224212   58557480    1% /var/static
/dev/sdb4              9803784    132164    9173616    2% /var/misc
/dev/sdb4              9803784    132164    9173616    2% /drive0
/dev/sdb4              9803784    132164    9173616    2% /Storage
/dev/loop0              9911        1043       8356   12%
/var/dm/tcl-root

```

fmsystem process

Use this command to view and kill processes.

Syntax

```

diagnose fmsystem process kill -<signal> <pid>
diagnose fmsystem process killall <module>
diagnose fmsystem process list

```

Variable	Description
kill -<signal> <pid>	Kill a process.
killall <module>	Kill all the related processes.
list	List all processes.

fmsystem raid

Use this command to diagnose RAID.

Syntax

diagnose fmsystem raid `alarms`

diagnose fmsystem raid `hwinfo`

diagnose fmsystem raid `status`

Variable	Description
<code>alarms</code>	Show RAID alarm logs.
<code>hwinfo</code>	Show RAID controller hardware information.
<code>status</code>	Show RAID status information.

fmsystem route

Use this command to diagnose routes.

Syntax

diagnose fmsystem route `list`

Variable	Description
<code>list</code>	List all routes.

Example

Here is an example of the output from `diagnose fmsystem route list`:

```
DestinationGatewayGenmask Flags Metric Ref Use Iface
10.2.0.0*255.255.0.0U000port1
169.254.0.0*255.255.0.0U000svr_fgfm
169.254.0.0* 255.255.0.0U000svr_fgfm
```

fmsystem server

Use this command to start the FortiManager server.

Syntax

diagnose fmsystem server `start`

Variable	Description
<code>start</code>	Start the server.

fmupdate

Use this command to diagnose update services.

Syntax

```
diagnose fmupdate add-device <serial> <ip> <firmware> <build>
diagnose fmupdate deldevice {fct | fds | fgd | fgc} <serial> <uid>
diagnose fmupdate faz-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fct-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fct-configure
diagnose fmupdate fct-dbcontract
diagnose fmupdate fct-delservicelist
diagnose fmupdate fct-getobject
diagnose fmupdate fct-log
diagnose fmupdate fct-restart
diagnose fmupdate fct-serverlist
diagnose fmupdate fct-update-status
diagnose fmupdate fct-updatenow
diagnose fmupdate fds-configure
diagnose fmupdate fds-dbcontract
diagnose fmupdate fds-delservicelist
diagnose fmupdate fds-dump-breg
diagnose fmupdate fds-dump-srul
diagnose fmupdate fds-get-downstream-device
diagnose fmupdate fds-getobject
diagnose fmupdate fds-log
diagnose fmupdate fds-restart
diagnose fmupdate fds-serverlist
diagnose fmupdate fds-service-info
diagnose fmupdate fds-update-status
diagnose fmupdate fds-updatenow
diagnose fmupdate fgc-configure
diagnose fmupdate fgc-delservicelist
diagnose fmupdate fgc-log
diagnose fmupdate fgc-restart
diagnose fmupdate fgc-serverlist
diagnose fmupdate fgc-update-status
diagnose fmupdate fgd-asdbver
diagnose fmupdate fgd-asdevice_stat {10m | 30m | 1h | 6h | 12h | 24h
| 7d}
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-configure
diagnose fmupdate fgd-dbcontract
diagnose fmupdate fgd-delasdb
diagnose fmupdate fgd-delavdb
diagnose fmupdate fgd-delservicelist
```

```

diagnose fmupdate fgd-delwfdb
diagnose fmupdate fgd-get-downstream-device
diagnose fmupdate fgd-log
diagnose fmupdate fgd-restart
diagnose fmupdate fgd-serverlist
diagnose fmupdate fgd-service-info
diagnose fmupdate fgd-update-status
diagnose fmupdate fgd-updatenow
diagnose fmupdate fgd-url-rating <string>
diagnose fmupdate fgd-wfas-log
diagnose fmupdate fgd-wfas-rate
diagnose fmupdate fgd-wfdbver
diagnose fmupdate fgd-wfdevice_stat {10m | 30m | 1h | 6h | 12h | 24h
| 7d}
diagnose fmupdate fgd-wfserver_stat {10m | 30m | 1h | 6h | 12h | 24h
| 7d}
diagnose fmupdate fgt-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fgt-del-statistics
diagnose fmupdate fgt-del-um-db
diagnose fmupdate fml-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fortitoken {seriallist | add | del}
{add | del | required}
diagnose fmupdate getdevice {fct | fds | fgd | fgc} <serial>

```

Variable	Description
add-device <serial> <ip> <firmware> <build>	Add an unregistered device. The build number is optional.
deldevice {fct fds fgd fgc} <serial> <uid>	Delete a device. The UID applies only to FortiClient devices.
faz-bandwidth {1h 6h 12h 24h 7d 30d}	Display the FortiAnalyzer download bandwidth.
fct-bandwidth {1h 6h 12h 24h 7d 30d}	Display the FortiClient download bandwidth.
fct-configure	Dump the FortiClient running configuration.
fct-dbcontract	Dump the FortiClient subscriber contract.
fct-delserverlist	Dump the FortiClient server list file fdni.dat.
fct-getobject	Get the version of all FortiClient objects.
fct-log	View the FortiClient linked log file.
fct-restart	Restart the FortiClient linked service.
fct-serverlist	Dump the FortiClient server list.
fct-update-status	Display the FortiClient update status.
fct-updatenow	Update the FortiClient AV/IPS immediately.

Variable	Description
fds-configure	Dump the FortiDNS running configuration.
fds-dbcontract	Dump the FortiDNS subscriber contract
fds-delserverlist	Delete the FortiDNS server list file fdni.dat.
fds-dump-breg	Dump the FortiDNS beta serial numbers.
fds-dump-srul	Dump the FortiDNS select filtering rules.
fds-get-downstream-device	Get information of all downstream FortiGate AV-IPS devices.
fds-getobject	Get the version of all FortiGate objects.
fds-log	View the FortiDNS linked log file.
fds-restart	Restart the FortiDNS linked service.
fds-serverlist	Dump the FortiDNS server list.
fds-service-info	Display FortiDNS service information.
fds-update-status	Display the FortiDNS update status.
fds-updatenow	Update the FortiGate AV/IPS immediately.
fgc-configure	Dump the FGC running configuration.
fgc-delserverlist	Delete the FGC server list file fdni.dat.
fgc-log	View the FortiGuard for FortiClient linked log file.
fgc-restart	Restart the FGC linked service.
fgc-serverlist	Dump the FGC server list.
fgc-update-status	Display the FGC update status.
fgd-asdbver	Get the SPAM database version.
fgd-asdevice_stat {10m 30m 1h 6h 12h 24h 7d}	Display antispam device statistics.
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-configure	Dump the FortiGuard running configuration.
fgd-dbcontract	Dump the FortiGuard subscriber contract.
fgd-delasdb	Delete the FortiGuard antispam database.
fgd-delavdb	Delete the FortiGuard AV database.
fgd-delserverlist	Delete the FortiGuard server list file fdni.dat.

Variable	Description
fgd-delwfdb	Delete the FortiGuard URLs database.
fgd-get-downstream-device	Get information on all downstream FortiGate web filter and spam devices.
fgd-log	View the FortiGuard linked log file.
fgd-restart	Restart the FortiGuard linked service.
fgd-serverlist	Dump the FortiGuard server list.
fgd-service-info	Display Fortiguard service information.
fgd-update-status	Display the Fortiguard update status.
fgd-updatenow	Update the FortiGate web filter / antispam immediately.
fgd-url-rating <string>	Rate URLs within the FortiManager database using the FortiGate serial number.
fgd-wfas-log	View the FortiGuard service log file.
fgd-wfas-rate	Get the web filter / antispam rating speed.
fgd-wfdbver	Get the URLs database version.
fgd-wfdevice_stat {10m 30m 1h 6h 12h 24h 7d}	Display web filter device statistics.
fgd-wfserver_stat {10m 30m 1h 6h 12h 24h 7d}	Display web filter server statistics.
fgt-bandwidth {1h 6h 12h 24h 7d 30d}	Display the FortiGate download bandwidth.
fgt-del-statistics	Remove all statistics (AV/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.
fml-bandwidth {1h 6h 12h 24h 7d 30d}	Display the FortiMail download bandwidth.
fortitoken {serialist add del} {add del required}	FortiToken related operations.
getdevice {fct fds fgd fgc} <serial>	Get device information.

Example

To view antispam server statistics for the past seven days, enter the following:

```
diagnose fmupdate fgd-asserver_stat 7d
```

The command returns information like this:

```
Server Statistics
```

Total Spam Look-ups: 47
Total # Spam: 21 (45%)
Total # Non-spam: 26 (55%)
Estimated bandwidth usage: 17MB

fwmanager

Use this command to manage firmware.

Syntax

```
diagnose fwmanager cancel-devsched <string> <firmware_version>
    <release_type> <build_num> <date_time>
diagnose fwmanager cancel-grpsched <string> <firmware_version>
    <release_type> <build_num> <date_time>
diagnose fwmanager delete-all
diagnose fwmanager delete-imported-images
diagnose fwmanager delete-offical-images
diagnose fwmanager delete-serverlist
diagnose fwmanager getall-schedule
diagnose fwmanager getdev-schedule <string>
diagnose fwmanager getgrp-schedule <string>
diagnose fwmanager imported-imagelist
diagnose fwmanager official-imagelist
diagnose fwmanager reset-schedule-database
diagnose fwmanager set-devsched <string> <firmware_version>
    <release_type> <build_num> <date_time>
diagnose fwmanager set-grpsched <string> <firmware_version>
    <release_type> <build_num> <date_time>
```

Variable	Description
cancel-devsched <string> <firmware_version> <release_type> <build_num> <date_time>	Cancel an upgrade schedule for a device. For special branches, the release type is the branch point. The build number for official releases is always -1, for special releases it is the build number. The date and time format is: YYYY/MM/DD_hh:mm:ss
cancel-grpsched <string> <firmware_version> <release_type> <build_num> <date_time>	Cancel an upgrade schedule for a group. For special branches, the release type is the branch point. The build number for official releases is always -1, for special releases it is the build number. The date and time format is: YYYY/MM/DD_hh:mm:ss
delete-all	Remove everything in the firmware manager folder. This command requires a reboot.
delete-imported-images	Remove all imported images. This command requires a reboot.
delete-offical-images	Remove all official images. This command requires a reboot.
delete-serverlist	Remove the server list file (fdni.dat). This command requires a reboot.
getall-schedule	Display all upgrade schedules recorded.

Variable	Description
getdev-schedule <string>	Get scheduled upgrades for the device.
getgrp-schedule <string>	Get scheduled upgrades for this group.
imported-imagelist	Get the imported firmware image list
official-imagelist	Get the official firmware image list.
reset-schedule-database	Cleanup and initialize the schedule database and restart the server.
set-devsched <string> <firmware_version> <release_type> <build_num> <date_time>	Create an upgrade schedule for a device.
set-grpsched <string> <firmware_version> <release_type> <build_num> <date_time>	Create an upgrade schedule for a group.

ha

Use this command to manage high availability.

Syntax

```
diagnose ha debug-sync {on | off}
diagnose ha dump-datalog
diagnose ha force-resync
diagnose ha stats
```

Variable	Description
debug-sync {on off}	Turn on synchronized data debug.
dump-datalog	Dump the HA data log.
force-resync	Force re-synchronization.
stats	Get HA statistics.

Example

To turn on debug synchronization, enter the following:

```
diagnose ha debug-sync on
```

hardware

Use this command to view hardware information.

Syntax

```
diagnose hardware info
```

rtm

Use this command to manage the real time monitor.

Syntax

```
diagnose rtm reset-database
diagnose rtm snmp-community-name {get | set} <communityname>
```

Variable	Description
reset-database	Reset the real time monitor database.
snmp-community-name {get set} <communityname>	Get or set the SNMP community name. The community name variable is only used when setting the community name.

Example

To set the community name to Local, enter the following:

```
diagnose rtm snmp-community-name set Local
```

The output from the `diagnose rtm snmp-community-name get` will be:

```
community name: Local
```

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.

FortiAnalyzer units have a built-in sniffer. Packet capture on FortiAnalyzer 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 FortiAnalyzer 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_name> <filter_str> <verbose>
<count>
```

Variable	Description
<interface_name>	Type 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_str>	<p>Type 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.</p> <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>Type one of the following numbers indicating the depth of packet headers and payloads to capture:</p> <ul style="list-style-type: none">• 1 - header only• 2 - IP header and payload• 3 - Ethernet header and payload <p>For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).</p> <p>Default: 1</p>
<count>	<p>Type 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>

Example

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 bolded.

```
FortiAnalyzer# 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

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 IP 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 Ctrl + 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 bolded.

```
FortiAnalyzer# 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

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP 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 Ctrl + 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 bolded.

```
FortiAnalyzer # 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 encodings 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. Type the packet capture command, such as:
diag 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 Ctrl + 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 like this:

```
===== PuTTY log 2013.07.25 11:34:40
=====
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 (formerly called Ethernet) 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:



Methods to open a command prompt vary by operating system.

On Windows XP, go to *Start > Run* and enter `cmd`.

On Windows 7, click the Start (Windows logo) menu to open it, then enter `cmd`.

```
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

Figure 2: Converting sniffer output to .pcap format

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

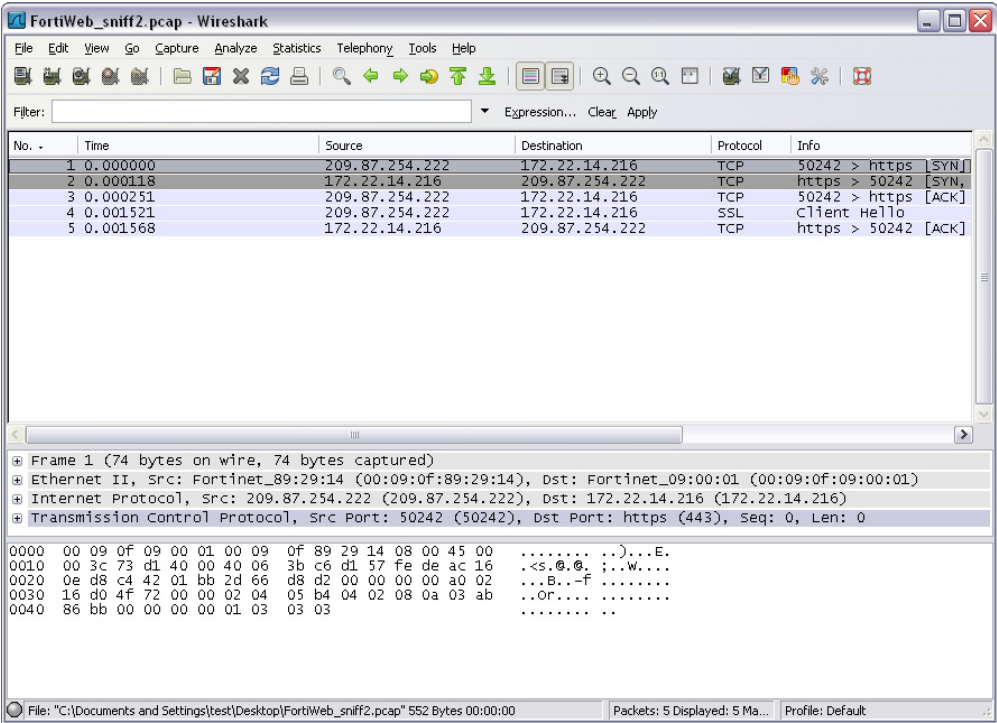
C:\Documents and Settings\test>cd Desktop

C:\Documents and Settings\test\Desktop>fgt2eth.pl -in FortiWeb_sniff.txt -out FortiWeb_sniff.pcap
Conversion of file FortiWeb_sniff.txt phase 1 (FGI verbose 3 conversion)
Output written to FortiWeb_sniff.pcap.
Conversion of file FortiWeb_sniff.txt phase 2 (windows text2pcap)
Output file to load in Ethereal is 'FortiWeb_sniff.pcap'

C:\Documents and Settings\test\Desktop>
```

15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

Figure 3: Viewing sniffer output in Wireshark



For additional information on packet capture, see the [Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer](#).

test application

Use this command to test applications.

Syntax

```
diagnose test application ddmd <var0> <var1> ... <var20>
diagnose test application rtmd <var0> <var1> ... <var20>
```

Variable	Description
ddmd <var0> <var1> ... <var20>	Test the dynamic data monitor daemon.
rtmd <var0> <var1> ... <var20>	Test the real time monitor daemon.

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 test applications.

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).

Syntax

```
diagnose test sftp auth <sftp server> <username> <password>
                        <directory>
```

Variable	Description
auth <sftp server> <username> <password> <directory>	Test the scheduled backup. The directory keyword represents the directory on the SFTP server where you want to put the file. The default directory is "/".

test sysalert

Use this command to test applications.

Syntax

```
diagnose test sysalert add <level> <msg>
diagnose test sysalert clear
diagnose test sysalert list
diagnose test sysalert send <level> <msg>
```

Variable	Description
add <level> <msg>	Add an alert to the alert console. The alert level can be 0 to 7.
clear	Clear the contents in the alert console.
list	List the contents in the alert console.
send <level> <msg>	Send an alert to the system alert daemon. The alert level can be 0 to 7.

get

The `get` commands display a part of your FortiManager unit's configuration in the form of a list of settings and their values.



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.

The `get` command displays all settings, even if they are still 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 fmsystem status
```

and this command would not:

```
get
```

This chapter describes the following `get` commands:

<code>fcdevice temp</code>	<code>fmsystem status</code>
<code>fcdevice unlicensed</code>	<code>fmsystem performance</code>
<code>fmclient status</code>	

fcdevice temp

Use this command to list FortiClient agents discovered and added to the Temporary Clients list.

Syntax

```
get fcdevice temp <host_name>
```

With no host name specified, the command lists the temporary clients. If you specify a host name that is on the temporary clients list, the command provides information like this:

```
host_name      : fips-1
dns_domain     : (null)
ip             : 172.20.120.54
uid            : C5867AD50F694412A34A61AD9A2B81FF
```

Variable	Description
<code><host_name></code>	FortiClient agent host name
<code>dns_domain</code>	The PC's DNS domain name.

Variable	Description
ip <ip>	The PC's IP address.
uid	The PC's UID.

fcdevice unlicensed

Use this command to obtain information about unlicensed FortiClient agents. You can also add a description for the ungrouped agents.

Syntax

```
get fcdevice unlicensed <uid>
```

The get command retrieves information like this:

```
host_name           : fips-1
dns_domain          : (null)
ip                  : 172.20.120.54
```

fmclient status

Use this command to view the status of the FortiClient.

Syntax

```
get fmclient status
```

Example

```
FMG-VM # get fmclient status
FortiClient License           : 2500
Update service at FortiManager : enable
AV version for FortiClient 4.0 : unknown
AV version for FortiClient 4.0 MR3 : unknown
Total managed clients         : 0
Temporary clients             : 0
Current connected clients     : 0
Clients with firewall enabled : 0
Clients with AV enabled       : 0
Patch ready to download       : 0
Patch downloaded to local     : 0
Patch failed download         : 0
Clients with AV up-to-date    : 0
Pending actions               : 0
Total firewall alerts         : 0
Total AV alerts               : 0
Total Patch alerts            : 0
```

fmsystem status

Use this command to view the status of your FortiManager unit.

Syntax

```
get fmsystem status
```

Example

```
FMG-VM # get fmsystem status
Platform Type           : FMG-VM
Version                 : v4.0-build0639 120403 (Interim)
Serial Number           : FMG-VM0A11000137
BIOS version            : 04000002
Hostname                : FMG-VM
Max Number of Admin Domains : 10
Admin Domain Configuration : Enabled
FIPS Mode               : Disabled
HA Mode                 : Stand Alone
Branch Point            : 639
Release Version Information : (Interim)
Current Time            : Wed Apr 11 08:15:27 PDT 2012
Daylight Time Saving    : Yes
Time Zone               : (GMT-8:00) Pacific Time (US&Canada)
License Status          : Valid
```

fmsystem performance

Use this command to view performance statistics on your FortiManager unit.

Syntax

```
get fmsystem performance
```

Example

```
FMG-VM # get fmsystem performance
CPU:
    Used:    5.8%
Memory:
    Total:   2,079,320 KB
    Used:    348,456 KB    16.8%
Hard Disk:
    Total:   9,803,784 KB
    Used:    727,140 KB    7.4%
Flash Disk:
    Total:   47,595 KB
    Used:    28,965 KB    60.9%
```

show

The `show` commands display a part of your Fortinet unit's configuration in the form of 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. For syntax examples and descriptions of each configuration object, field, and option, see [Chapter 8](#) through [Chapter 13](#).

Unlike the `get` command, `show` does not display settings that are assumed to remain in their default state.

Index

A

- accepting FortiClient requests for management 114
- accept_ports
 - fmclient discovery 114
- action
 - fcpolicy antivirus setting realtime 133
 - fcpolicy antivirus setting scheduledscan 135
 - fcpolicy firewall policy 143
- action_queue_interval
 - fmclient communication_setting 113
- action_queue_length
 - fmclient communication_setting 113
- address
 - fcpolicy misc trustedFMGs 155
- address_ipv4
 - execute traceroute 189
- add-vm-license
 - execute 162
- ad_grouping_setting
 - fmclient 110
- admin ldap
 - fmsystem 38
- admin profile
 - fmsystem 40
- admin radius
 - fmsystem 43
- admin setting
 - fmsystem 44
- admin tacacs
 - fmsystem 48
- admin user
 - fmsystem 49
 - trusted hosts 53
- administrative access 70
- administrative domains (ADOMs) 35
- administrator accounts 49
- administrator ldap 38
- administrator profile 40
- administrator settings 44
- ad_ou_grouping
 - fmclient 110
- alert-console
 - fmsystem 54
- alertemail
 - fmsystem 57
- alert-event
 - fmsystem 54
- allowaccess
 - fmsystem interface 70
- all-settings
 - execute restore 186
- analyzer
 - virusreport 92
- analyzer virusreport
 - fmupdate 92
- antileak
 - option 127
 - sensword 128
- antileak option
 - fcpolicy 127
- antileak sensword
 - fcpolicy 128
- antispam
 - bannedword 129
 - blackwhitelist 129
 - option 130
- antispam bannedword
 - fcpolicy 129
- antispam blackwhitelist
 - fcpolicy 129
- antispam option
 - fcpolicy 130
- antispam-port
 - fcpolicy antispam option 130
- antispam-server
 - fcpolicy antispam option 130
- antispam-using-override-server
 - fcpolicy antispam option 130
- antivirus
 - scheduledscan 131
 - setting email 132
 - setting realtime 133
 - setting scheduledscan 134
- antivirus scheduledscan
 - fcpolicy 131
- antivirus setting email
 - fcpolicy 132
- antivirus setting realtime
 - fcpolicy 133
- antivirus setting scheduledscan
 - fcpolicy 134
- archiving 162
- auto_submit
 - fcpolicy antispam option 130
- av-ips
 - advanced-log 93
 - fct server-override 93
 - fgt server-override 94
 - push-override 95
 - push-override-to-client 96
 - update-schedule 97
 - web-proxy 98
- av-ips advanced-log
 - fmupdate 93

- av-ips fct server-override
 - fmupdate 93
- av-ips fgt server-override
 - fmupdate 94
- av-ips push-override
 - fmupdate 95
- av-ips push-override-to-client
 - fmupdate 96
- av-ips update-schedule
 - fmupdate 97
- av-ips web-proxy
 - fmupdate 98

B

- backing up
 - on demand 162
- backup
 - execute 162
- backup all-settings
 - fmsystem 58
- bootimage
 - execute 163

C

- capture
 - packet 215
- certificate
 - ca 59, 163
 - fmsystem 59, 60
 - local 60, 163
 - local generate 164
 - vpn local 60
- certificate ca
 - execute 163
- certificate local
 - execute 163
- certificate local generate
 - execute 164
- checksum
 - fcpolicy firewall service 148
- CLI basics 30
- CLI session 172
- CLI structure 25
- client licenses, FortiClient
 - listing 173
- client_license
 - fmclient 111
- cluster 66
 - secondary 112
 - setting 112
- cluster secondary
 - fmclient 112
- cluster setting
 - fmclient 112
- command abbreviation 32
- command completion 31
- command help 31
- communication_setting
 - fmclient 113

- config 26
- config router 14
- connecting
 - to the CLI 22
 - to the CLI using SSH 24
 - to the FortiManager console 22
- connection
 - ping test 185
 - traceroute test 189
- console baudrate
 - execute 165
- cryptpasswd
 - execute backup all-settings 162
- custom-url-list
 - fmupdate 99

D

- database configuration, restoring 186
- date
 - execute 166
- date_str
 - execute date 166
- Daylight Saving Time 65
- daylightsavetime
 - fmsystem global 65
- debug
 - application 191
 - crashlog 194
 - disable 194
 - dpm 194
 - enable 195
 - info 195
 - sysinfo 195
 - timestamp 195
 - vminfo 196
- debug application
 - diagnose 191
- debug crashlog
 - diagnose 194
- debug disable
 - diagnose 194
- debug dpm
 - diagnose 194
- debug enable
 - diagnose 195
- debug info
 - diagnose 195
- debug sysinfo
 - diagnose 195
- debug timestamp
 - diagnose 195
- debug vminfo
 - diagnose 196
- delete, table shell command 26
- deployment
 - fmupdate 99
- Deployment Manager 61
- deployment mode 99

- description
 - fcdevice ungroup 125
- device
 - execute 167
- devicelog clear
 - execute 167
- device_name
 - execute fgt-cli-access 172
- device-version
 - fmupdate 100

- diagnose 190
 - debug application 191
 - debug cli 194
 - debug crashlog 194
 - debug disable 194
 - debug dpm 194
 - debug enable 195
 - debug info 195
 - debug sysinfo 195
 - debug timestamp 195
 - debug vminfo 196
 - dvm adom 196
 - dvm check-integrity 196
 - dvm debug 197
 - dvm device 197
 - dvm device-tree-update 197
 - dvm group 197
 - dvm lock 197
 - dvm proc 198
 - dvm task 198
 - dvm transaction-flag 198
 - fgfm 199
 - fmclient cache 199, 201
 - fmclient data 200
 - fmclient eventlog 201
 - fmclient performance 202
 - fmnetwork arp 202
 - fmnetwork interface 202
 - fmnetwork netstat 203
 - fmsystem admin-session 204
 - fmsystem disk 204
 - fmsystem export 205
 - fmsystem flash 205
 - fmsystem fsck 205
 - fmsystem logtoconsole 206
 - fmsystem ntp 206
 - fmsystem print 206
 - fmsystem process 207
 - fmsystem raid 208
 - fmsystem route 208
 - fmsystem server 208
 - fmupdate 209
 - fwmanager 213
 - ha 214
 - hardware 214
 - rtm 215
 - sniffer 215
 - test application 220
 - test deploymanager 221
 - test search 221
 - test sftp 222
 - test sysalert 222
 - testpolicy-check 221
- diagnose hardware 214
- disable_auto_vaccum
 - fmclient communication_setting 114
- disable-firewall-notify
 - fcpolicy firewall option 140
- discovery
 - fmclient 114

- disk-quota
 - fmupdate 101
- dm
 - fmsystem 61
- dmserver
 - revlist 167
 - showconfig 168
 - showdev 168
 - showrev 168
- dmserver delrev
 - execute 167
- dmserver revlist
 - execute 167
- dmserver showconfig
 - execute 168
- dmserver showdev
 - execute 168
- dmserver showrev
 - execute 168
- dns
 - fmsystem 63
- DNS servers 63
- dns_domain
 - fcdevice group 123
- dont_prompt
 - fcpolicy antispam option 131
- dst
 - fmsystem route 85
- dvm
 - adom 196
 - check-integrity 196
 - debug 197
 - device 197
 - device-tree-update 197
 - group 197
 - lock 197
 - proc 198
 - task 198
 - transaction-flag 198
- dvm adom
 - diagnose 196
- dvm check-integrity
 - diagnose 196
- dvm debug
 - diagnose 197
- dvm device
 - diagnose 197
- dvm device-tree-update
 - diagnose 197
- dvm group
 - diagnose 197
- dvm lock
 - diagnose 197
- dvm proc
 - diagnose 198
- dvm task
 - diagnose 198

- dvm transaction-flag
 - diagnose 198

E

- edit, table shell command 26
- editing commands 31
- editing the configuration file 34
- emailalert
 - fmclient 114
- enable_antispam
 - fcpolicy antispam option 131
- encrypted password support 32
- end
 - command in a table shell 26
 - command in an edit shell 26
- end_ip
 - fcpolicy firewall address 137
 - fcpolicy misc trustedFMGs 155
- enterprise license, FortiClient
 - downloading 174
 - listing 174
- enterprise_license
 - fmclient 115
- example command sequences 29
- executable
 - fcpolicy firewall service 148
- execute 161
- exempt-files
 - fcpolicy antivirus setting realtime 134
 - fcpolicy antivirus setting schedulescan 135
- exempt-folders
 - fcpolicy antivirus setting realtime 134
 - fcpolicy antivirus setting schedulescan 135
- exempt-types
 - fcpolicy antivirus setting realtime 134
 - fcpolicy antivirus setting scheduledscan 135

F

- failure detection time
 - HA 67
- fcdevice 123
 - addtomanaged 168
 - find-unit 169
 - search 169
 - temp 223
 - unlicensed 224
- fcdevice addtomanaged
 - execute 168
- fcdevice find-unit
 - execute 169
- fcdevice search
 - execute 169
- fcdevice temp
 - get 223
- fcdevice unlicensed
 - get 224

- fcpolicy 127
 - apply_to_members 169
 - deploy 170
 - grant unlicensed 170
 - group 170
 - retrieve 171
 - revoke unit 171
 - unit 171
- fcpolicy apply_to_members
 - execute 169
- fcpolicy deploy
 - execute 170
- fcpolicy grant unlicensed
 - execute 170
- fcpolicy group
 - execute 170
- fcpolicy retrieve
 - execute 171
- fcpolicy revoke unit
 - execute 171
- fcpolicy unit
 - execute 171
- fct server-override 105
- fct-services
 - fmupdate 101
- fgfm
 - diagnose 199
- fgfm reclaim-dev-tunnel
 - execute 172
- fgt-cli-access
 - execute 172
- firewall pingserver
 - fcpolicy 142
- filename
 - execute backup 162
 - execute restore 187
- filesize
 - fcpolicy firewall service 148
- fips
 - fmsystem 63
- firewall
 - address 136
 - addrgrp 137
 - apppolicy 138
 - option 139
 - pingserver 142
 - policy 142
 - protocol 144
 - protocolgrp 145
 - schedule recurring 145
 - schedulegrp 146
 - service 147
 - trustedip address 148
 - zone 149
- firewall address
 - fcpolicy 136
- firewall addrgrp
 - fcpolicy 137
- firewall apppolicy
 - fcpolicy 138
- firewall option
 - fcpolicy 139
- firewall policy
 - fcpolicy 142
- firewall protocol
 - fcpolicy 144
- firewall protocolgrp
 - fcpolicy 145
- firewall schedule recurring
 - fcpolicy 145
- firewall schedulegrp
 - fcpolicy 146
- firewall service
 - fcpolicy 147
- firewall trustedip address
 - fcpolicy 148
- firewall zone
 - fcpolicy 149
- firmware image, uploading 187
- fmclient 110
 - apply-lockdown 172
 - cache 199, 201
 - client_license list 173
 - client_license list_device 173
 - cluster 174
 - data 200
 - enterprise_license download 174
 - enterprise_license list 174
 - eventlog 201
 - group refresh 175
 - group rename 175
 - license_key deploy 175
 - license_key list 175
 - optimize-fcm-database 176
 - package delete 176
 - package deploy 176
 - package download 176
 - package list 177
 - performance 202
 - refresh_ou 177
 - status 224
 - sync-ldap 177
 - sync_ou_group 177
- fmclient apply-lockdown
 - execute 172
- fmclient cache
 - diagnose 199, 201
- fmclient client_license list 161
 - execute 173
- fmclient client_license list_device
 - execute 173
- fmclient cluster
 - execute 174
- fmclient data
 - diagnose 200
- fmclient enterprise_license download 161
 - execute 174
- fmclient enterprise_license list
 - execute 174

- fmclient eventlog
 - diagnose 201
- fmclient group refresh
 - execute 175
- fmclient group rename 161
 - execute 175
- fmclient license_key deploy
 - execute 175
- fmclient license_key list
 - execute 175
- fmclient optimize-fcm-database 161
 - execute 176
- fmclient package delete 161
 - execute 176
- fmclient package deploy 161
 - execute 176
- fmclient package download 161
 - execute 176
- fmclient package list 161
 - execute 177
- fmclient performance
 - diagnose 202
- fmclient refresh_ou 161
 - execute 177
- fmclient status
 - get 224
- fmclient sync ou_group 161
- fmclient sync-ldap 161
 - execute 177
- fmclient sync_ou_group
 - execute 177
- fmnetwork
 - arp 202
 - interface 202
 - netstat 203
- fmnetwork arp
 - diagnose 202
- fmnetwork interface
 - diagnose 202
- fmnetwork netstat
 - diagnose 203
- fmpolicy 178, 179
 - copy-global-object 178
 - install-config 178
 - print-device-database 179
 - print-global-database 179
 - print-global-object 179
- fmpolicy copy-global-object
 - execute 178
- fmpolicy install-config
 - execute 178
- fmpolicy print-device-database
 - execute 179
- fmpolicy print-global-database
 - execute 179
- fmpolicy print-global-object
 - execute 179

- fmscript
 - clean-sched 179
 - delete 180
 - import 180
 - list 181
 - run 181
 - showlog 182
- fmscript clean-sched
 - execute 179
- fmscript delete
 - execute 180
- fmscript import 161
 - execute 180
- fmscript list
 - execute 181
- fmscript run 161
 - execute 181
- fmscript showlog 161
 - execute 182
- fmsystem 38
 - admin-session 204
 - disk 204
 - export 205
 - flash 205
 - fsck 205
 - logtoconsole 206
 - ntp 206
 - performance 225
 - print 206
 - process 207
 - route 208
 - server 208
- fmsystem admin-session
 - diagnose 204
- fmsystem disk
 - diagnose 204
- fmsystem export
 - diagnose 205
- fmsystem flash
 - diagnose 205
- fmsystem fsck
 - diagnose 205
- fmsystem logtoconsole
 - diagnose 206
- fmsystem ntp
 - diagnose 206
- fmsystem performance
 - get 225
- fmsystem print
 - diagnose 206
- fmsystem process
 - diagnose 207
- fmsystem raid 208
- fmsystem route
 - diagnose 208
- fmsystem server
 - diagnose 208
- fmsystem status 225

- fmupdate 92
 - diagnose 209
 - export 183
 - import 183
- fmupdate export
 - execute 183
- fmupdate import
 - execute 183
- format disk
 - execute 184
- FortiAnalyzer
 - configuring 79
- fortianalyzer send_all_configurations 161
- fortianalyzer send_configurations 161
- FortiClient
 - configuring communication settings 113
- FortiClient group administrators 116
- FortiGate SNMP agent 88
- FortiGate, IP address 172
- FortiLog
 - configuring access 79
- FortiManager
 - rebooting 186
 - shutting down 187
 - status 225
 - trustedfortimanager setting 155
- FortiManager, resetting 186
- Fortinet
 - Technical Support 216
- fqdn
 - fcpolicy misc trustedFMGs 155
- fwmanager
 - diagnose 213

G

- get 223, 225
 - command in a table shell 26
 - command in an edit shell 26
 - fcdevice temp 223
 - fcdevice unlicensed 224
 - fmclient status 224
 - fmsystem performance 225
 - fmsystem status 225
- global
 - fmsystem 64
- global settings 64
- group
 - fcdevice 123
 - for FortiClient group administrator 116
- group_admin
 - fmclient 116
- grouptype
 - fcdevice group 124

H

- HA 66
 - configuration 68
 - failure detection time 67
 - synchronization interface 66
 - synchronization port 66

- ha
 - diagnose 214
 - fmsystem 66
 - fmsystem locallog filter 74
- hard disk
 - formatting 184
- hb-interval
 - fmsystem ha 67
- hb-lost-threshold
 - fmsystem ha 67
- heuristic
 - fcpolicy antivirus setting email 132
 - fcpolicy antivirus setting realtime 134
 - fcpolicy antivirus setting scheduledscan 135
- high availability 66
- host-name
 - execute traceroute 189
- HTTP 70
- HTTPS 70

I

- ICMP echo request 185
- image
 - execute restore 187
- interface
 - bringing up or down 69
 - configuring 69
 - fmsystem 69
 - system snmp community hosts 87
- International characters 33
- introduction 12
- ip
 - execute backup 162
 - fmsystem interface 69
 - fmsystem log fortianalyzer 80
 - system snmp community hosts 87
- IP address formats 33
- ip_address
 - fcdevice group 124
 - fcpolicy firewall address 137

L

- LCD PIN, setting 65
- lcdpin
 - fmsystem global 65
- ldapsetting
 - fmclient 118
- ldap_users
 - fmclient 117
- level
 - fmsystem log setting 81
- license keys, FortiClient
 - deploying 175
 - listing 175
- license_key
 - fmclient 118
- line continuation 32
- load_at_startup
 - fcpolicy system settings 154

- locallog
 - filter 73
 - FortiAnalyzer settings 76
 - memory setting 76
 - syslogd 77
- locallog disk setting
 - fmsystem 70
- locallog filter
 - fmsystem 73
- locallog fortianalyzer setting
 - fmsystem 76
- Locallog memory setting
 - fmsystem 76
- locallog syslogd setting
 - fmsystem 77
- local_maxfilesize
 - fcpolicy log setting 151
- location
 - system snmp sysinfo 88
- location_aware
 - fmclient 119
- lockdown
 - fmclient 120
- lockdown_status
 - fcpolicy system settings 154
- log
 - setting 150
- log filter
 - settings 73
- log fortianalyzer
 - fmsystem 79
- log setting
 - fcpolicy 150
 - fmsystem 80
- log settings 70
 - syslogd 77
- log-alert
 - action for fcpolicy antivirus setting email 132
- lrmgr
 - fmsystem locallog filter 74

M

- mail
 - fmsystem 81
- max-log-file-size
 - fmsystem locallog 71
 - fmsystem locallog disk setting 71
- member
 - fcdevice group 124
 - fcpolicy firewall addrgrp 138
 - fcpolicy firewall svcgrp 147
- memory
 - enabling virtual memory 65
- metadata
 - fmsystem 82
- min_message_interval
 - fmclient communication_setting 114
- month, setting 166
- multilayer
 - fmupdate 102

N

- name
 - system snmp community 86
- newclient_action
 - fmclient discovery 114
- next 27
- ntp
 - fmsystem 82
- NTP server, configuring 82

O

- option access_ungroup
 - for FortiClient group administrator 116
- os_name
 - fcdevice group 124

P

- packet
 - capture 215
 - trace 215
- passwd
 - fmsystem backup 58
 - fmsystem log fortianalyzer 80
- password
 - execute backup 162
 - fmclient lockdown 120
 - fmsystem admin user 50
 - for backup server 58
- password-policy
 - fmsystem 83
- path
 - execute backup all-settings 162
- performance
 - fmsystem 225
- performance statistics 225
- ping 70
 - execute 185
- policy
 - fcdevice group 124
 - fcpolicy vpn 157
- port
 - bringing up or down 69
 - configuring 69
 - fmsystem locallog syslogd setting 78
- primary
 - fmsystem dns 63
- primary image 163
- private-server
 - configuration 103
- processes, viewing 188
- profileid
 - fmsystem admin user 50
- protocol
 - fmsystem backup 58
- psk
 - fmsystem log fortianalyzer 80
- publicnetwork
 - fmupdate 102
- purge 26

Q

- query-v1-port
 - system snmp community 86
- query-v1-status
 - system snmp community 86
- query-v2c-port
 - system snmp community 86
- query-v2c-status
 - system snmp community 86

R

- raid 185
 - execute 185
- raise_alert_to_fmng
 - fcpolicy system settings 154
- real time monitor
 - diagnose 215
- reboot
 - execute 186
- recalling commands 31
- remote_facility
 - fcpolicy log setting 151
- reset
 - execute 186
- resources, viewing 188
- restore 161
 - execute 186
- roll-schedule
 - fmsystem locallog 71
 - fmsystem locallog disk setting 71
- rotatesize
 - fmsystem log setting 81
- route
 - fmsystem 84
- routing
 - configuring for FortiManager 84
 - ip 85
- rtm
 - diagnose 215
- rtmon
 - fmsystem locallog filter 75

S

- scan-compress
 - fcpolicy antivirus setting realtime 134
 - fcpolicy antivirus setting scheduledscan 136
- scan-grayware
 - fcpolicy antivirus setting realtime 134
 - fcpolicy antivirus setting scheduledscan 136
- scan_level
 - fcpolicy antivirus scheduledscan 132
- secondary
 - fmsystem dns 63
- secondary image 163
- serial connection 165
- server
 - fmsystem backup 58
 - fmsystem locallog syslogd setting 78
 - fmsystem ntp 83

- server-access-priorities
 - fmupdate 102
- server-override-status
 - fmupdate 104
- service
 - fmupdate 104
- set 27
- setting administrative access for SSH or Telnet 23
- severity
 - fmsystem locallog 71
 - fmsystem locallog disk setting 71
 - fmsystem locallog fortianalyzer setting 76
 - fmsystem locallog syslogd 79
- show 226
- shutdown
 - execute 187
- sniffer 215
 - diagnose 215
- SNMP
 - v1 86
 - v2c 86
- snmp
 - community 85
 - sysinfo 88
 - user 89
- snmp community
 - fmsystem 85
 - system 85
- snmp sysinfo
 - fmsystem 88
 - system 88
- snmp user
 - fmsystem 89
- software upgrade packages, FortiClient
 - deleting 176
- spaces, entering in strings 33
- special characters, where they are allowed 33
- ssh 70
 - execute 188
- ssh-public-key
 - fmsystem admin user 51
- start_ip
 - fcpolicy firewall address 137
 - fcpolicy misc trustedFMGs 155
- status
 - fcpolicy antivirus setting email 132
 - fcpolicy antivirus setting realtime 134
 - fmclient 224
 - fmclient lockdown 120
 - fmsystem 225
 - fmsystem backup 58
 - fmsystem interface 69
 - fmsystem locallog 71, 79
 - fmsystem locallog disk setting 71, 79
 - fmsystem locallog fortianalyzer setting 76
 - fmsystem locallog memory setting 77
 - fmsystem log fortianalyzer 80
 - fmsystem ntp 83
 - system snmp community 86
 - system snmp sysinfo 88

- strip-quarantine
 - action for fcpolicy antivirus setting email 132
- subnet
 - fcpolicy firewall address 137
 - fcpolicy misc trustedFMGs 155
- swapmem
 - fmsystem global 65
- synchronization interface
 - HA 66
- synchronization port
 - HA 66
 - See also synchronization interface 66
- sync_interval
 - fmsystem ntp 83
- syslog
 - fmsystem 90
- system
 - fmsystem locallog filter 75
 - locationaware 152
 - settings 152
 - trustedfortimanager 155
 - wan_optimization 156
- system locationaware
 - fcpolicy 152
- system settings
 - fcpolicy 152
- system trustedfortimanager
 - fcpolicy 155
- system wan_optimization
 - fcpolicy 156
- systemsetting
 - fmclient 120

T

- temp
 - fcdevice 223
- test
 - application 220
 - deploymanager 221
 - policy-check 221
 - search 221
 - sftp 222
 - sysalert 222
- test application
 - diagnose 220
- test deploymanager
 - diagnose 221
- test policy-check
 - diagnose 221
- test search
 - diagnose 221
- test sftp
 - diagnose 222
- test sysalert
 - diagnose 222
- time 161
 - execute 188
 - fcpolicy antivirus scheduledscan 132
 - fmsystem backup 58
 - setting automatically 82

- top
 - execute 188
- trace
 - packet 215
- tracert 161
 - execute 189
- trap-v1-rport
 - system snmp community 87
- trap-v1-status
 - system snmp community 87
- trap-v2c-rport
 - system snmp community 87
- trap-v2c-status
 - system snmp community 87
- troubleshooting 190, 216
- trusted FortiManager
 - setting 155
- trusted hosts
 - administrator 50
 - security issues 53
- trusthost
 - fmsystem admin user 50
- type
 - fcdevice group 124
 - fcpolicy antivirus scheduledscan 132
 - fcpolicy firewall address 137
 - fcpolicy misc trustedFMGs 155
- type automatic
 - fcpolicy vpn 157

U

- ungroup
 - fcdevice 125
- unit
 - fcdevice 126
- unlicensed
 - fcdevice 224
- unset 27
- update_server
 - fcpolicy system settings 154
- update_server_address
 - fcpolicy system settings 154
- update_server_port
 - fcpolicy system settings 154
- Upgrade Manager
 - disk space 101
- upload-delete-files
 - fmsystem locallog disk setting 72
- uploadaddr
 - fmsystem locallog disk setting 72
- uploadip
 - fmsystem locallog disk setting 72
- uploadpass
 - fmsystem locallog disk setting 72
- uploadport
 - fmsystem locallog disk setting 72
- uploadsched
 - fmsystem locallog disk setting 72

- upload-time
 - fmsystem locallog disk setting 72
- uploadtype
 - fmsystem locallog disk setting 72
- uploaduser
 - fmsystem locallog disk setting 72
- uploadzip
 - fmsystem locallog disk setting 72
- URL list
 - configure 99
- US-ASCII 218
- username
 - execute backup 162
 - execute fgt-cli-access 172
- using the CLI 21
- using the Command Line Interface 21

V

- virtual memory 65
- vpn 59
 - download 156
 - option 157
 - security policy 158
- vpn download
 - fcpolicy 156
- vpn option
 - fcpolicy 157
- vpn security_policy
 - fcpolicy 158

W

- webfilter
 - option 158
 - profile 160
- webfilter option
 - fcpolicy 158
- webfilter profile
 - fcpolicy 160

- webfilter-default-action
 - fcpolicy webfilter option 159
- webfilter-log-all-urls
 - fcpolicy webfilter option 159
- webfilter-port
 - fcpolicy webfilter option 159
- webfilter_profile
 - fmclient 121
- webfilter-server
 - fcpolicy webfilter option 159
- webfilter-status
 - fcpolicy webfilter option 159
- webfilter-using-override-server
 - fcpolicy webfilter option 159
- web-spam 105
 - fgd-log 106, 107
 - fgt server-override 107
 - poll-frequency 108
 - web-proxy 108
- web-spam fct server-override
 - fmupdate 105
- web-spam fgd-log
 - fmupdate 106, 107
- web-spam fgt server-override
 - fmupdate 107
- web-spam poll-frequency
 - fmupdate 108
- web-spam web-proxy
 - fmupdate 108
- week_days
 - fmsystem backup 58
- what's new 14
- windows_group
 - fcdevice group 124
- worm-scan
 - fcpolicy antivirus setting email 133

Y

- year, setting 166

