

# FortiManager<sup>™</sup>

Version 4.0 MR2

CLI Reference



## **FortiManager CLI Reference**

Version 4.0 MR2

15 July 2010

02-402-126283-20100701

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

### **Trademarks**

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

### **Regulatory compliance**

FCC Class A Part 15 CSA/CUS



**CAUTION:** Risk of Explosion if Battery is replaced by an Incorrect Type.  
Dispose of Used Batteries According to the Instructions.

# Contents

<b>Introduction .....</b>	<b>9</b>
<b>About the FortiManager system .....</b>	<b>9</b>
<b>Web-based manager .....</b>	<b>10</b>
<b>FortiManager system product life cycle .....</b>	<b>10</b>
<b>Registering your Fortinet product.....</b>	<b>11</b>
<b>Customer service and technical support.....</b>	<b>11</b>
<b>Fortinet documentation .....</b>	<b>11</b>
Fortinet Tools and Documentation CD .....	11
Fortinet Knowledge Center .....	11
Comments on Fortinet technical documentation .....	11
<b>Conventions .....</b>	<b>12</b>
IP addresses.....	12
CLI constraints.....	12
Notes, Tips and Cautions .....	12
Typographical conventions .....	13
<b>What's new .....</b>	<b>15</b>
<b>Using the CLI.....</b>	<b>17</b>
<b>CLI command syntax .....</b>	<b>17</b>
<b>Connecting to the CLI.....</b>	<b>18</b>
Connecting to the FortiManager console.....	18
Setting administrative access on an interface .....	19
Connecting to the FortiManager CLI using SSH.....	20
Connecting to the FortiManager CLI using the web-based manager .....	20
<b>CLI objects.....</b>	<b>20</b>
<b>CLI command branches .....</b>	<b>21</b>
config branch .....	21
get branch.....	23
show branch .....	24
execute branch .....	24
diagnose branch .....	24
Example command sequences.....	25

<b>CLI basics .....</b>	<b>25</b>
Command help .....	26
Command completion .....	26
Recalling commands .....	26
Editing commands .....	26
Line continuation .....	27
Command abbreviation .....	27
Environment variables .....	27
Encrypted password support .....	27
Entering spaces in strings .....	28
Entering quotation marks in strings .....	28
Entering a question mark (?) in a string .....	28
International characters .....	28
Special characters .....	29
IP address formats .....	29
Editing the configuration file .....	29
Changing the baud rate .....	29
<b>Administrative Domains (ADOMs) .....</b>	<b>31</b>
<b>ADOMs overview .....</b>	<b>31</b>
Elemental Management System .....	31
Global Management System .....	32
Administrative domain device modes .....	32
<b>Configuring ADOMs .....</b>	<b>33</b>
<b>fcdevice .....</b>	<b>35</b>
group .....	36
temp .....	38
ungroup .....	39
unit .....	40
unlicensed .....	41
<b>fmclient .....</b>	<b>43</b>
client_license .....	44
cluster secondary .....	45
cluster setting .....	46
communication_setting .....	47
discovery .....	48
emailalert .....	49
enterprise_license .....	50
group_admin .....	51
ldap_users .....	52

ldapsetting .....	53
license_key .....	54
lockdown.....	55
systemsetting .....	56
webfilter_profile .....	57
<b>fmupdate .....</b>	<b>59</b>
analyzer virusreport.....	60
av-ips advanced-log.....	61
av-ips fct server-override .....	62
av-ips fgt server-override .....	63
av-ips push-override.....	64
av-ip push-override-to-client.....	65
av-ips update-schedule .....	66
av-ips web-proxy.....	67
deployment .....	68
device-version .....	69
disk-quota .....	70
fct-services .....	71
publicnetwork.....	72
server-access-priorities.....	73
service.....	75
<b>fmsystem .....</b>	<b>77</b>
admin ldap .....	78
admin profile.....	80
admin radius.....	94
admin setting.....	95
admin user .....	97
alert-console.....	100
alert-event .....	101
alertemail .....	103
backup all-settings.....	104
certificate ca .....	106
certificate local .....	107
dm.....	108
dns.....	110
global.....	111

ha .....	113
interface .....	119
locallog disk setting.....	121
locallog filter .....	124
locallog fortianalyzer setting .....	126
locallog memory setting.....	127
locallog syslogd (syslogd2, syslogd3) setting.....	128
locallog syslogd (syslogd2, syslogd3) filter.....	130
log fortianalyzer .....	132
log setting .....	133
log rolling.....	134
metadata .....	136
ntp.....	137
ntpserver .....	138
performance .....	139
route .....	140
snmp community .....	141
snmp sysinfo .....	144
status.....	145
<b>execute.....</b>	<b>147</b>
backup.....	149
bootimage .....	150
certificate ca .....	151
certificate local .....	152
certificate local generate .....	153
console baudrate .....	154
date.....	155
device .....	156
dmserver delrev .....	157
dmserver showconfig .....	158
dmserver showdev.....	159
dmserver showrev .....	160
dmserver revlist .....	161
fcdevice addtomanaged .....	162
fcpolicy apply_to_members.....	163
fcdevice search .....	164

fcpolicy deploy .....	165
fcpolicy grant unlicensed.....	166
fcpolicy group .....	167
fcpolicy retrieve.....	168
fcpolicy revoke unit .....	169
fcpolicy unit .....	170
fgfm reclaim-dev-tunnel .....	171
fgt-cli-access .....	172
fmclient apply-lockdown .....	173
fmclient client_license list.....	174
fmclient client_license list_device .....	175
fmclient cluster.....	176
fmclient enterprise_license download .....	177
fmclient enterprise_license list.....	178
fmclient group refresh .....	179
fmclient group rename .....	180
fmclient license_key deploy.....	181
fmclient license_key list .....	182
fmclient optimize-fcm-database .....	183
fmclient package delete.....	184
fmclient package deploy .....	185
fmclient package download .....	186
fmclient package list.....	187
fmclient sync-ldap.....	188
fmclient refresh_ou.....	189
fmclient sync ou_group.....	190
fmpolicy print-global-database.....	191
fmpolicy copy-global-object .....	192
Fmpolicy print-global-object .....	193
fmscript delete.....	194
fmscript import.....	195
fmscript list.....	196
fmscript run .....	197
fmscript showlog .....	198
fmupdate {ftp   tftp} import.....	199
format disk.....	200

<b>fortianalyzer get_configurations .....</b>	<b>201</b>
<b>fortianalyzer send_all_configurations .....</b>	<b>202</b>
<b>fortianalyzer send_configurations .....</b>	<b>203</b>
<b>ping.....</b>	<b>204</b>
<b>raid.....</b>	<b>205</b>
<b>reboot .....</b>	<b>206</b>
<b>reset.....</b>	<b>207</b>
<b>restore .....</b>	<b>208</b>
<b>shutdown .....</b>	<b>209</b>
<b>ssh .....</b>	<b>210</b>
<b>time.....</b>	<b>211</b>
<b>top.....</b>	<b>212</b>
<b>tracert.....</b>	<b>213</b>
<b>Index.....</b>	<b>215</b>

# Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

The FortiManager system is an integrated platform for centralized management of the major Fortinet products.

Using the FortiManager system, you can:

- configure multiple FortiGate units, FortiSwitch units, FortiOS Carrier units, FortiMail units, FortiAnalyzer units, and FortiClient PCs,
- configure and manage VPN policies,
- monitor the status of these units,
- view and analyze device logs,
- update the virus and attack signatures,
- provide web filtering and antispam service to the licensed devices as a local Fortinet Distribution Network (FDN) server,
- update the firmware images of the devices.

The FortiManager system scales to manage up to a thousand devices and FortiClient PCs simultaneously. It is designed for 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:

- [Registering your Fortinet product](#)
- [Customer service and technical support](#)
- [Fortinet documentation](#)
- [Conventions](#)

## 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 an on-site FDN server for the managed devices to download virus and attack signatures, and to use the web filtering and antispam service. This will significantly reduce the network delay and usages, compared with the managed devices' connection to an FDN server over the Internet.

## Web-based manager

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

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 Console also allows these users to remotely upgrade device firmware, and virus and attack definitions.

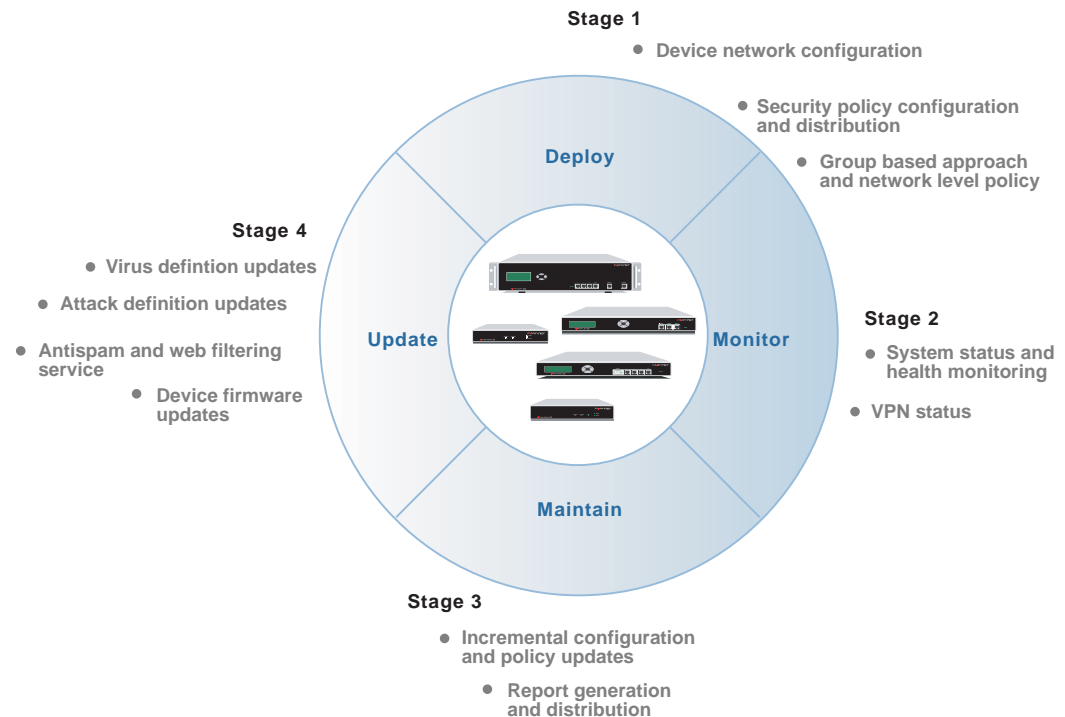
Administrators with read only access can view the configuration, device status, system health, real time logs, and historical logs of the devices assigned to them.

## FortiManager system product life cycle

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

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

Figure 1: FortiManager System product life cycle



## Registering your Fortinet product

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

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

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

## Customer service and technical support

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

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

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Center article [What does Fortinet Technical Support require in order to best assist the customer?](#)

## Fortinet documentation

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

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

### Fortinet Tools and Documentation CD

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

### Fortinet Knowledge Center

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

### Comments on Fortinet technical documentation

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

# Conventions

Fortinet technical documentation uses the conventions described below.

## IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

## CLI constraints

CLI constraints, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable input for a given parameter or variable value. CLI constraint conventions are described in the CLI Reference document for each product. See “Using the CLI” on [page 17](#).

## Notes, Tips and Cautions

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.



**Tip:** Highlights useful additional information, often tailored to your workplace activity.



**Note:** Also presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.



**Caution:** Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

## Typographical conventions

Fortinet documentation uses the following typographical conventions:

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

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns   set primary &lt;address_ipv4&gt; end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments           : (null) opmode              : nat</pre>
Emphasis	HTTP connections are <b><i>not</i></b> secure and can be intercepted by a third party.
File content	<pre>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt; &lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</pre>
Hyperlink	Visit the Fortinet Technical Support web site, <a href="https://support.fortinet.com">https://support.fortinet.com</a> .
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <i>VPN &gt; IPSEC &gt; Auto Key (IKE)</i> .
Publication	For details, see the <a href="#">FortiGate Administration Guide</a> .



# What's new

The tables below list commands which have changed the FortiManager v4.0 MR2 release.

Command	Change
<code>config fmsystem admin - profile</code>	Added variable to the admin profile. <ul style="list-style-type: none"><li>• domain-install</li></ul>
<code>config fmsystem log fortianalyzer</code>	Removed secure connection information: <ul style="list-style-type: none"><li>• secure connection</li></ul>
<code>config fmsystem ntp</code>	Added ntp server ID information. <ul style="list-style-type: none"><li>• ntpserver id</li><li>• metadata</li></ul>
<code>config fmsystem radius</code>	Added variables to configure secondary server and password. <ul style="list-style-type: none"><li>• secondary-server</li><li>• secondary-secret</li></ul>
<code>config fmsystem tacacs</code>	Added a new command to configure TACACS,
<code>config fmsystem user metatdata</code>	Added a new variable: <ul style="list-style-type: none"><li>• status</li></ul>
<code>config fmsystem locallog disk</code>	Added new variable: <ul style="list-style-type: none"><li>• server-type</li><li>• filter</li></ul>
<code>config fmsystem locallog memory</code>	Added link to filter information: <ul style="list-style-type: none"><li>• filter</li></ul>
<code>config fmsystem locallog fortianalyzer filter</code>	Added link to filter information. <ul style="list-style-type: none"><li>• filter</li></ul>
<code>config fmsystem locallog syslogd</code>	Added link to filter information. <ul style="list-style-type: none"><li>• filter</li></ul>
<code>config fmsystem locallog syslogd2, 3</code>	Added link to filter information. <ul style="list-style-type: none"><li>• filter</li></ul>
<code>config fmupdate av-ipspush-override-to-client</code>	Added new command.
<code>config fmupdate {ftp   tftp} import</code>	Updated information.
<code>config fmupdate publicnetwork</code>	Added new command.
<code>execute fcpolicy deploy</code>	Added information to deploy fcpolicy to members and related child groups.
<code>execute fmpolicy print global database.</code>	Command added.
<code>execute fmpolicy print global database</code>	Added new command and related variables.
<code>execute format-disk raid</code>	Added new commands to manage RAID disks. <ul style="list-style-type: none"><li>• add-disk</li><li>• delete-disk</li><li>• rebuild-ecc</li></ul>
<code>execute enterprise-license list</code>	Added new commands to refresh and sync ldap server. <ul style="list-style-type: none"><li>• refresh ou</li><li>• sync ougroup</li></ul>



# Using the CLI

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 netmask.

<xxx\_ipv4mask> indicates a dotted decimal IPv4 address followed by a dotted decimal IPv4 netmask.

- 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

You need:

- a computer with an available communications port
- a null modem 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



**Note:** 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 FortiManager-400):

```
FMG400 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 FortiManager-400):

```
FMG400 #
```

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
```



**Note:** 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.



**Note:** 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 manual.

**Table 2: CLI objects**

<b>fcdevice</b>	Configures FortiClient PCs and client groups.
<b>fcpolicy</b>	Configures the settings of FortiClient PCs or client groups.
<b>fmclient</b>	Configures the FortiManager settings used to manage clustering, discovering and adding FortiClient PCs, licenses, client lockdown, and web filtering for managed FortiClient PCs.
<b>fmsystem</b>	Configures options related to the overall operation of the FortiManager unit, such as interfaces, virtual domains, and administrators.
<b>fmupdate</b>	Configures settings related to FortiGuard service updates and the FortiManager unit's built-in FDS.

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 25](#).

### 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 are multiple, 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:

<b>delete</b>	Remove an entry from the FortiManager configuration. For example in the <code>config system admin shell</code> , type <code>delete newadmin</code> and press Enter to delete the administrator account named <code>newadmin</code> .
<b>edit</b>	Add an entry to the FortiManager configuration or edit an existing entry. For example in the <code>config system admin shell</code> : <ul style="list-style-type: none"> <li>• type <code>edit admin</code> and press Enter to edit the settings for the default admin administrator account.</li> <li>• type <code>edit newadmin</code> and press Enter to create a new administrator account with the name <code>newadmin</code> and to edit the default settings for the new administrator account.</li> </ul>
<b>end</b>	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. You return to the root FortiManager CLI prompt. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.
<b>get</b>	List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the keywords and their values.

**purge** Remove all entries configured in the current shell. For example in the `config user local shell`:

- type `get` to see the list of user names added to the FortiManager configuration,
- type `purge` and then `y` to confirm that you want to purge all the user names,
- type `get` 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:

<b>abort</b>	Exit an edit shell without saving the configuration.
<b>config</b>	In a few cases, there are subcommands that you access using a second config command while editing a table entry. An example of this is the command to add host definitions to an SNMP community.
<b>end</b>	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.
<b>get</b>	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.
<b>next</b>	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> . <ul style="list-style-type: none"> <li>• Type <code>edit User1</code> and press Enter.</li> <li>• Use the <code>set</code> commands to configure the values for the new admin account.</li> <li>• Type <code>next</code> to save the configuration for User1 without leaving the <code>config fmsystem admin user shell</code>.</li> <li>• Continue using the <code>edit</code>, <code>set</code>, and <code>next</code> commands to continue adding admin user accounts.</li> <li>• type <code>end</code> and press Enter to save the last configuration and leave the shell.</li> </ul>
<b>set</b>	Assign values. For example from the <code>edit admin</code> command shell, typing <code>set passwd newpass</code> changes the password of the admin administrator account to <code>newpass</code> . Note: When using a <code>set</code> command to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
<b>show</b>	Show changes to the default configuration in the form of configuration commands.
<b>unset</b>	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 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 netmask 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**.



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

## Example command sequences



**Note:** 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 3](#) to edit the command.

**Table 3: 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 non-ambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st`.

## Environment variables

The FortiManager CLI supports several environment variables.

- \$USERFROM** The management access type (SSH, Telnet and so on) and the 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+ZnrgbudK7aryyflscXcXdnQxskRcU3E9XqOit82PgS
cwzGzGuJ5a9f
    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+ZnrgbudK7aryyflscXcXdnQxskRcU3E9XqOit82PgSc
wzGzGuJ5a9f
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.



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



# Administrative Domains (ADOMs)

This chapter provides information about the Administrative Domain (ADOM) functionality introduced in FortiManager 4.0.

This chapter includes the following sections:

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

## ADOMs overview

Administrative domains have two modes of operation. When you create a new administrative domain, you select the mode best suited for the administration of the devices. The modes are Elemental Management System (EMS) and Global Management System (GMS). Depending on the mode selected, there are slight variances to the feature set available within the web-based manager. These variances do not necessarily restrict an administrator from managing their devices. Each mode has unique capabilities to complement their roles.



**Note:** A device can only be managed in one mode. For example you cannot have a FortiGate unit managed by two administrators in two different modes. Due to the differences in each mode, outlined below, this could not be a feasible option.

The default operating mode for the FortiManager unit is Element Management System. The `admin` administrator, by default, always logs into the `root` administrative domain, which is always in Element Management mode. These administrators can switch to Global Management mode if required. To always log in to the FortiManager in Global Management mode, you need to create a super-user admin tied to a Global Management mode administrative domain.

By default, administrator accounts other than the `admin` account are assigned to the `root` administrative domain, which includes all devices in the device list. By creating administrative domains that contain a subset of devices in the device list, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiManager unit's total devices or VDOMs.



**Note:** The `admin` administrator account cannot be restricted to an administrative domain.

## Elemental Management System

Simply put, Element Management System (EMS) mode enables administrators to manage multiple devices with multiple or varying configurations. That is, administrators may have many FortiGate units (or FortiGate VDOMs), and each unit requires a unique or specific configuration, whether its firewall policies, user groups, VPN configurations and so on.

Element Management mode provides a number of features that are not available in GMS mode. This does not limit one mode over another, but provides a different feature set for managing devices.

Element Management mode includes:

- administrative web portal configurations
- XML API support
- Script Manager

- Security Console is not available.

## Global Management System

Simply put, Global Management System (GMS) mode enables administrators to manage multiple devices with a single configuration. That is, administrators may have many FortiGate units (or FortiGate VDOMs). In a corporate environment, each firewall configuration and installation will have the same policies, groups, VPN configurations and setup. In GMS mode administrators can create the configurations and push them to all devices in a “shotgun” approach. It is important to remember that in this mode, updating or changing an individual device is not an option. Any update or change will affect all devices being managed.

Global Management mode provides a number of features that are not available in EMS mode. This does not limit one mode over another, but provides a different feature set for managing devices.

Global Management mode includes a Security Console management for global elements including VPN, dynamic objects and policy console. Global Management mode does not include the administrative web portal configurations, or the XML API.

## Administrative domain mode matrix

To summarize the FortiManager administrative domain modes and what features are available as shown in the table below

	Element Management System	Global Management System
Web Portal	X	
Script Manager	X	
Security Console		X
XML API	X	

## Administrative domain device modes

An administrative domain has two device modes: normal and advanced. In normal mode, you cannot assign different FortiGate VDOMs to multiple FortiManager administrative domains. Only the FortiGate unit can be added to an administrative domain.

In advanced mode, you can assign different VDOMs from the same FortiGate unit to multiple administrative domains.

To change to a different mode, use the following commands in the CLI:

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

Normal mode is the default. To change from advanced back to normal, you must ensure none of the FortiGate VDOMs are assigned to an administrative domain.

## Configuring ADOMs

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



**Caution:** 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 ADOMs

Enter the following CLI command:

```
configure fmsystem global
  set adom-status enable
end
```

### To assign an administrator to an ADOM

Enter the following CLI command:

```
configure 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.



# fcdevice

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

This chapter contains following sections:

[group](#)

[temp](#)

[ungroup](#)

[unit](#)

[unlicensed](#)

## group

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

### Syntax

```
config fcdevice group
  edit <name>
    set comment <string>
    set dns_domain <domain_name>
    set fmgaddr <fmgr_ip>
    set fmg_sn <serno>
    set ip_address <ip>
    set member <name>
    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
```

Keywords and variables	Description	Default
edit <name>	Add or modify a FortiClient PC group.	No default.
comment <string>	Enter a description for this group. Enclose the description in quotes if it contains spaces.	No default.
dns_domain <domain_name>	If policy is dns_domain, enter the DNS domain name.	No default.
fmgaddr <fmgr_ip>	Enter the IP Address of the FortiManager server.	0.0.0.0
fmg_sn <serno>	Enter the serial number of the FortiManager server.	No default.
ip_address <ip>	If policy is ip_address, enter one of: IP address, for example "192.168.1.2" IP address range, for example "192.168.1.2-192.168.1.5" Subnet address, for example "192.168.1.0/24"	No default.
member <name>	If policy is static, enter the device names to be included in the group.	No default.
order <order-int>	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.	Set on creation.
os_name <os-name>	If policy is os, enter the OS name.	No default.
policy {dnsdomain   ip_address   os   windows_group}	If type is dynamic, select criterion for group membership: dnsdomain — DNS domain ip_address — IP Address os — Operating system type windows_group — Windows Group	No default.
parent <grp_name>	If this is a nested group, enter the parent group name.	No default.
type {dynamic   static}	Select a group type. static - specify members by name dynamic - define membership by DNS domain, IP address, OS type or Windows group.	static
windows_group <wingrpname>	If policy is windows_group, enter the Windows workgroup or domain name.	No default.

## History

<b>FortiManager v3.0</b>	New.
<b>FortiManager v3.0 MR4</b>	Removed end-ip, iprange, netmask, priority, start-ip, subnet. Added ip_address, windows_group.
<b>FortiManager v3.0 MR5</b>	Added fmg_addr, fmg_sn, order, parent.
<b>FortiManager v3.0 MR6</b>	Changed fmg_addr to fmgaddr
<b>FortiManager v4.0</b>	Added enterprise client license keyword and policy option.
<b>FortiManager v4.0 MR1</b>	Removed enterprise client license keyword and policy option.

## Related topics

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

## temp

Use this command to list FortiClient PCs 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
```

Keywords	Description
<host_name>	FortiClient PC host name
dns_domain	The PC's DNS domain name.
ip <ip>	The PC's IP address.
uid	The PC's UID.

### History

**FortiManager v3.0** New.

**FortiManager v3.0 MR4** Now a `get` command only.

### Related topics

- [fcdevice addtomanaged](#)

## ungroup

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

### Syntax

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

Keywords and variables	Description	Default
edit <name>	Modify a FortiClient PC. You can only modify description. All other keywords are read-only.	No default.
description <string>	Enter a comment of up to 255 bytes.	No default.

```
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
version            : 3.0.395
windows_group      : WORKGROUP
```

### History

**FortiManager v3.0 MR4** New.

### Related topics

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

## unit

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

### Syntax

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

Keywords and variables	Description	Default
description <string>	Enter a description for this PC. Enclose the description in quotes if it contains spaces.	No default.
edit <host_name>	Edit the PC.	

```
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
ip                  : 172.20.120.54
last_connection     : 2007-08-14 20:38:47
online              : yes
os_name             : Windows 2000 Service Pack 4
sn                  : FCT9003215254778
status_av           : enable
status_firewall     : enable
status_vpn          : enable
version             : 3.0.395
windows_group       : TECHDOC
```

### History

**FortiManager v3.0** New.

**FortiManager v3.0 MR5** comment changed to description. Removed option.

### Related topics

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

## unlicensed

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

### Syntax

```
get fcdevice unlicensed
```

### History

<b>FortiManager v4.0</b>	New.
--------------------------	------



# fmclient

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

This chapter contains following sections:

- [client\\_license](#)
- [cluster secondary](#)
- [cluster setting](#)
- [communication\\_setting](#)
- [discovery](#)
- [emailalert](#)
- [enterprise\\_license](#)
- [group\\_admin](#)
- [ldap\\_users](#)
- [ldapsetting](#)
- [license\\_key](#)
- [lockdown](#)
- [systemsetting](#)
- [webfilter\\_profile](#)

## client\_license

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

Keywords and variables	Description	Default
<name>	Enter a name for this client license.	No default.
description <string>	Optionally, enter a description.	No default.
emailaddress <string>	Enter the email address for the contact person.	No default.
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.	null
groupid <integer>	Enter the group id number. To find the number, enter this keyword followed by a ?.	No default.
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.	0
status {enable   disable}	Enable or disable this license.	disable
username <string>	Enter the user name for the license key.	No default.

### History

**FortiManager v3.0 MR7** New.

**FortiManager v4.0 MR1** Added emailaddress, groupid and username keywords.

### Related topics

- [execute fmclient enterprise\\_license download](#)
- [execute fmclient enterprise\\_license list](#)
- [fmclient enterprise\\_license](#)

## 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 [“fmclient cluster setting” on page 46](#).

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
```

Keywords and variables	Description	Default
<sec_fmgr_serno>	The serial number of the secondary FortiManager unit.	No default
enable {enable   disable}	Enable or disable this unit as a secondary cluster member.	disable

### History

**FortiManager v3.0 MR5**      New.

### Related topics

- [fmclient cluster setting](#)
- [execute fmclient cluster](#)

## 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 PCs. 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 PC 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 PC, even if that PC 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 [fmclient cluster secondary](#) command to register each secondary unit.

### Syntax

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

Keywords and variables	Description	Default
cluster_enable {enable   disable}	Enable or disable clustering.	enable
cluster_role {primary   secondary}	Select whether this FortiManager unit is a primary or secondary FortiClient Manager. This is available only when cluster_enable is set to enable.	primary
primary_ip <ip4>	Enter the IP address of the primary FortiManager unit. This is available only if cluster_role is secondary.	0.0.0.0

### History

**FortiManager v3.0 MR5**      New.

### Related topics

- [fmclient cluster secondary](#)
- [execute fmclient cluster](#)

## communication\_setting

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

### 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
```

Keywords and variables	Description	Default
action_queue_interval <q1,q2,q3,q4>	Set sending interval in seconds of each message queue. <b>q1</b> — Deploy/retrieve messages <b>q2</b> — Lockdown/License key messages <b>q3</b> — Patch update messages <b>q4</b> — AV update messages	60,60, 120,180
action_queue_length <q1,q2,q3,q4>	Set length of each message queue. <b>q1</b> — Deploy/retrieve messages <b>q2</b> — Lockdown/License key messages <b>q3</b> — Patch update messages <b>q4</b> — AV update messages	300,1500, 60,60
disable_auto_vaccum {yes   no}	By default, the FortiManager database performs periodic cleanup operations to maintain performance. You can disable this feature.	no
min_message_interval <seconds>	Minimum interval, in seconds, allowed for two continuous messages.	0

### History

**FortiManager v3.0 MR7** New.

**FortiManager v4.0** `action_queue_length` default changed from 200,3000,120,120.

## discovery

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

### Syntax

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

Keywords and variables	Description	Default
accept_ports {port1 port2...portn}	Enter FortiManager ports that will accept requests for management from FortiClient PCs. Separate port names with spaces.	No default.
newclient_action {add-to-temp   auto-pop}	Select add-to-temp to add new discovered FortiClient PCs to temporary clients list, and auto-pop to display the discovered FortiClient PCs in the managed clients list.	auto-pop

### History

**FortiManager v3.0** New.

**FortiManager v3.0 MR7** Replaced broadcast\_ports and unicast\_ports with accept\_ports.

## 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_event {enable | disable}
  set smtpserver <mail_server>
  set use_auth {enable | disable}
  set username <string>
end
```

Keywords and variables	Description	Default
admin_email <email_addr>	Enter the email address of the person who will receive alerts.	No default.
enable_email_alert {enable   disable}	Enable sending of alert email.	disable
fromaddr <from_addr>	Enter the reply-to address to provide in alert email messages.	No default.
password <string>	If use_auth is enable, enter the sender email account password.	No default.
port <port_num>	Enter the port number that the mail server uses.	25
secure_connection {None   TLS}	Select secure TLS connection or non-secured connection.	None
send_alert {enable   disable}	Enable sending management alerts.	enable
send_event {enable   disable}	Enable sending management events.	disable
smtpserver <mail_server>	Enter the SMTP mail server IP address or fully qualified domain name.	No default.
use_auth {enable   disable}	Set to enable if the mail server requires authentication.	disable
username <string>	If use_auth is enable, enter the sender email account user name.	No default.

### History

**FortiManager v4.0.0**      New.

## enterprise\_license

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

### Syntax

```
config fmclient enterprise_license
  set external_url <url>
  set model {redistribute | standard | volume}
  set validation_type {internal | external}
end
```

Keywords and variables	Description	Default
external_url <url>	If validation_type is external, enter the validation facility URL.	No default.
model {redistribute   standard   volume}	Set the type of license model.	No default.
validation_type {internal   external}	Set validation type for client license key: internal — Validate on FortiManager unit. external — Validate through external facility.	internal

### History

<b>FortiManager v3.0 MR7</b>	New.
<b>FortiManager v4.0 MR1</b>	Added model keyword.

### Related topics

- [execute fmclient enterprise\\_license download](#)
- [execute fmclient enterprise\\_license list](#)
- [fmclient client\\_license](#)

## 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
```

Keywords and variables	Description	Default
<name>	Enter the name of the administrator. The administrator must not have the Super_User administrative profile.	No default.
group group1[,group2][,groupn]	Enter the names of one or more client groups. Separate group names with commas.	No default.
option {none   access_ungroup}	Set option to access_ungroup to enable this group administrator to configure ungrouped clients. Otherwise, set option to none.	none

### History

**FortiManager v3.0 MR7** New.

## 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 [fmclient ldapsetting](#) command and then run the [execute fmclient sync-ldap](#) command to retrieve user and group information.

### Syntax

```
config fmclient ldap_users
    edit <dn>
        set webfilter-profile <profile_name>
    end
```

Keywords and variables	Description	Default
edit <dn>	Enter the distinguished name (DN) for this LDAP user.	
webfilter-profile <profile_name>	Enter the web filter profile for this user. The profile must be configured in <a href="#">fmclient webfilter_profile</a> .	No default.

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
```

### History

**FortiManager v3.0 MR5**    New.

### Related topics

- [fmclient ldapsetting](#)
- [execute fmclient sync-ldap](#)
- [fmclient webfilter\\_profile](#)

## 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 [execute 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
```

Keywords and variables	Description	Default
edit <srvname>	Enter a name for this LDAP server.	
base_dn <basedn>	Enter the base distinguished name for the LDAP server. (Maximum 255 characters)	No default.
bind_dn <binddn>	Enter the bind distinguished name for the LDAP server. (Maximum 255 characters)	No default.
ldap_host <hostaddr>	Enter the IP address or host name of the LDAP server.	No default.
ldap_port <portno>	Enter the port number for the LDAP server.	389
password <pwd_str>	Enter the password for authenticated access to the LDAP server.	No default.

### History

**FortiManager v3.0 MR5** New.

**FortiManager v3.0 MR7** Maximum length for `bind_dn` and `base_dn` increased from 64 to 255 characters.

### Related topics

- [execute fmclient sync-ldap](#)
- [fmclient ldap\\_users](#)
- [fmclient webfilter\\_profile](#)

## 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 <grpl_id grpn_id>
  end
```

Keywords and variables	Description	Default
edit <lic_key>	Enter the license key.	
comment <comment_str>	Optionally enter a description or comment.	No default.
groups <grpl_id grpn_id>	Enter the IDs of client groups licensed with this key. To list client group IDs and names, enter <code>set groups ?</code>	No default.

### History

**FortiManager v3.0 MR6** New.

## lockdown

Use this command to configure FortiClient lockdown through the FortiManager unit. With the lock-down enabled, all configuration on the managed FortiClient PCs 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
```

Keywords and variables	Description	Default
password <passwd>	Enter the lockdown password.	
status {enable   disable}	Disable or enable lockdown setting.	disable

### History

<b>FortiManager v3.0</b>	New.
<b>FortiManager v3.0 MR6</b>	display keyword removed. There is no longer a lockdown warning message.

## 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
```

Keywords and variables	Description	Default
debug_timing {enable   disable}	Enable debug timing to support performance monitoring.	disable
grouping_skip_static {yes   no}	Select yes to skip searching members of static groups when forming dynamic groups.	no
log_level <log_level>	Set logging level. 0 = error, 1 = information, 2 = debug	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.	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.	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.	no
update_for_unmanaged {enable   disable}	Select to provide antivirus update services for unmanaged FortiClient installations.	disable

### History

**FortiManager v3.0 MR5** New.

**FortiManager v4.0** Added monitor\_eventlogging\_duration keyword.

**FortiManager v4.0 MR1** Added update\_for\_unmanaged keyword.

## 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
```

Keywords and variables	Description	Default
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 set blocked_categories?	No default.
blocked_classification {class1,class2, ...classn}	Enter a comma-separated list of FortiGuard classifications to block. For a list of classifications, enter set blocked_classification?	No default.
blocked_urls {url1,url2,...urln}	Enter a comma-separated list of URLs to always block, regardless of FortiGuard ratings.	No default.
bypassed_urls {url1,url2,...urln}	Enter a comma-separated list of URLs that are not subject to web filtering.	No default.
comments <string>	Optionally, enter a descriptive comment about this profile.	No default.

### History

**FortiManager v3.0 MR5** New.

**FortiManager v3.0 MR6** Added blocked\_classification keyword.

### Related topics

- [fmclient ldapsetting](#)
- [execute fmclient sync-ldap](#)
- [fmclient ldap\\_users](#)



# fmupdate

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

This chapter contains following sections:

[analyzer virusreport](#)

[av-ips advanced-log](#)

[av-ips fct server-override](#)

[av-ips fgt server-override](#)

[av-ips push-override](#)

[av-ip push-override-to-client](#)

[av-ips update-schedule](#)

[av-ips web-proxy](#)

[disk-quota](#)

[device-version](#)

[fct-services](#)

[publicnetwork](#)

[server-access-priorities](#)

[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
```

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

### Example

This example enables virus detection notifications to Fortinet.

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

### History

**FortiManager v3.0 MR3** New.

## 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
```

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

### History

**FortiManager v3.0 MR1** New.

**FortiManager v4.0 MR1** Removed log-forticlient.

## 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 FortiGuard Distribution Network (FDN).

### Syntax

```
config fmupdate av-ips fct server-override
  set ip <FDNserver_ipv4>
  set port <port_int>
  set status {enable | disable}
end
```

Variables	Description	Default
ip <FDNserver_ipv4>	Enter the IP address of the preferred FDN server.	0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDN.	443
status {enable   disable}	Enable or disable the override.	disable

### 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
  set ip 192.168.25.152
  set port 80
end
```

### History

**FortiManager v3.0** New.

## 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 FortiGuard Distribution Network (FDN).

### Syntax

```
config fmupdate av-ips fgt server-override
  set ip <FDNserver_ipv4>
  set port <port_int>
  set status {enable | disable}
end
```

Variables	Description	Default
ip <FDNserver_ipv4>	Enter the IP address of the preferred FDN server.	0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDN.	443
status {enable   disable}	Enable or disable the override.	disable

### 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
  set ip set ip 172.27.152.144
  set port 8890
end
```

### History

**FortiManager v3.0** New.

## 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
```

Variables	Description	Default
ip <recipientaddress_ipv4>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiManager unit.	0.0.0.0
port <recipientport_int>	Enter the receiving port number on the NAT device.	9443
status {enable   disable}	Enable or disable the push updates.	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.

### History

## av-ip 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 <recipientaddress_ipv4>
    set port <recipientport_int>

end
```

Variables	Description	Default
status {enable   disable}	Enable or disable the push updates.	disable
announce-ip	Config the ip information of the device.	
<id>	Edit the ip information of the device.	
ip <recipientaddress_ipv4>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiManager unit.	0.0.0.0
port <recipientport_int>	Enter the receiving port number on the NAT device.	9443

### Example

### History

FortiManager v4.0 MR2    New

## 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 day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday |
    Saturday}
  set frequency {every | daily | weekly}
  set status {enable | disable}
  set time <hh:mm>
end
```

Variables	Description	Default
day {Sunday   Monday   Tuesday   Wednesday   Thursday   Friday   Saturday}	Enter the day of the week when the update will begin. This option only appears when the frequency is weekly.	Monday
frequency {every   daily   weekly}	Enter to configure the frequency of the updates.	every
status {enable   disable}	Enable or disable regularly scheduled updates.	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.	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 update-schedule
  set status enable
  set frequency every
  set time 05:60
end
```

### History

**FortiManager v3.0 MR1** New.

**FortiManager v3.0 MR5** Added day keyword.

## 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 password <passwd_str>
  set port <port_int>
  set status {enable | disable}
  set username <username_str>
end
```

Variables	Description	Default
ip <proxy_ipv4>	Enter the IP address of the web proxy.	0.0.0.0
password <passwd_str>	If the web proxy requires authentication, enter the password for the user name.	No default.
port <port_int>	Enter the port number of the web proxy.	80
status {enable   disable}	Enable or disable connections through the web proxy.	disable
username <username_str>	If the web proxy requires authentication, enter the user name.	No default.

### 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 ip 10.10.30.1
  set port 8890
  set username avipsupdater
  set password cvhk3rf3u9jvsYU
end
```

### History

**FortiManager v3.0** New.

## 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
```

Variables	Description	Default
delaytime <integer>	Enter the delay time you want to use in the delay mode deployment.	60
mode {auto   delay   manual}	Set the mode of deployment. 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.	auto

### Example

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

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

### History

**FortiManager v4.0 MR2** New.

## 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
```

Variables	Description	Default
faz <firmware_version>	Enter the correct firmware version that is currently running on the FortiAnalyzer units.	No default
fct <firmware_version>	Enter the correct firmware version that is currently running for FortiClients.	No default
fgt <firmware_version>	Enter the correct firmware version that is currently running for FortiGate units.	No default
fml <firmware_version>	Enter the correct firmware version that is currently running for the FortiMail units.	No default
fsw <firmware_version>	Enter the correct firmware version that is currently running for the FortiSwitch units.	No default

### Example

In the following example, the FortiAnalyzer and FortiGate units, including FortiClients, are configured with the new firmware version 4.0.

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

### History

**FortiManager v4.0** New.

## 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 MBytes. The default size is 10 GBytes. 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.

### History

**FortiManager v3.0 MR7** New.

## 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
```

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

### History

**FortiManager v3.0** New.

## publicnetwork

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

### Syntax

```
config fmupdate publicnetwork
  set status {enable | disable}
end
```

Variables	Description	Default
status {enable   disable}	Enable or disable the publicnetwork.	enable

### Example

The following example shows how to enable public network.

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

### History

**FortiManager v4.2** New

## 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.



**Note:** 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 lookup_default_server {disable | enable}
  set web-spam {disable | enable}
end
```

Variables	Description	Default
access-public {disable   enable}	Disable to prevent FortiManager default connectivity to public FDS and FortiGuard servers.	enable
av-ips {disable   enable}	Enable to allow the FortiGate unit to get antivirus updates from other FortiManager units or private FDS servers.	disable
lookup_default_server {disable   enable}	Enable to allow to connect to the built-in FDS server.	disable
web-spam {disable   enable}	Disable to not have the FortiGate unit receive web filtering service from other FortiManager units and private FDS servers.	enable

### 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 <ipv4>
      set time_zone <integer>
    end
  end
```

Variables	Description	Default
<id>	Enter a number to identify the FortiManager unit or private server.	No default
<ipv4>	Enter the IP address of the FortiManager unit or private server.	No default
time_zone <integer>	Enter the correct time zone of the private server. Using -24 indicates that the server is using the local time zone.	No default.

### 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
```

## History

**FortiManager v3.0 MR7** New.

**FortiManager v4.0** Added the keyword, `time_zone`, to the `config private-server` subcommand.

## service

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

### Syntax

```
config fmupdate service
  set avips {enable | disable}
end
```

Variables	Description	Default
avips {enable   disable}	Enable the built-in FDS to provide FortiGuard Antivirus and IPS updates.	disable

### Example

```
config fmupdate service
  set avips enable
  set fct enable
  set web-spam enable
end
```

### History

**FortiManager v3.0 MR3** New.



# fmsystem

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

This chapter contains following sections:

<a href="#">admin ldap</a>	<a href="#">certificate local</a>	<a href="#">log fortianalyzer</a>
<a href="#">admin profile</a>	<a href="#">dm</a>	<a href="#">log setting</a>
<a href="#">admin radius</a>	<a href="#">dnsglobal</a>	<a href="#">log rolling</a>
<a href="#">admin setting</a>	<a href="#">ha</a>	<a href="#">metadata</a>
<a href="#">admin user</a>	<a href="#">interface</a>	<a href="#">ntp</a>
<a href="#">alert-console</a>	<a href="#">locallog disk setting</a>	<a href="#">ntpserver</a>
<a href="#">alertemail</a>	<a href="#">locallog filter</a>	<a href="#">performance</a>
<a href="#">alert-event</a>	<a href="#">locallog fortianalyzer setting</a>	<a href="#">route</a>
<a href="#">backup all-settings</a>	<a href="#">locallog memory setting</a>	<a href="#">snmp community</a>
<a href="#">certificate ca</a>	<a href="#">locallog syslogd (syslogd2, syslogd3) setting</a>	<a href="#">snmp sysinfo</a>
		<a href="#">status</a>

For more information about configuring ADOMs, see [Administrative Domains \(ADOMs\)](#).

## admin ldap

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

### Syntax

```
config fmsystem admin ldap
  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>
end
```

Keywords and variables	Description	Default
server {name_str   ip_str}	Enter the LDAP server name or IP address.	No default.
cnid <string>	Enter common name identifier.	cn
dn <string>	Enter the distinguished name.	No default.
port <integer>	Enter the port number for LDAP server communication.	389
type {anonymous   regular   simple}	Set a binding type: anonymous - bind using anonymous user search regular - bind using username/password and then search simple - simple password authentication without search	simple
username <string>	Enter a username. This keyword appears only when type is set to regular.	No default
password <string>	Enter a password for the username above. This keyword appears only when type is set to regular.	No default
group <string>	Enter an authorization group. The authentication user must be a member of this group (full DN) on the server.	No default
filter <query_string>	Enter contnet for group searching. For example: ( &(objectcategory=group)(member=*) ) ( &(objectclass=groupofnames)(member=*) ) ( &(objectclass=groupofuniquenames)(unique member=*) ) ( &(objectclass=posixgroup)(memberuid=*) )	No default

### 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
```

## History

FortiManager v4.0 MR1 New.

## Related topics

- [fmsystem 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 deploy-management {none | read | read-write}
    set description <text>
    set devcfg-adminuser {none | read | read-write}
    set devcfg-authuser {none | read | read-write}
    set devcfg-avconfig {none | read | read-write}
    set devcfg-fgdupdate {none | read | read-write}
    set devcfg-fw-address {none | read | read-write}
    set devcfg-fw-other {none | read | read-write}
    set devcfg-fw-policy {none | read | read-write}
    set devcfg-fw-profile {none | read | read-write}
    set devcfg-fw-schedule {none | read | read-write}
    set devcfg-fw-service {none | read | read-write}
    set devcfg-ipsconfig {none | read | read-write}
    set devcfg-logreport {none | read | read-write}
    set devcfg-maintenance {none | read | read-write}
    set devcfg-netconfig {none | read | read-write}
    set devcfg-routerconfig {none | read | read-write}
    set devcfg-spamfilter {none | read | read-write}
    set devcfg-sysconfig {none | read | read-write}
    set devcfg-vpnconfig {none | read | read-write}
    set devcfg-webfilter {none | read | read-write}
    set device-op {none | read-write}
    set device-summary {none | read | read-write}
    set faz-management {none | read | read-write}
    set fct-manager {none | read | read-write}
    set fgd-center {none | read-write}
    set firmware-management {none | read | read-write}
    set fmwimage-database {none | read-write}
    set global-storage {none | read | read-write}
    set group-op {none | read-write}
    set read-passwd {none | read-write}
    set realtime-monitor {none | read | read-write}
    set script-database {none | read-write}
    set script-management {none | read | read-write}
    set security-console {none | read | read-write}
    set service-usage {none | read | read-write}
    set system-setting {none | read-write}
    set vpn-manager {none | read | read-write}
    set web-portal {none | read | read-write}
    set av_read {conf_config conf_grayware fileblock quar_autosubmit
      quar_config}
    set av_write {conf_config conf_grayware fileblock quar_autosubmit
      quar_config}
    set firewall_read {address address_group ippool policy profile
      schedule_onetime schedule_recurring service service_group vip}
```

```
set firewall_write {address address_group ippool policy profile
  schedule_onetime schedule_recurring service service_group vip}
set fullaccess {enable | disable}
set global_privileges {admin devconf devices devop groups profile
  revision session system}
set imp2p_read {user policy}
set imp2p_write {user policy}
set ips_read {anomaly sig_custom sig_predefined}
set ips_write {anomaly sig_custom sig_predefined}
set logrep_read {alert_email filter setting}
set logrep_write {alert_email filter setting}
set logrepmgr_read {conarh_browse conarh_config conarh_search
  conarh_viewer fortianalyzer_config fortianalyzer_policy logs_browse
  logs_config logs_search logs_viewer reports_browse reports_config
  quarantine_config quarantine_repository security_config security_ips
  security_suspicious security_virus sys_alert_event sys_alert_snmp
  sys_alert_syslog sys_alias sys_config_log sys_config RAID sys_net_dns
  sys_net_intf sys_net_route sys_status traffic_email traffic_ftp
  traffic_im traffic_web}
set logrepmgr_write {conarh_browse conarh_config conarh_search
  conarh_viewer fortilog_config fortilog_policy logs_browse logs_config
  logs_search logs_viewer reports_browse reports_config
  quarantine_config quarantine_repository security_config security_ips
  security_suspicious security_virus sys_alert_event sys_alert_snmp
  sys_alert_syslog sys_alias sys_config_log sys_config RAID sys_net_dns
  sys_net_intf sys_net_route sys_status traffic_email traffic_ftp
  traffic_im traffic_web}
set other_read { deploy_manager forticlient_manager firmware_manager
  script_manager update_manager vpn_manager}
set other_write { deploy_manager forticlient_manager firmware_manager
  script_manager update_manager vpn_manager}
set realtime_read { global rtm_dashboard }
set realtime_write { global rtm_dashboard }
set router_read {dyna_bgp dyna_mcast dyna_ospf dyna_rip obj_accesslist
  obj_keychain obj_prefixlist obj_routemap policy_router rip_distlist
  rip_general rip_interface rip_networks rip_offlist static}
set router_write {dyna_bgp dyna_ospf dyna_rip obj_accesslist
  obj_keychain obj_prefixlist obj_routemap policy_router rip_distlist
  rip_general rip_interface rip_networks rip_offlist static}
set spamf_read {antispam banned dns email ip mime}
set spamf_write {antispam banned dns email ip mime}
set system_read {admin_access_profile admin_administrators auto_isntall
  config_ha config_mode config_options config_replacement_messages
  config_snmp config_time device_status dhcp_exclude_range
  dhcp_ipmac_binding dhcp_server dhcp_service maintenance net_dns
  net_interface net_modem net_routing_table net_zone virtual_domain
  wireless_config wireless_mac_filter}
set system_write {admin_access_profile admin_administrators auto_install
  config_ha config_mode config_options config_replacement_messages
  config_snmp config_time device_status dhcp_exclude_range
  dhcp_ipmac_binding dhcp_server dhcp_service maintenance net_dns
  net_interface net_modem net_routing_table net_zone virtual_domain
  wireless_config wireless_mac_filter}
set user_read {ldap radius user user_group windows_ad}
```

```

set user_write {ldap radius user user_group windows_ad}
set vpn_read {certificate ipsec_concentrator ipsec_manualkey
  ipsec_phase1 ipsec_phase2 ipsec_pinggen l2tp pptp ssl_setting}
set vpn_write {certificate ipsec_concentrator ipsec_manualkey
  ipsec_phase1 ipsec_phase2 ipsec_pinggen l2tp pptp ssl_setting}
set webf_read {category_block content_block content_exempt
  fgd_localcategory fgd_localrating fgd_override list_management
  script_block url_exempt web_pattern_block web_url_block}
set webf_write {category_block content_block content_exempt
  fgd_localcategory fgd_localrating fgd_override list_management
  script_block url_exempt web_pattern_block web_url_block}

end

```

Keywords and variables	Description
edit <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.
av_read {conf_config conf_grayware fileblock quar_autosubmit quar_config}	Permit read access to the listed Anti-Virus configurations in the Policy Manager and Device Manager.
conf_config	Config > Config
conf_grayware	Config > Grayware
fileblock	File Block
quar_autosubmit	Quarantine > Autosubmit
quar_config	Quarantine > Config
av_write {conf_config conf_grayware fileblock quar_autosubmit quar_config}	Permit write access to the listed antivirus configurations in the Policy Manager and Device Manager.
conf_config	Config > Config
conf_grayware	Grayware - categories
fileblock	File Block
quar_autosubmit	Quarantine > Autosubmit
quar_config	Quarantine > Config
deploy-management {none   read   read-write}	Enter the level of access to the deployment management configuration settings for this profile.
description <text>	Enter a description for this access profile. Enclose the description in quotes if it contains spaces.
devcfg-adminuser {none   read   read-write}	Enter the level of access to admin user configurations for this profile.
devcfg-authuser {none   read   read-write}	Enter the level of access to authenticated user configurations for this profile.
devcfg-avconfig {none   read   read-write}	Enter the level of access to antivirus configuration settings for this profile.
devcfg-fgdupdate {none   read   read-write}	Enter the level of access to FortiGuard update configurations for this profile.
devcfg-fw-address {none   read   read-write}	Enter the level of access to firewall address configuration settings for this profile.
devcfg-fw-other {none   read   read-write}	Enter the level of access to other configuration settings for this profile, such as the VPN manager, FortiClient manager, and Script manager.
devcfg-fw-policy {none   read   read-write}	Enter the level of access to firewall policy configuration settings for this profile.

Keywords and variables	Description
devcfg-fw-profile {none   read   read-write}	Enter the level of access to firewall profile configuration settings for this profile.
devcfg-fw-schedule {none   read   read-write}	Enter the level of access to firewall schedule configuration settings for this profile.
devcfg-fw-service {none   read   read-write}	Enter the level of access to firewall service configuration settings for this profile.
devcfg-ipsconfig {none   read   read-write}	Enter the level of access to IPS configuration settings for this profile.
devcfg-logreport {none   read   read-write}	Enter the level of access to log reporting configuration settings for this profile.
devcfg-maintenance {none   read   read-write}	Enter the level of access to device maintenance details for this profile.
devcfg-netconfig {none   read   read-write}	Enter the level of access to network configuration settings for this profile.
devcfg-routerconfig {none   read   read-write}	Enter the level of access to router configuration settings for this profile.
devcfg-spamfilter {none   read   read-write}	Enter the level of access to spam filter configuration settings for this profile.
devcfg-sysconfig {none   read   read-write}	Enter the level of access to system configuration settings for this profile.
devcfg-vpnconfig {none   read   read-write}	Enter the level of access to VPN configuration settings for this profile.
devcfg-webfilter {none   read   read-write}	Enter the level of access to web filter configuration settings for this profile.
device-op {none   read-write}	Add the capability to add, delete, and edit devices to this profile.
device-summary {none   read   read-write}	Enter the level of access to device summary details for this profile.
faz-management {none   read   read-write}	Enter the level of access to FortiAnalyzer configuration management settings for this profile.
fct-manager {none   read   read-write}	Enter the level of access to the FortiClient manager configuration settings for this profile.
fgd-center {none   read-write}	Enter the level of access to FortiGuard Center for this profile.
firmware-management {none   read   read-write}	Enter the level of access to firmware management configuration settings for this profile.
fmwimage-database {none   read-write}	Enter the level of access to firmware images for this profile.
global-storage {none   read   read-write}	Enter the level of access to global object storage configuration settings for this profile.
group-op {none   read-write}	Add the capability to add, delete, and edit groups to this profile.
read-passwd {none   read-write}	Add the capability to view the authentication password in clear text to this profile.
realtime-monitor {none   read   read-write}	Enter the level of access to the Real-Time monitor configuration settings for this profile.
script-database {none   read-write}	Enter the level of access to script databases for this profile.

Keywords and variables	Description	
script-management {none   read   read-write}	Enter the level of access to the Script manager configuration settings for this profile.	
security-console {none   read   read-write}	Enter the level of access to security console configuration settings for this profile.	
service-usage {none   read   read-write}	Enter the level of access to the service usage configuration settings for this profile.	
system-setting {none   read-write}	Enter the level of access to system settings for this profile.	
vpn-manager {none   read   read-write}	Enter the level of access to VPN console configuration settings for this profile.	
web-portal {none   read   read-write}	Enter the level of access to web portal configuration settings for this profile.	
firewall_read {address address_group ippool policy profile schedule_onetime schedule_recurring service service_group vip}	Permit write access to the listed Firewall configurations in the Policy Manager and Device Manager.	
	address	Address
	address_group	Address Group
	ippool	IP Pool
	policy	Policy
	profile	Protection Profile
	schedule_onetime	Schedule > One-Time
	schedule_recurring	Schedule > Recurring
	service	Service
	service_group	Service > Group
firewall_write {address address_group ippool policy profile schedule_onetime schedule_recurring service service_group vip}	Permit write access to the listed firewall configurations in the Policy Manager and Device Manager.	
	address	Address
	address_group	Address > Address Group
	ippool	IP Pool
	policy	Policy
	profile	Protection Profile
	schedule_onetime	Schedule > One-Time
	schedule_recurring	Schedule > Recurring
	service	Service
	service_group	Service > Group
fullaccess {enable   disable}	Enable for read-write access to all devices and device groups.	

Keywords and variables	Description	
global_privileges {admin devconf devices devop groups profile revision session system}	Enable the listed global privileges.	
	admin	Add / Delete / Edit Administrators sysconf should be set as well.
	devconf	View / Download Device Configuration
	devices	Add / Delete / Edit Devices
	devop	Install / Re-sync Devices
	groups	Add / Delete / Edit Groups
	profile	Add / Delete / Edit Admin Profiles sysconf should be set as well.
	revision	Create/check out/delete revisions
	session	View / Edit user sessions sysconf should be set as well.
	system	System Settings If profile, admin or session are set, sysconf should be set as well.
imp2p_read {user policy}	Permit read access to the following methods of Instant Messaging (IM) and Peer-to-Peer (P2P) regulation:	
	user	by user
	policy	by policy
imp2p_write {user policy}	Permit write access to the following methods of Instant Messaging (IM) and Peer-to-Peer (P2P) regulation.	
	user	by user
	policy	by policy
ips_read {anomaly sig_custom sig_predefined}	Permit read access to the following IPS configurations in the Policy Manager and Device Manager.	
	anomaly	Anomaly
	sig_custom	Signatures > Custom
	sig_predefined	Signatures > Predefined
ips_write {anomaly sig_custom sig_predefined}	Permit write access to the following IPS configurations in the Policy Manager and Device Manager.	
	anomaly	Anomaly
	sig_custom	Signatures > Custom
	sig_predefined	Signatures > Predefined
logrep_read {alert_email filter setting}	Permit read access to the following Log & Report configurations in the Policy and Device Manager.	
	alert_email	Log Config > Alert E-mail
	filter	Log Config > Log Filter
	setting	Log Config > Log Setting
logrep_write {alert_email filter setting}	Permit write access to the following Log & Report configurations in the Policy and Device Manager.	
	alert_email	Log Config > Alert E-mail
	filter	Log Config > Log Filter
	setting	Log Config > Log Setting

Keywords and variables	Description	
logrepmgr_read {conarh_browse conarh_config conarh_search conarh_viewer fortianalyzer_config fortianalyzer_policy logs_browse logs_config logs_search logs_viewer reports_browse reports_config quarantine_config quarantine_repository security_config security_ips security_suspicious security_virus sys_alert_event sys_alert_snmp sys_alert_syslog sys_alias sys_config_log sys_config_raid sys_net_dns sys_net_intf sys_net_route sys_status traffic_email traffic_ftp traffic_im traffic_web}	Permit read access to the following Log & Report Manager configurations	
	conarh_browse	Content archive browse
	conarh_config	Content archive settings
	conarh_search	Content archive search
	conarh_viewer	Content archive viewer
	fortianalyzer_config	FortiAnalyzer settings
	fortianalyzer_policy	FortiAnalyzer log policy
	logs_browse	Logs browse
	logs_config	Logs settings
	logs_search	Logs search
	logs_viewer	Logs viewer
	reports_browse	Reports browse
	reports_config	Reports settings
	quarantine_config	Quarantine settings
	quarantine_repository	Quarantine repository
	security_config	Security events config
	security_ips	Security events IPS
	security_suspicious	Security events suspicious
	security_virus	Security events virus
	sys_alert_event	System alerts event
	sys_alert_snmp	System alerts SNMP
	sys_alert_syslog	System alerts syslog
	sys_alias	System IP alias
	sys_config_log	System config log
	sys_config_raid	System config raid
	sys_net_dns	System network DNS
	sys_net_intf	System network interface
	sys_net_route	System network route
	sys_status	System status
	traffic_email	Traffic summary email
	traffic_ftp	Traffic FTP
	traffic_im	Traffic IM
	traffic_web	Traffic web

Keywords and variables	Description	
logrepmgr_write {conarh_browse conarh_config conarh_search conarh_viewer fortilog_config fortilog_policy logs_browse logs_config logs_search logs_viewer reports_browse reports_config quarantine_config quarantine_repository security_config security_ips security_suspicious security_virus sys_alert_event sys_alert_snmp sys_alert_syslog sys_alias sys_config_log sys_config_raid sys_net_dns sys_net_intf sys_net_route sys_status traffic_email traffic_ftp traffic_im traffic_web}	Permit write access to the following Log & Report Manager configurations	
	conarh_browse	Content archive browse
	conarh_config	Content archive settings
	conarh_search	Content archive search
	conarh_viewer	Content archive viewer
	fortianalyzer_config	FortiAnalyzer settings
	fortianalyzer_policy	FortiAnalyzer log policy
	logs_browse	Logs browse
	logs_config	Logging settings
	logs_search	Logs search
	logs_viewer	Logs viewer
	reports_browse	Reports browse
	reports_config	Reports settings
	quarantine_config	Quarantine configure
	quarantine_repository	Quarantine repository
	security_config	Security configure
	security_ips	Security IPS
	security_suspicious	Security suspicious
	security_virus	Security virus
	sys_alert_event	System alert event
	sys_alert_snmp	System alert SNMP
	sys_alert_syslog	System alert syslog
	sys_alias	System alias
	sys_config_log	System configure log
	sys_config_raid	System configure RAID
	sys_net_dns	System network DNS
	sys_net_intf	System network interface
	sys_net_route	System network route
	sys_status	System Dashboard
	traffic_email	Traffic email
	traffic_ftp	Traffic FTP
	traffic_im	Traffic IM
	traffic_web	Traffic web
other_read { deploy_manager forticlient_manager firmware_manager script_manager update_manager vpn_manager}	Permit read access to the following other all-or-none configurations	
	deploy_manager	Deployment Manager
	forticlient_manager	FortiClient Manager
	firmware_manager	Firmware Manager
	script_manager	Script Manager
	update_manager	Update Manager
	vpn_manager	VPN Manager

Keywords and variables	Description	
other_write { deploy_manager forticlient_manager firmware_manager script_manager update_manager vpn_manager}	Permit write access to the following other all-or-none configurations	
	deploy_manager	Deployment Manager
	forticlient_manager	FortiClient Manager
	firmware_manager	Firmware Manager
	script_manager	Script Manager
	update_manager	Update Manager
	vpn_manager	VPN Manager
realtime_read { global rtm_dashboard }	Permit read access to the following Realtime Monitor configurations	
	alert_profiles	Alert profiles
	global	Global settings
	rtm_dashboard	Realtime Monitor dashboard settings
realtime_write { global rtm_dashboard }	Permit write access to the following Realtime Monitor configurations	
	alert_profiles	Alert profiles
	global	Global settings
	rtm_dashboard	Realtime Monitor dashboard settings
router_read {dyna_bgp dyna_mcast dyna_ospf dyna_rip obj_accesslist obj_keychain obj_prefixlist obj_routemap policy_router rip_distlist rip_general rip_interface rip_networks rip_offlist static}	Permit read access to the following Router configurations in the Policy Manager and Device Manager	
	dyna_bgp	Dynamic > BGP
	dyna_mcast	Dynamic > Multicast
	dyna_ospf	Dynamic > OSPF
	dyna_rip	Dynamic > RIP
	obj_accesslist	Router Objects > Access List
	obj_keychain	Router Objects > Key-chain
	obj_prefixlist	Router Objects > Prefix List
	obj_routemap	Router Objects > Route-Map
	policy_router	Policy Route
	rip_distlist	RIP > Distribute List
	rip_general	RIP > General
	rip_interface	RIP > Interface
	rip_networks	RIP > Networks
	rip_offlist	RIP > Offset List
	static	Static > Static Route

Keywords and variables	Description	
router_write {dyna_bgp dyna_ospf dyna_rip obj_accesslist obj_keychain obj_prefixlist obj_routemap policy_router rip_distlist rip_general rip_interface rip_networks rip_offlist static}	Permit write access to the following router configurations in the Policy Manager and Device Manager	
	dyna_bgp	Dynamic > BGP
	dyna_ospf	Dynamic > OSPF
	dyna_rip	Dynamic > RIP
	obj_accesslist	Router Objects > Access List
	obj_keychain	Router Objects > Key-chain
	obj_prefixlist	Router Objects > Prefix List
	obj_routemap	Router Objects > Route-Map
	policy_router	Policy Route
	rip_distlist	RIP > Distribute List
	rip_general	RIP > General
	rip_interface	RIP > Interface
	rip_networks	RIP > Networks
	rip_offlist	RIP > Offset List
	static	Static > Static Route
spamf_read {antispam banned dns email ip mime}	Permit read access to the following Spam filter (Anti-Spam) configurations in the Policy Manager and Device Manager	
	antispam	FortiGuard - AntiSpam
	banned	Banned Word
	dns	DNSBL & ORDBL
	email	Email Address
	ip	IP Address
spamf_write {antispam banned dns email ip mime}	Permit write access to the following Spam filter (Anti-Spam) configurations in the Policy Manager and Device Manager	
	antispam	FortiGuard - AntiSpam
	banned	Banned Word
	dns	DNSBL & ORDBL
	email	Email Address
	ip	IP Address
	mime	MIME Headers

Keywords and variables	Description	
<pre> system_read {admin_access_profile admin_administrators auto_isntall config_ha config_mode config_options config_replacement_messages config_snmp config_time device_status dhcp_exclude_range dhcp_ipmac_binding dhcp_server dhcp_service maintenance net_dns net_interface net_modem net_routing_table net_zone virtual_domain wireless_config wireless_mac_filter} </pre>	Permit read access to the following System configurations in the Policy Manager and Device Manager	
	admin_access_profile	Admin > Access Profile
	admin_administrators	Admin > Administrators
	auto_install	Auto Install DH - build 260
	config_ha	Config > HA
	config_mode	Config > Mode (NAT/TP + Mgmt IP)
	config_options	Config > Options
	config_replacement_messages	Config > Replacement Messages
	config_snmp	Config > SNMP
	config_time	Config > Time
	device_status	Device Status DH - build 260
	dhcp_exclude_range	DHCP > Exclude Range
	dhcp_ipmac_binding	DHCP > IP/MAC Binding
	dhcp_server	DHCP > Server
	dhcp_service	DHCP > Service
	maintenance	Maintenance
	net_dns	Network > DNS
	net_interface	Network > Interface
	net_modem	Network > Modem (Models 50, 60 only)
	net_routing_table	Network > Routing Table (TP mode)
	net_zone	Network > Zone
	virtual_domain	Virtual Domain name
	wireless_config	Wireless > Config (WiFi models only)
	wireless_mac_filter	Wireless > Wireless MAC filter (WiFi models only)

Keywords and variables	Description	
system_write {admin_access_profile admin_administrators auto_install config_ha config_mode config_options config_replacement_messages config_snmp config_time device_status dhcp_exclude_range dhcp_ipmac_binding dhcp_server dhcp_service maintenance net_dns net_interface net_modem net_routing_table net_zone virtual_domain wireless_config wireless_mac_filter}	Permit write access to the following system configurations in the Policy and Device Manager	
	admin_access_profile	Admin > Access Profile
	admin_administrators	Admin > Administrators
	auto_install	Auto Install DH - build 260
	config_ha	Config > HA
	config_mode	Config > Mode (NAT/TP + Mgmt IP)
	config_options	Config > Options
	config_replacement_messages	Config > Replacement Messages
	config_snmp	Config > SNMP
	config_time	Config > Time
	device_status	Device Status DH - build 260
	dhcp_exclude_range	DHCP > Exclude Range
	dhcp_ipmac_binding	DHCP > IP/MAC Binding
	dhcp_server	DHCP > Server
	dhcp_service	DHCP > Service
	maintenance	Maintenance
	net_dns	Network > DNS
	net_interface	Network > Interface
	net_modem	Network > Modem (Models 50, 60 only)
	net_routing_table	Network > Routing Table (TP mode)
	net_zone	Network > Zone
	virtual_domain	Virtual Domain name
	wireless_config	Wireless > Config (WiFi models only)
	wireless_mac_filter	Wireless > Wireless MAC filter (WiFi models only)
user_read {ldap radius user user_group windows_ad}	Permit read access to the following user configurations in the Policy Manager and Device Manager	
	ldap	LDAP Server
	radius	Radius Server
	user	Local User
	user_group	User Group
	windows_ad	MS Windows Active Directory
user_write {ldap radius user user_group windows_ad}	Permit write access to the following user configurations in the Policy Manager and Device Manager	
	ldap	LDAP Server
	radius	Radius Server
	user	Local User
	user_group	User Group
	windows_ad	MS Windows Active Directory

Keywords and variables	Description	
vpn_read {certificate ipsec_concentrator ipsec_manualkey ipsec_phase1 ipsec_phase2 ipsec_pinggen l2tp pptp ssl_setting}	Permit read access to the following VPN configurations in the Policy Manager and Device Manager	
	certificate	Certificate DH - build 260
	ipsec_concentrator	IPSec > Concentrator
	ipsec_manualkey	IPSec > Manual Key
	ipsec_phase1	IPSec > Phase 1
	ipsec_phase2	IPSec > Phase 2
	ipsec_pinggen	IPSec > Ping Generator
	l2tp	L2TP
	pptp	PPTP
	ssl_setting	SSL setting DH - build 260
vpn_write {certificate ipsec_concentrator ipsec_manualkey ipsec_phase1 ipsec_phase2 ipsec_pinggen l2tp pptp ssl_setting}	Permit write access to the following VPN configurations in the Policy Manager and Device Manager	
	certificate	Certificate
	ipsec_concentrator	IPSec > Concentrator
	ipsec_manualkey	IPSec > Manual Key
	ipsec_phase1	IPSec > Phase 1
	ipsec_phase2	IPSec > Phase 2
	ipsec_pinggen	IPSec > Ping Generator
	l2tp	L2TP
	pptp	PPTP
	ssl_setting	SSL setting
webf_read {category_block content_block content_exempt fgd_localcategory fgd_localrating fgd_override list_management script_block url_exempt web_pattern_block web_url_block}	Permit read access to the following Web Filter configurations in the Policy Manager and Device Manager	
	category_block	Category Block
	content_block	Content Block
	content_exempt	Content exempt
	fgd_localcategory	FortiGuard Local Category
	fgd_localrating	FortiGuard Local Rating
	fgd_override	FortiGuard Override
	list_management	Web Content Block List > Management List
	script_block	Script Filter
	url_exempt	URL Exempt
	web_pattern_block	URL Block > Web Pattern Block
	web_url_block	URL Block > Web URL Block

Keywords and variables	Description	
webf_write {category_block content_block content_exempt fgd_localcategory fgd_localrating fgd_override list_management script_block url_exempt web_pattern_block web_url_block}	Permit write access to the following webfilter configurations in the Policy Manager and Device Manager	
	category_block	Category Block
	content_block	Content Block
	content_exempt	Content exempt
	fgd_localcategory	FortiGuard Local Category
	fgd_localrating	FortiGuard Local Rating
	fgd_override	FortiGuard Override
	list_management	Web Content Block List > Management List
	script_block	Script Filter
	url_exempt	URL Exempt
	web_pattern_block	URL Block > Web Pattern Block
	web_url_block	URL Block > Web URL Block

## History

**FortiManager v3.0** New.

**FortiManager v3.0 MR1** global\_privileges sysconf keyword removed, system keyword added  
other\_\* deployment\_manager and script\_manager keywords added  
realtime\_\* alertemail keyword removed  
system\_\* device\_status and autoinstall keywords added  
VPN\_\* certificate and ssh\_setting keywords added  
webf\_\* management\_list keyword added

**FortiManager v3.0 MR3** imp2p\_\* keyword added  
user\_\* windows\_ad keyword added  
webf\_\* content\_exempt, and fgd\_\* keywords added

**FortiManager v3.0 MR7** Added fullaccess command. Changed parameters for realtime\_read and realtime\_write.

**FortiManager v4.0** Complete revision to all admin profile variables except profile\_name and description.

## Related topics

- [fmsystem admin radius](#)

## admin radius

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

### Syntax

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

Keywords and variables	Description	Default
auth-type <auth_prot_type>	Enter the authentication protocol the RADIUS server will use. any — use any supported authentication protocol mschap2 chap pap	No default.
port <integer>	Enter the radius server port number.	1812
secret <passwd>	Enter the password to access the radius server.	No default.
server <string>	Enter the radius server DNS resolvable domain name or IP address.	No default.

### 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
```

### History

**FortiManager v3.0**      New.

**FortiManager v4.0**      Added auth-type variable.

### Related topics

- [fmsystem admin profile](#)

## admin setting

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

### Syntax

```
config fmsystem admin setting
  set admin_server_cert <admin_server_cert>
  set allow_register {enable | disable}
  set autosync {enable | disable}
  set autosync_interval <integer>
  set demo-mode {enable | disable}
  set device_locks {enable | disable}
  set device_sync_status {enable | disable}
  set http_port <integer>
  set https_port <integer>
  set idle_timeout <integer>
  set offline_mode {enable | disable}
  set register_passwd <password>
  set unreg_dev_opt {add_allow_service | add_no_service | ignore}
  set verify_serial_number {enable | disable}
  set webadmin_language {auto_detect | english | japanese |
    simplified_chinese | traditional_chinese}
end
```

Keywords and variables	Description	Default
admin_server_cert <admin_server_cert>	Enter the name of an https server certificate to use for secure connections.	server.crt
allow_register {enable   disable}	Enable an unregistered device to be registered.	disable
autosync {enable   disable}	Set the automatic synchrhonization of device configurations	disable
autosync_interval <integer>	Enter the time after the last device configuration to synchronize the device configuration.	No default.
demo-mode {enable   disable}	Enable demo mode.	disable
device_locks {enable   disable}	Enable or disable device locks. Locking a device prevents problems that can occur when two administrators make different changes to the same device at the same time.	disable
device_sync_status {enable   disable}	Enable or disable device synchronization status indication.	enable
http_port <integer>	Enter the HTTP port number for web administration.	80
https_port <integer>	Enter the HTTPS port number for web administration.	443
idle_timeout <integer>	Enter the idle timeout value. The range is from 1 to 480 minutes.	5
offline_mode {enable   disable}	Enable offline mode to shut down the protocol used to communicate with managed devices.	
register_passwd <password>	Enter the password to use when registering a device.	

Keywords and variables	Description	Default
unreg_dev_opt {add_allow_service   add_no_service   ignore}	Select action to take when an unregistered device connects to FortiManager. add_allow_service — Add unregistered devices and allow service requests. add_no_service — Add unregistered devices and deny service requests. ignore — Ignore unregistered devices.	add_allow_service
verify_serial_number {enable   disable}	Enable to disallow deployment if the FortiGate serial number does not match FortiManager database record.	disable
webadmin_language {auto_detect   english   japanese   simplified_chinese   traditional_chinese}	Enter the language to be used for web administration.	auto_detect

## History

<b>FortiManager v3.0</b>	New.
<b>FortiManager v3.0 MR4</b>	Added device_locks, device_sync_status, verify_serial_number.
<b>FortiManager v3.0 MR5</b>	Added japanese option to webadmin_language.
<b>FortiManager v3.0 MR7</b>	device_sync_status default changed to enable.
<b>FortiManager v4.0</b>	Added admin_server_cert, allow_register, offline_mode, register_passwd, unreg_dev_opt.
<b>FortiManager V4.0 MR1</b>	Added autosync, autosync_interval and demo_mode.

## 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 \(ADOMs\)](#).



**Note:** 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 Administration Guide.

### Syntax

```
config fmsystem admin user
  edit <name_str>
    set adom <adom_name>
    set description <string>
    set password <password>
    set profileid <profile-name>
    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 trusthost1 <ip_mask>
    set trusthost2 <ip_mask>
    set trusthost3 <ip_mask>
    set user_type <local | radius>
  end
  config meta-data
    edit <fieldname>
      set fieldlength
      set fieldvalue <string>
      set importance
    end
  end
end
```

Keywords and variables	Description	Default
adom <adom_name>	Enter the name of the ADOM the administrator belongs to. Any configuration of ADOMs takes place via the FortiManager web-based manager. For more information, see <a href="#">Administrative Domains (ADOMs)</a> .	No default.
description <string>	Enter a description for this administrator account. When using spaces, enclose description in quotes.	No default.
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 user_type is local.	No default.
profileid <profile-name>	Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiManager features.	No default.

Keywords and variables	Description	Default
ssh-public-key1 " <key-type> <key-value> "	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application.  <key type> is ssh-dss for a DSA key, ssh-rsa for an RSA key. <key-value> is the public key string of the SSH client.	No default.
ssh-public-key2 " <key-type> <key-value> "		No default.
ssh-public-key3 " <key-type> <key-value> "		No default.
trustrhost1 <ip_mask> trustrhost2 <ip_mask> trustrhost3 <ip_mask>	Optionally, type the trusted host IP address and netmask from which the administrator can log in to the FortiManager system. You can specify up to three trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see <a href="#">"Using trusted hosts"</a> .	0.0.0.0/0 0.0.0.0/0 127.0.0.1/32
user_type <local   radius>	Enter local if the FortiManager system verifies the administrator's password. Enter radius if a RADIUS server verifies the administrator's password.	local
<b>Keywords and variables for config meta-data subcommand:</b> <b>Note:</b> This subcommand can only change the value of an existing field. To create a new metadata field, use the config fmsystem metadata command.		
fieldname	The label/name of the field. Read-only.	
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 config meta-data subcommand.	
importance	Indicates whether the field is compulsory (required) or optional (optional). Read-only.	

## 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 netmask of 255.255.255.255.

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

The trusted hosts you define apply both to the 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
```

# History

FortiManager v3.0	New.
FortiManager v3.0 MR4	Added ssh-public-key1, ssh-public-key2, ssh-public-key3.
FortiManager v4.0	Added adom, config meta-data (fieldlength, fieldvalue, importance).

## 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
```

Keywords and variables	Description	Default
period <integer>	Enter the number of days to keep the alert console information on the dashboard in days between 1 and 7.	7
severity-level {information   notify   warning   error   critical   alert   emergency}	Enter the severity level to display on the alert console on the dashboard.	No default

### Example

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

```
config fmsystem alert-console
  set period 7
  set severity-level warning
end
```

### History

FortiManager v4.0 MR1 New. DH - current as of build 373

### Related topics

- [fmsystem 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
end
```

Variable	Description	Default
<name_string>	Enter a name for the alert event.	No default.
destination_id <integer>	Enter the table sequence number, beginning at 1.	No default.
type {mail   snmp   syslog}	Select the alert event message method of delivery.	mail
from <email_addr>	Enter the email address of the sender of the message. This is available when the type is set to mail.	No default.
to <email_addr>	Enter the recipient of the alert message. This is available when the type is set to mail.	No default.
smtp-name <server_name>	Enter the name of the mail server. This is available when the type is set to mail.	No default.
snmp-name <server_name>	Enter the snmp server name. This is available when the type is set to snmp.	No default.
syslog-name <server_name>	Enter the syslog server name or IP address. This is available when the type is set to syslog.	No default.
enable-generic-text {enable   disable}	Enable the text alert option.	disable

Variable	Description	Default
enable-severity-filter {enable   disable}	Enable the severity filter option.	disable
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.	No default.
generic-text <string>	Enter the text the alert looks for in the log messages.	No default.
num-events {1   5   10   50   100}	Set the number of events that must occur in the given interval before it is reported.	No default.
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.	No default.
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.	No default.
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.	No default.

## 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
```

## History

**FortiManager v4.0 MR1** New. DH - current as of build 373

## 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
```

Keywords and variables	Description	Default
authentication {enable   disable}	Enable or disable alert email authentication.	enable
fromaddress <email-addr_str>	The email address the alertmessage is from. This is a required variable.	No default.
fromname <name_str>	The SMTP name associated with the email address. To enter a name that includes spaces, enclose the whole name in quotes.	No default.
smtppassword <pass_str>	Set the SMTP server password.	No default.
smtpport <port_int>	The SMTP server port.	25
smtpserver {<ipv4> <fqdn_str>}	The SMTP server address. Enter either a DNS resolvable host name or an IP address.	No default.
smtpuser <username_str>	Set the SMTP server username.	No default.

### 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
```

### History

**FortiManager v3.0 MR1** New. DH - current as of build 373

**FortiManager v3.0 MR5** Added smtppassword and smtpuser keywords. DH - current as of build 373

### Related topics

- [backup all-settings](#)

## backup all-settings

124

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

### Syntax

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

Keywords and variables	Description	Default
crptpasswd <pass_str>	Optional password to protect backup content	No default
directory <dir_str>	Enter the name of the directory on the backup server in which to save the backup file.	No default.
passwd <pass_str>	Enter the password for the backup server.	No default.
protocol {ftp   sftp}	Enter the transfer protocol.	sftp
server {<ipv4> <fqdn_str>}	Enter the IP address or DNS resolvable host name of the backup server.	No default.
status {enable   disable}	Enable or disable scheduled backups.	disable
time <hh:mm:ss>	Enter time of day to perform the backup. Time is required in the form <hh:mm:ss>.	No default.
user <username_str>	Enter the user account name for the backup server.	No default.
week_days {monday tuesday wednesday thursday friday saturday sunday}	Enter days of the week on which to perform backups. You may enter multiple days.	No default.

### 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
```

## History

**FortiManager v3.0** New.

**FortiManager v3.0 MR1** Added crtpasswd variable. DH - current as of build 373

## 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.
  - 5 Use the `fmsystem certificate crl` command to install the CRL. jc not present in 4.0.0
- 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>
```

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

### History

**FortiManager v4.0** New.

### Related topics

- [fmsystem certificate local](#)
- [certificate local generate](#)

## 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.
  - 5 Use the `fmsystem certificate crl` command to install the CRL. jc not present in 4.0.0
- 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 <pwd>
    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]
```

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

### History

**FortiManager v4.0**    New.

### Related topics

- [fmsystem certificate ca](#)
- [certificate local generate](#)

## dm

457

Use this command to configure Deployment Manager settings.

### Syntax

```
config fmsystem dm
  set autosync-cfg {enable | disable}
  set concurrent-install-limit <installs_int>
  set concurrent-install-script-limit <scripts_int>
  set dpm-logsize <kbytes_int>
  set fgfm_heartbeat_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 <kbytes_int>
  set verify-install {enable | disable}
end
```

Keywords and variables	Description	Default
autosync-cfg {enable   disable}	Enable or disable configuration automatic synchronization.	disable
concurrent-install-limit <installs_int>	Enter the maximum number of concurrent installs. The range can be from 5 to 30.	10
concurrent-install-script-limit <scripts_int>	Enter the maximum number of concurrent install scripts. The range can be from 5 to 30.	10
dpm-logsize <kbytes_int>	Enter the maximum dpm log size per device in Kbytes. The range can be from 1 to 10000.	10 000
fgfm_heartbeat_itvl <sec_int>	The interval at which the FortiManager will send a heartbeat signal to a FortiGate unit to keep the FortiManager/FortiGate communication protocol active. The interval can be from 30 to 600 seconds.	60
force-remote-diff {enable   disable}	Enable to always use remote diff when installing.	disable
max-revs <revs_int>	Enter the maximum number of revisions saved. Valid numbers are from 1 to 250.	100
nr-retry <retries_int>	Enter the number of times the FortiManager unit will retry.	3
retry {enable   disable}	Enable or disable configuration installation retries.	enable
retry-intvl <sec_int>	Enter the interval between attempting another configuration installation following a failed attempt.	15
rollback-allow-reboot {enable   disable}	Enable to allow a FortiGate unit to reboot when installing a script or configuration.	disable
script-logsize <kbytes_int>	Enter the maximum log size, in kilobytes, for all scripts that run on that device. Valid numbers are from 1 to 1000.	100
verify-install {enable   disable}	Enable to verify install against remote configuration.	disable

## 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
```

## History

<b>FortiManager v3.0 MR3</b>	New. DH - current as of build 373
<b>FortiManager v3.0 MR4</b>	Added concurrent-install-limit, concurrent-install-script-limit, dpm-logsize, force-remote-diff, verify-install.
<b>FortiManager v3.0 MR5</b>	Removed autosync-cfg.
<b>FortiManager v3.0 MR7</b>	Changed dpm-logsize range and default value.
<b>FortiManager v4.0</b>	Added fgfm_keepalive_itvl and rollback-allow-reboot commands

## Related Commands

To be added.

## 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
```

Keywords and variables	Description	Default
primary <ipv4>	Enter the primary DNS server IP address.	65.39.139.53
secondary <ipv4>	Enter the secondary DNS IP server address.	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
```

### History

**FortiManager v3.0** New.

### Related Commands

To be added.

# global

189

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

## Syntax

```
config fmsystem global
  set adom-status {enable | disable}
  set console-output {more | standard}
  set daylightsavetime {enable | disable}
  set global-custom-service {enable | disable}
  set hostname <hostname_str>
  set install-used-objs-only {enable | disable}
  set lcdpin <pin_int>
  set reload-service-overwrite {enable | disable}
  set remoteauthtimeout <seconds>
  set revision-control {enable | disable}
  set ssl-low-encryption {enable | disable}
  set swapmem {enable | disable}
  set timezone <timezone_int>
end
```

Keywords and variables	Description	Default
adom-status {enable   disable}	Enable or disable administrative domains (ADOMs).	disable
console-output {more   standard}	Select how the output is displayed on the console. Select <b>more</b> to pause the output at each full screen until keypress. Select <b>standard</b> for continuous output without pauses.	standard
daylightsavetime {enable   disable}	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.	enable
global-custom-service {enable   disable}	Enable or disable policy global service. When enabled custom services cannot be configured separately. This should be used with <b>install-used-objs-only {enable   disable}</b> .	disable
hostname <hostname_str>	Enter a name for this FortiManager unit.	FortiManager model name.
install-used-objs-only {enable   disable}	Enable or disable committing and installing of firewall addresses, services, and groups by firewall policy only.	disable
lcdpin <pin_int>	Set the 6 digit PIN administrators must enter to use the LCD panel.	No default.
reload-service-overwrite {enable   disable}	Enable or disable the ability to override global services.	disable
remoteauthtimeout <seconds>	Select the number of seconds before the remote authentication timeout. The valid range is from 1 to 60 seconds.	5
revision-control {enable   disable}	Enable or disable revision control.	disable
ssl-low-encryption {enable   disable}	Enable or disable low-grade (40-bit) encryption.	disable

Keywords and variables	Description	Default
swapmem {enable   disable}	Enable or disable virtual memory.	enable
timezone <timezone_int>	The number corresponding to your time zone. Press ? to list time zones and their numbers. Choose the time zone for the FortiManager unit from the list and enter the correct number.	00

## Example

The following command turns on daylight saving time, sets the FortiManager unit name to FMG3k, sets the LCD password to 123456, and chooses the Eastern time zone for US & Canada.

```
config fmsystem global
  set daylightsavetime enable
  set hostname FMG3k
  set lcdpin 123456
  set timezone 12
end
```

## History

<b>FortiManager v3.0</b>	New. Includes set swapmem and set timezone from v2.8.
<b>FortiManager v3.0 MR1</b>	Added console-output and ssl-low-encryption variables.
<b>FortiManager v3.0 MR3</b>	Added policy-commit-prompt variable.
<b>FortiManager v3.0 MR5</b>	Added global-custom-service, install-used-obj-only, reload-service-overwrite, remoteauthtimeout, revision-control keywords. Removed policy-commit-prompt.
<b>FortiManager v4.0</b>	Added adom-status keyword. Removed global-custom-service, install-used-objs-only, reload-service-overwrite, remoteauthtimeout, and revision-control commands.

## 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 FortiAnalyzer 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>
    end
```

Keywords and variables	Description	Default
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>	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. The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds.	

Keywords and variables	Description	Default
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>	
mode {master   slave   standalone}	Select <b>master</b> to configure the FortiManager unit to be the primary unit in a cluster. Select <b>slave</b> to configure the FortiManager unit to be a backup unit in a cluster. Select <b>standalone</b> 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.	

## 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
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.

## History

**FortiManager v2.8** New.

**FortiManager v3.0** Completely revised.

**FortiManager v3.0 MR4** Described the `get fmsystem ha` keywords: `ha_role`, `ha_status`, `monitor_port_status`, `port_status`, and `sync_status`. Corrected the description of the `arp-interval` keyword.

**FortiManager 4.0** Completely revised. `config fmsystem peer` command removed and its functionality moved into this command.

BD most likely we will never need this stuff again, but I am keeping it for now.

You can use the `get fmsystem ha` command to display HA settings and HA status information:

```

get fmsystem ha
    arp-interval      : 0
    groupid           : 0
    ha_role            : master
    ha_status          : up
    hb-interval        : 5
    hb-lost-threshold : 3
    local-ip1          : 1.1.1.1
    local-ip2          : 2.2.2.2
    mode               : ha

```

```

monitor-ports      : port1 port2
monitor_port_status : port1
password           : *
peer-ip1           : 1.1.1.2
peer-ip2           : 2.2.2.1
port_status        : port3 port4
priority           : 5
sync_status        : in sync
syncport1          : port3
syncport2          : port4

```

`ha_role` can be `singleton` if the FortiManager unit configured for HA operation starts up but has not yet found another FortiManager unit also configured for HA, `master` if the FortiManager unit is configured for HA and is operating as the master (or primary) unit, and `slave` if the FortiManager unit is configured for HA and is operating as the backup unit.

`ha_status` can be `up` if a cluster is operating normally and `down` if a FortiManager unit configured for HA cannot communicate with the other FortiManager unit in the cluster.

`monitor_port_status` indicates the monitored ports that are connected. In the example above both `port1` and `port2` are monitored ports, but `monitor_port_status` shows that only `port1` is connected.

`port_status` indicates the synchronization ports that are connected. In the example above `port_status` indicates that both `syncport1` (set to `port3`) and `syncport2` (set to `port4`) are connected.

`sync_status` can be `out of sync` if the FortiManager configuration and database are not synchronized and if the FortiManager units in the cluster cannot communicate with each other to complete the synchronization process. For example, one of the FortiManager units could be down or the synchronization interfaces could be disconnected. `sync_status` can also be `in sync` if the cluster is operating normally and the FortiManager configuration and database is synchronized between the primary and back units, and `syncing` if both FortiManager units in the cluster are operating normally and the FortiManager configuration and database of the primary unit is in the process of being synchronized to the backup unit.

For more information about HA roles, status, and synchronization see the HA chapter of the [FortiManager Administration Guide](#).

## Example

The following example shows how configure two FortiManager-400 units with the basic settings required for them to operate as an HA cluster. For both FortiManager units the example shows setting the `mode` to `ha` and `syncport1` to `port3`. The first FortiManager-400 unit `local-ip1` is `1.1.1.1` and `peer-ip1` is `1.1.1.2`. The second FortiManager-400 unit `local-ip1` is `1.1.1.2` and `peer-ip1` is `1.1.1.1`. To form a cluster the `port1` interfaces are connected to a switch and to your network and the `port3` interfaces are connected together for HA heartbeat communication.

To configure the first FortiManager unit:

```

config fmsystem ha
  set mode ha
  set syncport1 port3
  set local-ip1 1.1.1.1
  set peer-ip1 1.1.1.2
end

```

To configure the second FortiManager unit:

```
config fmsystem ha
  set mode ha
  set synchport1 port3
  set local-ip1 1.1.1.2
  set peer-ip1 1.1.1.1
end
```

After you connect and start up the cluster you can use the following command to display the HA configuration of the primary unit:

```
get fmsystem ha
  arp-interval      : 0
  groupid           : 0
  ha_role           : master
  ha_status         : up
  hb-interval       : 5
  hb-lost-threshold : 3
  local-ip1         : 1.1.1.1
  local-ip2         : 0.0.0.0
  mode              : ha
  monitor-ports     :
  monitor_port_status :
  password          : *
  peer-ip1          : 1.1.1.2
  peer-ip2          : 0.0.0.0
  port_status       : port3
  priority          : 5
  sync_status       : in sync
  syncport1         : port3
  syncport2         : (null)
```

Use the following command to display the HA configuration of the backup unit:

```
get fmsystem peer
  groupid           : 0
  ha_hostname       : FMG400
  ha_role           : slave
  ha_serialnumber   : FMG4002803030041
  ha_status         : up
  hb-interval       : 5
  hb-lost-threshold : 3
  local-ip1         : 1.1.1.2
  local-ip2         : 0.0.0.0
  mode              : ha
  monitor-ports     :
  monitor_port_status :
  password          : *
  peerip1           : 1.1.1.1
  peerip2           : 0.0.0.0
  port_status       : port3
  priority          : 5
  sync_status       : in sync
  syncport1         : port3
  syncport2         : (null)
  uptime           : 1140205468
```

The following example shows how to configure the first FortiManager unit from the previous example with a higher `priority` so that this FortiManager unit always becomes the primary unit. You can change the priority as part of the initial HA configuration. You can also change the priority of the primary unit in an operating cluster.

```
config fmsystem ha
  set priority 10
end
```

The following example shows how to add the second synchronization interface to a functioning cluster. To add the second synchronization interface you use the `synchport2` keyword to set the second synchronization interface to `port4` and use the `local-ip2` and `peer-ip2` keywords to configure IP addresses for the second synchronization interface. Adding `synchport2` is synchronized to the backup unit. But you must also use the `config fmsystem peer` command to add `local-ip2` and `peer-ip2` to the backup unit.

To configure the primary unit:

```
config fmsystem ha
  set synchport port4
  set local-ip2 2.2.2.1
  set peer-ip2 2.2.2.2
end
```

To configure the backup unit:

```
config fmsystem peer
  set local-ip2 2.2.2.2
  set peerip2 2.2.2.1
end
```

## interface

189

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

### Syntax

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

Variable	Description	Default
<port_str>	On the FM-400, <port_str> can be port1, port2, port3, or port4. On the FM-3000, <port_str> can be port1 or port2.	No default.
allowaccess {http https ping snmp ssh telnet webservice}	Enter the types of management access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.	Varies for each interface.
ip <ipv4_mask>	Enter the interface IP address and netmask. The IP address cannot be on the same subnet as any other interface.	No default
serviceaccess {fclupdates fgtupdates}	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.	Varies for each interface.
speed {1000full 100full 100half 10full 10half auto}	Enter the speed and duplexing the network port uses. Enter auto to automatically negotiate the fastest common speed.	auto
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.	up

### Example

This example shows how to set the FortiManager port1 interface IP address and netmask 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
```

### History

**FortiManager v3.0** New. Includes v2.8 set ip command.

**FortiManager v4.0** Added the speed command.

## Related topics

- [fmsystem route](#)

## 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 diskfull {nolog | overwrite}
  set max-log-file-size <size_int>
  set roll-schedule {none | daily | weekly}
  set severity {alert | critical | debug | emergency | error | information |
    notification | warning}
  set status {enable | disable}
  set server-type {faz | ftp | scp | sftp}
  set upload {disable | enable}
  set upload-delete-files {disable | enable}
  set upload-time <hh:mm>
  set uploadaddir <dir_str>
  set uploadip <ipv4>
  set uploadpass <passwd_str>
  set uploadport <port_int>
  set uploadsched {disable | enable}
  set uploadtype <event>
  set uploaduser <user_str>
  set uploadzip {disable | enable}
end
```

Variable	Description	Default
diskfull {nolog   overwrite}	Enter action to take when the disk is full: nolog — stop logging overwrite — overwrites oldest log entries	overwrite
max-log-file-size <size_int>	Enter the size at which the log is rolled. The range is from 1 to 1024 megabytes.	100
roll-schedule {none   daily   weekly}	Enter the period for the scheduled rolling of a log file. If roll-schedule is none, the log rolls when max-log-file-size is reached.	none

Variable	Description	Default
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. The logging levels in descending order are:	alert
	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 enable to begin logging.	disable
server-type {faz   ftp   scp   sftp}	Enter the type the server to use to store the logs.	No default
upload {disable   enable}	Enable to permit uploading of logs.	disable
upload-delete-files {disable   enable}	Enable to delete log files after uploading.	enable
upload-time <hh:mm>	Enter to configure when to schedule an upload.	No default.
uploadaddr <dir_str>	Enter the destination directory on the remote server.	No default.
uploadip <ipv4>	Enter IP address of the destination server.	0.0.0.0
uploadpass <passwd_str>	Enter the password of the user account on the destination server.	No default.
uploadport <port_int>	Enter the port to use when communicating with the destination server.	21
uploadsched {disable   enable}	Enable to schedule log uploads.	No default.
uploadtype <event>	Enter to upload the event log files.	event
uploaduser <user_str>	Enter the user account on the destination server.	No default.
uploadzip {disable   enable}	Enable to compress uploaded log files.	disable

## 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
```

## History

**FortiManager v3.0**      New

**FortiManager v3.0 MR1**   Rearranged commands to alphabetical order. Added notices about variable visibility.

**FortiManager v4.0 MR2**   Added the command server-type.

## Related topics

- [fmsystem log setting](#)

## 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 | syslog | syslog2 |
  syslog3] filter
  set devcfg {disable | enable}
  set dm {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 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 updmgr {disable | enable}
  set vpnmgr {disable | enable}
  set webport {disable | enable}
end
```

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

Variable	Description	Default
pdmgr {disable   enable}	Enable to log Policy and Device Manager messages.	disable
rtmon {disable   enable}	Enable to log real-time monitor messages.	disable
scfw {disable   enable}	Enable to log firewall objects messages.	disable
scply {disable   enable}	Enable to log policy console messages.	disable
scrmgr {disable   enable}	Enable to log script manager messages.	disable
scvpn {disable   enable}	Enable to log VPN console messages.	disable
system {disable   enable}	Enable to log system manager messages	disable
updmgr {disable   enable}	Enable to log Update Manager messages.	disable
vpnmgm {disable   enable}	Enable to log VPN Manager messages.	disable
webport {disable   enable}	Enable to log web portal messages.	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
```

## History

**FortiManager v3.0** New.

**FortiManager v3.0 MR3** Added fctmgr keyword.

**FortiManager v3.0 MR4** Added dm keyword.

**FortiManager v4.0** Removed ipsec, pdmgr, updmgr, and vpnmgm commands. Added devcfg, epmgr, fgd, fgfm, fmwmgr, glbcfg, rev, scfw, scply, scrmgr, scvpn, and webport commands.

**FortiManager v4.2** Added objcft keyword.

## Related topics

- [fmsystem locallog disk setting](#)

## 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 [locallog filter on page 124](#).

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

Variable	Description	Default
severity {emergency   alert   critical   error   warning   notification   information   debug}	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 “ <a href="#">fmsystem severity {alert   critical   debug   emergency   error   information   notification   warning}</a> ” on <a href="#">page 122</a> .	alert
diskfull		
status {disable   enable}	Enable or disable remote logging to the FortiAnalyzer unit.	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
```

### History

**FortiManager v3.0** New.

**FortiManager v4.0** Added diskfull command.

**MR2**

**FortiManager v4.0** Added note to refer to locallog filter.

**MR2**

## locallog memory setting

Use this command to configure memory settings for local logging purposes. Refer to [locallog filter on page 124](#).

### Syntax

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

Variable	Description	Default
severity {emergency   alert   critical   error   warning   notification   information   debug}	Enter to configure the severity level to log files. See <a href="#">"fmsystem severity {alert   critical   debug   emergency   error   information   notification   warning}" on page 122</a> for more information on the severity levels.	alert
status <disable   enable>	Enable or disable the memory buffer log.	disable

### Example

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

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

### History

**FortiManager v3.0** New. DH - current as of build 373

**FortiManager v4.2** Added note to refer to the locallog filter.

## 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	Default
csv {disable   enable}	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.	disable
facility {alert   audit   auth   authpriv   clock   cron   daemon   ftp   kernel   local0   local1   local2   local3   local4   local5   local6   local7   lpr   mail   news   ntp   syslog   user   uucp}	Enter the facility type. facility identifies the source of the log message to syslog. Change facility to distinguish log messages from different FortiManager units so you can determine the source of the log messages. Available facility types are: alert — log alert audit — log audit auth — security/authorization messages authpriv — security/authorization messages (private) clock — clock daemon cron — cron daemon performing scheduled commands daemon — system daemons running background system processes ftp — File Transfer Protocol (FTP) daemon kernel — kernel messages local0 – local7 — reserved for local use lpr — line printer subsystem mail — email system news — network news subsystem ntp — Network Time Protocol (NTP) daemon syslog — messages generated internally by the syslog daemon	local7
port <port_int>	Enter the port number for communication with the syslog server.	514
server <address_ipv4>	Enter the IP address of the syslog server that stores the logs.	No default.

Variable	Description	Default
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. The logging levels in descending order are:	alert
	emergency	
	alert	
	critical	
	error	
	warning	
	notification	
	information	
	debug	
status {enable   disable}	Enter enable to begin logging.	disable

## 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
```

## History

**FortiManager v3.0 MR4** New

**FortiManager v4.0 MR2** Added a note referring to the filter information.

## Related topics

- [fmsystem log setting](#)

## locallog syslogd (syslogd2, syslogd3) filter

Use this command to enable or disable filters for logs on the syslogd servers.

### Syntax

```
config fmsystem locallog {syslogd, syslogd2, syslogd3} filter
  set devcfg {disable | enable}
  set dm {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 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 updmgr {disable | enable}
  set vpnmgr {disable | enable}
  set webport {disable | enable}
end
```

Variable	Description	Default
devcfg {disable   enable}	Enable to log device configuration messages.	disable
dm {disable   enable}	Enable to log deployment manager messages.	disable
epmgr {disable   enable}	Enable to log endpoint manager messages.	disable
event {disable   enable}	Enable to configure log filter messages.	disable
fctmgr {disable   enable}	Enable to log FortiClient manager messages.	disable
fgd {disable   enable}	Enable to log FortiGuard service messages.	disable
fgfm {disable   enable}	Enable to log FortiGate/FortiManager communication protocol messages.	disable
fmlmgr {disable   enable}	Enable to log FortiMail manager messages.	disable
fmwmgr {disable   enable}	Enable to log firmware manager messages.	disable
glbcfg {disable   enable}	Enable to log global database messages.	disable
ha {disable   enable}	Enable to log high availability activity messages.	disable
ipsec {disable   enable}	Enable to log IPSec messages.	disable
lrmgr {disable   enable}	Enable to log log and report manager messages.	disable
objcft {disable   enable}	Enable to log object configuration.	disable
rev {disable   enable}	Enable to log revision history messages.	disable
pdmgr {disable   enable}	Enable to log Policy and Device Manager messages.	disable

Variable	Description	Default
rtmon {disable   enable}	Enable to log real-time monitor messages.	disable
scfw {disable   enable}	Enable to log firewall objects messages.	disable
scply {disable   enable}	Enable to log policy console messages.	disable
scrmgr {disable   enable}	Enable to log script manager messages.	disable
scvpn {disable   enable}	Enable to log VPN console messages.	disable
system {disable   enable}	Enable to log system manager messages	disable
updmgr {disable   enable}	Enable to log Update Manager messages.	disable
vpnmgm {disable   enable}	Enable to log VPN Manager messages.	disable
webport {disable   enable}	Enable to log web portal messages.	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 syslogd filter
  set event enable
  set lrmgr enable
  set system enable
end
```

## History

**FortiManager v4.2**      New.

## Related topics

- [fmsystem locallog syslogd \(syslogd2, syslogd3\) setting](#)

## 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 [locallog filter on page 124](#) for details of the filters.

### Syntax

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

Keywords and variables	Description	Default
auto_install {enable   disable}	Enable to automatically update the FortiAnalyzer settings as they are changed on the FortiManager unit.	disable
ip <ipv4>	Enter the IP address of the FortiAnalyzer unit.	No default.
passwd <pass_str>	Enter the FortiAnalyzer administrator password for the account specified in username.	No default.
status {disable   enable}	Enable or disable to configure the connection to the FortiAnalyzer unit.	disable
username <username_str>	Enter the FortiAnalyzer administrator login that the FortiManager unit will use to administer the FortiAnalyzer unit.	No default.

### 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
```

### History

<b>FortiManager v3.0</b>	New. DH - current as of build 373 - reordered keywords to alpha order
<b>FortiManager v3.0 MR4</b>	Added auto_install. jc current to build 457
<b>FortiManager v3.0 MR5</b>	Removed auto_install.
<b>FortiManager v4.0</b>	Added auto_install command.
<b>FortiManager v4.0</b>	Removed information about the secure connection as per Mantis ID 0113999

## 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>
  set toconsole {disable | enable}
end
```

Keywords and variables	Description	Default
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.	6
level {emerg   alert   crit   error   warn   notice   info   debug}	Enter the required log level.	alert
rotatesize <int>	Enter a number (in bytes) to configure the rotate size of the log file. Dh - should this be Kbytes?	10 000 000
toconsole {disable   enable}	Enable or disable logging to the console.	disable

### 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
```

### History

**FortiManager v3.0** New. Merged four get/set log v2.8 commands.

**FortiManager v3.0 MR1** toconsole variable was removed. DH - current as of build 260

**FortiManager v3.0 MR3** toconsole variable was added. DH - current as of build 373

**FortiManager v3.0 MR4** toconsole variable was removed. jc - current as of build 457

### Related topics

- [fmsystem locallog disk setting](#)

## log rolling

Use this command to configure when and how the FortiManager rolls log files and creates a fresh file.

### Syntax

```
config rolling-analyzer
  set del_files {enable | disable}
  set directory <dir_str>
  set file-size <size_int>
  set gzip-format {enable | disable}
  set ip <ip_address>
  set password <password_str>
  set server_type {FAZ | FTP | SCP | SFTP}
  set uploading {enable | disable}
  set uploading_sch {Daily_at | When_rolled}
  set uploading_time <0-23>
  set when {daily | weekly | none}
  set username <username_str>
end
```

Keywords and variables	Description	Default
del_files {enable   disable}	Select to delete the log files once uploading is complete.	disable
directory <dir_str>	Select a directory on the upload server where the FortiManager unit stores the uploaded logs.	No default.
file-size <size_int>	The maximum size of the current log file that the FortiManager unit saves to the disk. When the log file reaches the specified maximum size, the FortiManager unit saves the current log file and starts a new active log file. When a log file reaches its maximum size, the FortiManager unit saves the log files with an incremental number, and starts a new log file with the same name. A value of 0 (zero) is unlimited.	0
gzip-format {enable   disable}	Select to compress the log files using the gzip format to save space and time during upload.	disable
ip <ip_address>	Enter the upload server ip address.	0.0.0.0
password <password_str>	Enter the password for the upload server user name.	No default.
server_type {FAZ   FTP   SCP   SFTP}	Select the type of upload server.	FTP
uploading {enable   disable}	Select to enable the FortiManager unit to upload the rolled log file to an FTP site. When selecting enable, use the set ip to define the server location.	disable
uploading_sch {Daily_at   When_rolled}	Select when the FortiManager uploads the log files.	No default.
uploading_time <0-23>	Enter the hour that you want to upload the log files. Enter the number, without minutes, in the 24-hour format.	0
when {daily   weekly   none}	Set the frequency of when the FortiManager unit saves the current log file and starts a new active log file. Select this option if you want to start new log files even if the maximum log file size has not been reached. For example, you want to roll a daily log on a FortiManager unit that does not see a lot of activity.	none
username <username_str>	Enter the user name for the upload server.	No default

## Example

The following commands enables log rolling when log files are 100 MB to an FTP server.

```
config fmsystem log rolling
  set uploading enable
  set server-type ftp
  set ip 172.20.21.12
  set username ftpadmin
  set password *****
  set uploading_sch When_rolled
  set file-size 100
end
```

## History

**FortiManager v4.0 MR1**    New.

## Related topics

- [log setting](#)
- [locallog filter](#)

## metadata

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



**Note:** 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	Default
<name_str>	Enter the name of the new data field.	No default.
field_length {20   50   255}	Select the maximum number of characters allowed in this field: 20, 50, or 255.	50
importance {optional   required}	Select if this field is required or optional when entering standard information.	optional
status {enable   disable}	Enable or disable the metadata.	Disable

### History

**FortiManager v3.0 MR1** New. DH - current as of build 373

**FortiManager v4.0** Removed the `addresses`, `addrgroups`, `fwpolicies`, `servgroups`, and `services` commands. Only `config fmsystem metadata admins` remains.

**FortiManager v4.0 MR2** Added information about the status variable.

### Related topics

- [time](#)

## ntp

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

### Syntax

```
config fmsystem ntp
  set server {<ipv4> | <fqdn_str>}
  set status {enable | disable}
  set sync_interval <min_str>
end
```

Variable	Description	Default
server {<ipv4>   <fqdn_str>}	Enter the IP address or fully qualified domain name of the NTP server.	No default.
status {enable   disable}	Enable or disable NTP time setting.	disable
sync_interval <min_str>	Enter time, in minutes, how often the FortiManager unit synchronizes its time with the NTP server.	60

### History

**FortiManager v3.0** New. DH - current as of build 373

**FortiManager v4.2** Added status

### Related topics

- [time](#)

## ntpserver

Use this command to configure ntpserver used to update automatic time setting.

### Syntax

```
config fmsystem ntp
  config ntpserver
    edit id <integer>
      (n)# set <server>
    end
```

Variable	Description	Default
id <integer>	Enter the IP address or name of the NTP server.	No default.
<server>	Enter the IP address or the host name of the NTP server.	No default

### History

**FortiManager v3.0** New. DH - current as of build 373

**FortiManager v4.2** Added status

### Related topics

- [time](#)

## performance

Use this command to view performance statistics on your FortiManager unit.

### Syntax

```
get fmsystem performance
```

The command returns information like this:

CPU:

Used: 0.4%

Memory:

Total: 2,078,512 KB

Used: 220,652 KB 10.6%

Hard Disk:

Total: 115,380,224 KB

Used: 2,722,248 KB 2.4%

Flash Disk:

Total: 29,745 KB

Used: 27,457 KB 92.3%

### History

**FortiManager v3.0 MR4** New.

### Related Commands

-

## 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
```

Variable	Description	Default
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.	No default.
device <port_str>	Enter the port used for this route.	No default.
dst <dst_ipv4mask>	Enter the IP address and mask for the destination network.	No default.
gateway <gateway_ipv4>	Enter the default gateway IP address for this network.	No default.

### History

**FortiManager v2.8** New.

**FortiManager v3.0** Command format changed from `set route <network_IP> <netmask> gw <gw_IP>`. DH - current as of build 373

### Related topics

- [fmsystem interface](#)

## 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 [FortiManger Administration Guide](#), or the [Fortinet Knowledge Center](#) online.



**Note:** 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
  end
end
```

Variables	Description	Default
edit <index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.	
events <events_list>	Enable the events for which the FortiManager unit should send traps to the SNMP managers in this community.	All events enabled.
	disk_low	
	ha_switch	
	intf_ip_chg	
	sys_reboot	

Variables	Description	Default
name <community_name>	Enter the name of the SNMP community. Names can be used to distinguish between the roles of the hosts in the groups. For example the Logging and Reporting group would be interested in the <code>disk_low</code> events, but likely not the other events. The name is included in SNMP v2c trap packets to the SNMP manager, and is also present in query packets from, the SNMP manager.	No default.
query-v1-port <port_number>	Enter the SNMP v1 query port number used when SNMP managers query the FortiManager unit.	161
query-v1-status {enable   disable}	Enable or disable SNMP v1 queries for this SNMP community.	enable
query-v2c-port <port_number>	Enter the SNMP v2c query port number used when SNMP managers query the FortiManager unit. SNMP v2c queries will include the name of the community.	161
query-v2c-status {enable   disable}	Enable or disable SNMP v2c queries for this SNMP community.	enable
status {enable   disable}	Enable or disable this SNMP community.	enable
trap-v1-rport <port_number>	Enter the SNMP v1 remote port number used for sending traps to the SNMP managers.	162
trap-v1-status {enable   disable}	Enable or disable SNMP v1 traps for this SNMP community.	enable
trap-v2c-rport <port_number>	Enter the SNMP v2c remote port number used for sending traps to the SNMP managers.	162
trap-v2c-status {enable   disable}	Enable or disable SNMP v2c traps for this SNMP community. SNMP v2c traps sent out to SNMP managers include the community name.	enable
<b>hosts variables</b>		
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.	No Default
ip <address_ipv4>	Enter the IP address of the SNMP manager.	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
end
```

## History

FortiManger v4.0    New

## Related topics

- [fmsystem snmp sysinfo](#)

## 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 Center](#) online.

### Syntax

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

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

### 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
```

### History

**FortiOS v3.0** Changed contact\_info to contact-info.

**FortiOS v3.0 MR2** Added trap-high-cpu-threshold, trap-log-full-threshold, and trap-low-memory-threshold commands. DH - as of build 300.310.

**FortiOS v4.0** Revised.

### Related topics

- [fmsystem snmp community](#)

## status

Use this command to view the status of your FortiManager unit.

### Syntax

```
get fmsystem status
```

### Example

Here is an example of the output from `get fmsystem status`:

```
Platform type           : FMG400A
Version                 : v4.0.0-build0076,110309
Serial Number          : FMG40A3906500500
Current Time            : Thu Apr 16 14:02:26 EDT 2009
Daylight Time Saving    : Yes
Time Zone               : (GMT-5:00)Eastern Time(US & Canada)
HA Mode                 : Stand Alone
```

### History

**FortiManager v3.0** New.

**FortiManager v3.0 MR1** Command format changed from `get status`. Output changed.



# 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:

<a href="#">backup</a>	<a href="#">fgt-cli-access</a>	<a href="#">fmupdate {ftp   tftp} import</a>
<a href="#">bootimage</a>	<a href="#">fmclient apply-lockdown</a>	<a href="#">format disk</a>
<a href="#">certificate ca</a>	<a href="#">fmclient client_license list</a>	<a href="#">fortianalyzer get_configurations</a>
<a href="#">certificate local</a>	<a href="#">fmclient client_license list_device</a>	<a href="#">fortianalyzer</a>
<a href="#">certificate local generate</a>	<a href="#">fmclient cluster</a>	<a href="#">send_all_configurations</a>
<a href="#">console baudrate</a>	<a href="#">fmclient enterprise_license download</a>	<a href="#">fortianalyzer send_configurations</a>
<a href="#">date</a>	<a href="#">fmclient enterprise_license list</a>	<a href="#">ping</a>
<a href="#">device</a>	<a href="#">fmclient group refresh</a>	<a href="#">execute</a>
<a href="#">dmserver delrev</a>	<a href="#">fmclient group rename</a>	<a href="#">reboot</a>
<a href="#">dmserver showconfig</a>	<a href="#">fmclient license_key deploy</a>	<a href="#">reset</a>
<a href="#">dmserver showdev</a>	<a href="#">fmclient license_key list</a>	<a href="#">restore</a>
<a href="#">dmserver showrev</a>	<a href="#">fmclient optimize-fcm-database</a>	<a href="#">shutdown</a>
<a href="#">dmserver revlist</a>	<a href="#">fmclient package delete</a>	<a href="#">ssh</a>
<a href="#">fcdevice addtomanaged</a>	<a href="#">fmclient package deploy</a>	<a href="#">time</a>
<a href="#">fcdevice search</a>	<a href="#">fmclient package download</a>	<a href="#">top</a>
<a href="#">fcpolicy deploy</a>	<a href="#">fmclient package list</a>	<a href="#">traceroute</a>
<a href="#">fcpolicy grant unlicensed</a>	<a href="#">fmclient refresh_ou</a>	
<a href="#">fcpolicy group</a>	<a href="#">fmclient sync-ldap</a>	
<a href="#">fcpolicy retrieve</a>	<a href="#">fmclient sync ou_group</a>	
<a href="#">fcpolicy revoke unit</a>	<a href="#">fmpolicy print-global-database</a>	
<a href="#">fcpolicy unit</a>	<a href="#">fmscript delete</a>	
	<a href="#">fmscript import</a>	
	<a href="#">fmscript list</a>	
	<a href="#">fmscript run</a>	
	<a href="#">fmscript showlog</a>	



## 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 <ipv4> <path_str> <user_str> <pass_str>
                                <key_str>
```

Keywords and variables	Description
<ipv4>	Enter FTP server IP address.
<path_str>	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_str>	Enter username to use to log on the backup server.
<pass_str>	Enter the password for the username on the backup server.
<key_str>	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...

### History

<b>FortiManager v3.0</b>	New.
<b>FortiManager v3.0 MR4</b>	Replaced <filename> with <filepath>. Removed <path>. Added <cryptkey>.
<b>FortiManager v3.0 MR5</b>	Added dpm, sm, full, and basic keywords.
<b>FortiManager v3.0 MR7</b>	Added backup file naming convention.
<b>FortiManager v4.0</b>	Removed the dpm, sm, full, and basic backup types.

### 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
```

### History

**FortiManager v3.0**   New.

### 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.

### History

FortiOS v4.0	New.
--------------	------

### 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 153.

### 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.

### History

**FortiOS v4.0**      New.

### 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> <key-length>
<subject> [<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.
<subject>	Enter one of the following pieces of information to identify the FortiManager unit being certified: <ul style="list-style-type: none"> <li>the FortiManager unit IP address</li> <li>the fully qualified domain name of the FortiManager unit</li> <li>an email address that identifies the FortiManager unit</li> <li>An IP address or domain name is preferable to an email address.</li> </ul>
<key-length>	Enter 512, 1024, 1536 or 2048 for the size in bits of the encryption key.
[<optional_information>]	Enter optional_information as required to further identify the unit. See <a href="#">"Optional information variables"</a> 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 organization_name_str, you must first enter the country_code_str, state_name_str, and city_name_str. While entering optional variables, you can type ? for help on the next required variable.

## 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.
<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.

## History

FortiOS v4.0      New.

## Related commands

- [certificate local](#)

## 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.



**Note:** 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
```

### History

**FortiManager v3.0** New.

# 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
```

## History

**FortiOS v2.80 MR4** New.

**FortiManager v3.0** Command format used to be `set time date <mm:dd:yy>`.

## Related topics

- [time](#)
- [fmsystem metadata](#)

## 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.	

### History

**FortiManager v4.0 MR1**      New.

## 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.

### History

<b>FortiManager v3.0 MR4</b>	New.
<b>FortiManager v3.0 MR5</b>	<devicename> replaced <device_name>, <conftype> replaced <configType>, and <rev> replaced <revno>.
<b>FortiManager v4.0</b>	<startrev> and <endrev> replaced <<conftype> and <rev>.

## 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.

### History

<b>FortiManager v3.0 MR1</b>	New.
<b>FortiManager v3.0 MR5</b>	<devicename> replaced <device_name> and <revisionNo> replaced <revno>.
<b>FortiManager v3.0 MR6</b>	<revno> replaced <revisionNo>.
<b>FortiManager v4.0</b>	Removed <configType> and <revno>.

## 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
```

**FortiManager v3.0 MR1** New.

**FortiManager 4.0** <showdev> replaced <showinfo>.

## dmserver showrev

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

You cannot use this command with read-only permission.

### Syntax

```
execute dmserver showrevdiff <devicename> <revision>
```

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

### History

**FortiManager v4.0**      New.

## 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.

### History

<b>FortiManager v3.0 MR1</b>	New.
<b>FortiManager v3.0 MR5</b>	<devicename> replaced <device_name> to identify device.
<b>FortiManager v4.0</b>	<revlist> replaced <showrevlist>. Removed <<configType>.

## fcdevice addtomanaged

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

### Syntax

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

### History

**FortiManager v3.0 MR4**      New.

### Related topics

- [fmclient discovery](#)

## 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>
```

Keywords and variables	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.

### History

**FortiManager v4.2**      New

### Related topics

## fcdevice search

Use this command to discover FortiClient PCs 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.

### History

**FortiManager v3.0** New.

### Related topics

- [fmclient discovery](#)

## fcpolicy deploy

Use this command to deploy the configuration changes to managed FortiClient PCs and PC groups.

### Syntax

```
execute fcpolicy deploy group <group_name>
execute fcpolicy deploy group_child <group_name>
execute fcpolicy deploy ungroup <host_name>
execute fcpolicy deploy unit <host_name>
```

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 PC.

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

### History

<b>FortiManager v3.0</b>	New (as <code>fcpolicy install</code> )
<b>FortiManager v3.0 MR4</b>	Renamed. <code>ungroup</code> keyword added.
<b>FortiManager v4.0</b>	Added <code>group_child</code> keyword.

### 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 <host_name>
```

where <host\_name> is the unlicensed client's host name.

### History

<b>FortiManager v4.0</b>	New.
--------------------------	------

### Related topics

- [fcpolicy revoke unit](#)

## fcpolicy group

Use this command to select a FortiClient group for configuration.

### Syntax

```
execute fcpolicy group <group_name>
```

If you do not specify <group\_name>, the command reports the currently selected group.

### History

**FortiManager v3.0 MR4**    New.

### Related topics

- [fcpolicy unit](#)

## fcpolicy retrieve

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

### Syntax

```
execute fcpolicy retrieve group <group_name>
execute fcpolicy retrieve ungroup <host_name>
execute fcpolicy retrieve unit <host_name>
```

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

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

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

### History

**FortiManager v3.0**      New (as `fcpolicy resync`).

**FortiManager v3.0 MR4**    Renamed. `ungroup` option added.

### Related topics

- [fcpolicy deploy](#)

## fcpolicy revoke unit

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

### Syntax

```
execute fcpolicy revoke unit <host_name>
```

### History

<b>FortiManager v4.0</b>	New.
--------------------------	------

### Related topics

- [fcpolicy grant unlicensed](#)

## fcpolicy unit

Use this command to select a FortiClient PC for configuration.

### Syntax

```
execute fcpolicy unit <host_name>
```

If you do not specify <host\_name>, the command reports the currently selected FortiClient PC.

### History

**FortiManager v3.0 MR4**    New.

### 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 <device_name>
end
```

Keywords and variables	Description
<device_name>	Enter the device name.

### History

FortiManager v4.0 MR2    New.

### Related topics

## 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>
```

Keywords and variables	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 #
```

### History

**FortiManager v3.0** New.

### Related topics

- [ssh](#)

## fmclient apply-lockdown

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

### Syntax

```
execute fmclient apply-lockdown
```

### History

**FortiManager v3.0 MR4**    New.

## fmclient client\_license list

Use this command to list the FortiClient PC 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
- Last Update
- Status
- Comment

### History

**FortiManager v3.0 MR7**    New.

### 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>
```

### History

<b>FortiManager v4.0</b>	New.
--------------------------	------

### 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]
```

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.

### History

<b>FortiManager v3.0 MR5</b>	New.
<b>FortiManager v3.0 MR6</b>	Removed <code>connect</code> and <code>disconnect</code> keywords.

## fmclient enterprise\_license download

Use this command to download the FortiClient enterprise license from FortiCare. You need the license key.

### Syntax

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

### History

**FortiManager v3.0 MR7**    New.

### Related Topics

- [fmclient enterprise\\_license list](#)
- [fmclient enterprise\\_license](#)
- [fmclient client\\_license](#)

## 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

### History

**FortiManager v3.0 MR7**    New.

### Related Topics

- [fmclient enterprise\\_license download](#)
- [fmclient enterprise\\_license](#)
- [fmclient client\\_license](#)

## **fmclient group refresh**

Refresh dynamic FortiClient PC group membership.

### **Syntax**

```
execute fmclient group refresh
```

### **History**

**FortiManager v3.0 MR4**    New.

## fmclient group rename

Rename a FortiClient PC group.

### Syntax

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

Keywords and variables	Description
<group name>	Enter the current name of the group.
<new group name>	Enter the new name of the group.

### History

**FortiManager v4.0 MR2** Documented in FortiManager v4.2.

## fmclient license\_key deploy

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

### Syntax

To display a list of the license keys configured on the FortiManager unit:

```
execute fmclient license_key list
```

To deploy license keys:

```
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.

### History

**FortiManager v3.0 MR6**    New.

### Related topics

- [fmclient license\\_key list](#)
- [fmclient license\\_key](#)

## 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
```

### History

**FortiManager v3.0 MR6**    New.

### Related topics

- [fmclient license\\_key deploy](#)
- [fmclient license\\_key](#)

## **fmclient optimize-fcm-database**

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

### **Syntax**

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

### **History**

**FortiManager v3.0 MR7**    New.

## fmclient package delete

Use this command to delete unneeded FortiClient upgrade packages.

### Syntax

```
execute fmclient package delete <package_version_id>
```

Use the [fmclient package list](#) command to determine the value of <package\_version\_id>.

### History

**FortiManager v3.0 MR7**    New.

### Related commands

- [fmclient package list](#)
- [fmclient package download](#)

## fmclient package deploy

Use this command to deploy upgrade packages to FortiClient PCs.

### Syntax

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

Use the [fmclient package list](#) command to determine the value of <package\_version\_id>.

Use the get [fcdevice group](#) and get [fcdevice unit](#) commands to obtain group names and unit host names.

### History

**FortiManager v3.0 MR6**    New.

### 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_version_id>
```

Use the [fmclient package list](#) command to determine the value of <package\_id>.

### History

**FortiManager v3.0 MR6**    New.

### 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
```

### History

**FortiManager v3.0 MR6**    New.

## 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>
```

### History

**FortiManager v3.0 MR6**    New.

## 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>
```

### History

**FortiManager v4.0 MR2**    New.

## 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.....
```

### History

**FortiManager v4.0 MR2**    New.

## **fmpolicy print-global-database**

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

### **Syntax**

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

### **History**

**FortiManager v4.2**

New.

## 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
```

Keywords and variables	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.

### History

#### FortiManager v4.2

Added the missing description for this command. Category field was added in FortiManager v4.2.

## Fmpolicy print-global-object

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

### Syntax

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

Keywords and variables	Description
<adom>	Enter the name of the ADOM.
<category>	Enter the category of the ADOM.

### History

FortiManager v4.2

New.

## fmscript delete

Delete a script.

### Syntax

```
execute fmscript delete <script_name>
```

Keywords and variables	Description
<script_name>	The name of the script to delete.

### History

**FortiManager v3.0 MR7**    New.

# fmscript import

Import a script from an FTP server.

## Syntax

```
execute fmscript import <ftpserver_ipv4> <filename> <username_str>
<password_str> <scriptname_str> { CLI | TCL } <comment_str> <adom name> {
any | 300 | 400 } <platform> <devicename> <buildno> <hostname> <serialno>
```

Keywords and variables	Description
<ftpserver_ipv4>	The IP address of the FTP server.
<filename>	The filename of the script to be imported to the FortiManager system.
<username_str>	The user name used to access the FTP server.
<password_str>	The password used to access the FTP server.
<scriptname_str>	The name of the script to import.
{ CLI   TCL }	The type of script as one of CLI or TCL.
<comment_str>	A comment about the script being imported, such as a brief description.
<adom name>	Name of the administrative domain.
{ any   300   400 }	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.
<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 any or the specific serial number of the device, such as FGT5002803033042.

## History

**FortiManager v4.0**      New.

## Related topics

- [fmscript list](#)
- [fmscript run](#)

## 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
```

### History

<b>FortiManager v4.0</b>	New.
--------------------------	------

### 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> { device | devicedb | globaldb }
[<devname_str>]
```

Keywords and variables	Description
<scriptid_int>	The ID number of the script to run.
{ device   devicedb   globaldb }	Select where to run the script - on the device, on the device's object database, or on the global database.
<devname_str>	Enter the device name to run the script on. This is required if device or devicedb were chosen for where to run the script.

### History

**FortiManager v3.0 MR7** New.

**FortiManager v4.0** All old keywords removed. Added scriptid\_int, { device | devicedb | globaldb }, and devname\_string.

### Related topics

- [fmscript import](#)
- [fmscript list](#)

## fmscript showlog

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

### Syntax

```
execute fmscript showlog <unit_name>
```

Keywords and variables	Description
<unit_name>	The name of a managed FortiGate device.

### Example

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

```
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)
```

### History

**FortiManager v3.0 MR7** New.

**FortiManager v4.0** Changed from `fmscript show-log` to `fmscript showlog`.

### Related topics

- [fmscript run](#)

## fmupdate {ftp | tftp} import

You can import or export packages using the ftp or tftp servers.

### Syntax

```
execute fmupdate {ftp | tftp} import {ac-ips | fct | fds | spam | url}
    <filename_str> <server_ipv4> <path_str> <user_str> <password_str>
```

Keywords and variables	Description
{ftp   tftp}	Select FTP or TFTP as the file transfer protocol to use.
{ac-ips   fct   fds   spam   url}	Select the type of file to export or import.
<filename_str>	Enter the name of the file to download.
<server_ipv4>	Enter the FQDN or the IP Address of the FTP or TFTP server.
<path_str>	Enter the name of the directory of the file to download from the FTP server. If the directory name has spaces, use quotes instead.
<user_str>	Enter the user name to log into the FTP server.
<password_str>	Enter the password to log into the FTP server.

### History

**FortiManager v3.0** New.

**FortiManager v4.2** Corrected this command.

## format disk

Format the hard disk on the FortiManager system.

### Syntax

```
execute format disk
```

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



**Note:** 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.

### History

**FortiManager v3.0** New.

### Related topics

- [restore](#)

## fortianalyzer get\_configurations

Use this command to retrieve the configuration from the managed FortiAnalyzer unit to the Device Manager.

This command is useful to update the Device Manager's configuration copy with changes you may have made locally on the FortiAnalyzer unit.

### Syntax

```
execute fortianalyzer get_configurations <fortianalyzer_name>
```

### Example

After editing the FortiAnalyzer unit's configuration locally, you can retrieve it to synchronize the configuration copy stored by FortiManager unit's Device Manager.

```
execute fortianalyzer get_configurations FortiAnalyzer-800
```

A message appears:

```
Retrieve configurations successfully
```

### History

<b>FortiManager v3.0</b>	New.
<b>FortiManager v3.0 MR5</b>	Updated completion message.

## fortianalyzer send\_all\_configurations

Use this command to send the complete configuration from the Device Manager to the managed FortiAnalyzer unit.

This is useful when you want to completely overwrite the FortiAnalyzer configuration, such as when restoring the configuration after restoring firmware on a FortiAnalyzer unit, or when you want to undo all configuration changes made locally on the FortiAnalyzer unit.

### Syntax

```
execute fortianalyzer send_all_configurations <fortianalyzer_name>
```

### Example

You could, after editing the FortiAnalyzer unit's configuration remotely, undo all local configuration changes by sending the complete configuration copy stored by FortiManager unit's Device Manager.

```
execute fortianalyzer send_all_configurations FortiAnalyzer_2000A
```

A message appears:

```
Install all configurations successfully
```

### History

**FortiManager v3.0**      New.

**FortiManager v3.0 MR5**   Updated completion message.

## fortianalyzer send\_configurations

Use this command to send only the changed parts of the configuration from the Device Manager to the managed FortiAnalyzer unit.



**Note:** If there are no configuration changes made since the last update, no configurations are sent.

### Syntax

```
execute fortianalyzer send_configurations <fortianalyzer_name>
```

### Example

You could, after editing the FortiAnalyzer unit's configuration remotely, send changes made to the configuration copy stored by FortiManager unit's Device Manager.

```
execute fortianalyzer send_configurations FortiAnalyzer_800B
```

A message appears:

```
Install configurations successfully
```

### History

<b>FortiManager v3.0</b>	New.
<b>FortiManager v3.0 MR5</b>	Updated completion message.

## 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>}
```

<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
```

### History

**FortiManager v2.8** New.

**FortiManager v3.0** Command format changed from `execute ping <host_ip>`

### 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
```

Variables	Description	Default
add-disk <integer>	Enables you to add a disk and giving it a number.	No default
delete-disk <integer>	Enables you to delete the selected disk.	No default
rebuild-ecc {enable   disable}	Enables you to build the ecc table.	disable

### 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
```

### History

**FortiManager v4.2** New.

### Related topics

## reboot

Restart the FortiManager system.

This command will disconnect all sessions on the FortiManager system.

### Syntax

```
execute reboot
```

### History

**FortiManager v2.8** New.

### 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
```

### History

<b>FortiManager v2.8</b>	New.
<b>FortiManager v3.0</b>	Command format changed from <code>set reset {all   data}</code> .
<b>FortiManager v3.0 MR5</b>	Added <code>&lt;database&gt;</code> keyword.
<b>FortiManager v4.0</b>	Removed the <code>data</code> command.

### 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 <server_ipv4> <file_str> <user_str>
execute restore image {ftp | tftp} <file_str> <server_ipv4> <user_str>
```

Variables	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.
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.
<file_str>	The file to get from the server. You can enter a path with the filename, if required.
<server_ipv4>	IP address of the server to get the file from.
<user_str>	The username to log on to the FTP server. This option is not available for restore operations from TFTP servers.
<pass_str>	The password for username on the FTP server. This option is not available for restore operations from TFTP servers.

### 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
```

### History

<b>FortiManager v3.0</b>	New.
<b>FortiManager v3.0 MR5</b>	Added <code>dpm</code> , <code>fortianalyzer_package</code> , <code>sm</code> , and <code>&lt;backuptype&gt;</code> keywords.
<b>FortiManager v4.0</b>	Removed the <code>config</code> , <code>database</code> , <code>dpm</code> , <code>fortianalyzer_package</code> , and <code>sm</code> keywords.

### Related topics

- [execute backup](#)
- [execute bootimage](#)

# shutdown

Shut down the FortiManager system.

This command will disconnect all sessions.

## Syntax

```
execute shutdown
```

## History

**FortiManager v2.8**   New.

## Related topics

- [reboot](#)
- [reset](#)

## 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.

### History

**FortiManager v3.0**      New.

### 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
```

### History

**FortiManager v2.8** New.

**FortiManager v3.0** Command format changed from `set time clock <hh:mm:ss>`.

### Related topics

- [date](#)
- [fmsystem ntp](#)

## 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:

```
8:22am up 2 days, 20:13, 0 users, load average: 0.00, 0.00, 0.00
150 processes: 146 sleeping, 1 running, 3 zombie, 0 stopped
CPU0 states: 0.0% user, 0.0% system, 0.0% nice, 100.0% idle
CPU1 states: 0.0% user, 0.3% system, 0.0% nice, 99.2% idle
Mem: 2069772K av, 485764K used, 1584008K free, 0K shrd, 40124K buff
Swap: 2069764K av, 0K used, 2069764K free 307480K cached
```

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	COMMAND
967	root	15	0	908	908	664	R	0.5	0.0	0:00	top_bin
1	root	8	0	408	408	360	S	0.0	0.0	0:06	init
2	root	9	0	0	0	0	SW	0.0	0.0	0:00	keventd
3	root	18	19	0	0	0	SWN	0.0	0.0	0:00	ksoftirqd_CPU0
4	root	18	19	0	0	0	SWN	0.0	0.0	0:00	ksoftirqd_CPU1
5	root	9	0	0	0	0	SW	0.0	0.0	0:00	kswapd
6	root	9	0	0	0	0	SW	0.0	0.0	0:00	bdflush
7	root	9	0	0	0	0	SW	0.0	0.0	0:03	kupdated
12	root	9	0	0	0	0	SW	0.0	0.0	1:06	kjournald
13	root	9	0	0	0	0	SW	0.0	0.0	0:32	kjournald
68	root	9	0	8440	8436	5612	S	0.0	0.4	0:12	cmdbsvr
147	postgres	11	0	1308	1308	1232	S	0.0	0.0	0:05	postmaster
148	postgres	9	0	2056	2056	1232	S	0.0	0.0	0:01	postmaster
149	postgres	9	0	1348	1348	1240	S	0.0	0.0	0:04	postmaster
169	root	9	0	1192	1192	868	S	0.0	0.0	0:10	fmlogger
171	postgres	9	0	4132	4132	3736	S	0.0	0.1	0:00	postmaster
172	root	9	0	768	768	580	S	0.0	0.0	0:58	cfgman

### History

FortiManager v2.8 New.

### Related topics

- [fmsystem status](#)

## 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 {<address_ipv4> | <host-name>}
```

Variables	Description
<address_ipv4>	IP address of network device.
<host-name>	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
```

### History

**FortiManager v3.0**    New.

### Related topics

- [ping](#)



# Index

## A

- accept\_ports
  - fmclient discovery, 48
- accepting FortiClient requests for management, 48
- accprofile
  - fmsystem admin, 97
- action\_queue\_interval
  - fmclient communication\_setting, 47
- action\_queue\_length
  - fmclient communication\_setting, 47
- address\_ipv4
  - execute traceroute, 213
- admin ldap
  - fmsystem, 78
- admin profile
  - fmsystem, 80, 141
- admin user
  - fmsystem, 97
- administrative access, 119
- Administrative Domains (ADOM), 31
- administrator accounts, 97
- administrator ldap, 78
- administrator profile, 80, 141
- alert-console
  - fmsystem, 100
- allowaccess
  - fmsystem interface, 119
- all-settings
  - execute restore, 208
- archiving, 149
- auto, 68
- av-ips fct server-override
  - fmupdate, 62
- av-ips fgt server-override
  - fmupdate, 63
- av-ips push-override
  - fmupdate, 64
- av-ips web-proxy
  - fmupdate, 67

## B

- backing up
  - on demand, 149
- backup
  - execute, 149
- backup status
  - fmsystem, 108
- bootimage
  - execute, 150

## C

- certificate
  - vpn ca, 106
  - vpn local, 107

- CLI basics, 25
- CLI session, 172
- CLI structure, 21
- client licenses, FortiClient
  - listing, 174
- cluster, 113
- cluster secondary
  - fmclient, 45
- cluster setting
  - fmclient, 46
- command abbreviation, 27
- command completion, 26
- command help, 26
- comments, documentation, 11
- communication\_setting
  - fmclient, 47
- compression
  - fmsystem log settings, 133
- config, 22
- config router, 15, 59
- configuration file, importing, 199
- connecting
  - to the CLI, 18
  - to the CLI using SSH, 20
  - to the FortiManager console, 18
- connection
  - ping test, 204
  - traceroute test, 213
- console baudrate
  - execute, 154
- contact-info
  - system snmp sysinfo, 144
- CPU, 139
- CPU usage, SNMP event, 141
- cryptpasswd
  - execute backup all-settings, 149
- csv
  - fmsystem locallog syslogd setting, 128
- customer service, 11

## D

- database configuration, restoring, 208
- date
  - execute, 155
- date\_str
  - execute date, 155
- Daylight Saving Time, 111
- daylightsavetime
  - fmsystem global, 111
- delay, 68
- delaytime, 68
- delete, table shell command, 21
- deployment, 68
- Deployment Manager, 108

- description
  - fcdevice ungroup, 39
  - fmsystem admin user, 97, 103
  - system snmp sysinfo, 144
- device
  - fmsystem route, 140
- device lock enable, 95
- device\_locks
  - fmsystem admin setting, 95
- device\_name
  - execute fgt-cli-access, 172
- device\_sync\_status
  - fmsystem admin setting, 95
- directory
  - fmsystem backup, 104
- disable\_auto\_vaccum
  - fmclient communication\_setting, 47
- discovery
  - fmclient, 48
- diskfull
  - fmsystem locallog, 121
  - fmsystem locallog disk setting, 121
- dm
  - fmsystem locallog filter, 124, 130
- dns
  - fmsystem, 108
- DNS servers, 110
- dns\_domain
  - fcdevice group, 36
  - fcdevice temp (get), 38
- documentation
  - commenting on, 11
  - Fortinet, 11
- dst
  - fmsystem route, 140

## E

- edit
  - fcdevice group, 36
  - fcdevice ungroup, 39
- edit, table shell command, 21
- editing commands, 26
- editing the configuration file, 29
- encrypted password support, 27
- end
  - command in a table shell, 21
  - command in an edit shell, 22
- enterprise license, FortiClient
  - downloading, 177
  - listing, 178
- enterprise\_license
  - fmclient, 50
- employment, 68
- event
  - fmsystem locallog filter, 124, 130
- events
  - system snmp communities, 141
- example command sequences, 25
- execute, 147

## F

- facility
  - fmsystem locallog syslogd setting, 128
- failure detection time
  - HA, 114
- fcdevice search
  - execute, 164
- fcpolicy deploy
  - execute, 165
- fcpolicy group
  - execute, 167
- fcpolicy retrieve
  - execute, 168
- fcpolicy unit
  - execute, 170
- fct ip address
  - fmupdate av-ips fct server-override, 62
- fct-services
  - fmupdate, 71
- fgt ip address
  - fmupdate av-ips fgt server-override, 63
- fgt-cli-access
  - execute, 172
- filename
  - execute backup, 149
  - execute restore, 208
- firmware image, uploading, 208
- flash disk, 139
- fmclient apply-lockdown
  - execute, 173
- fmclient client\_license list, 147
  - execute, 174
- fmclient cluster
  - execute, 176
- fmclient enterprise\_license download, 147
  - execute, 177
- fmclient enterprise\_license list
  - execute, 178
- fmclient group refresh
  - execute, 179
- fmclient group rename, 147, 180
- fmclient license\_key deploy
  - execute, 181
- fmclient license\_key list
  - execute, 182
- fmclient optimize-fcm-database, 147
- fmclient package delete, 147
  - execute, 184
- fmclient package deploy, 147
  - execute, 185
- fmclient package download, 147
  - execute, 186
- fmclient package list, 147
  - execute, 187
- fmclient refresh\_ou, 147
- fmclient sync ou\_group, 147
- fmclient sync-ldap, 147
- Fmpolicy, 193
- fmpolicy, 192
- fmscript import, 147

- fmscript run, 147
- fmscript showlog, 147
- fmupdate
  - execute, 199
  - server-access-priorities, 73
- fmwmgr
  - fmsystem locallog filter, 124, 130
- format disk
  - execute, 200
- FortiAnalyzer
  - configuring, 132
- fortianalyzer send\_all\_configurations, 147
- fortianalyzer send\_configurations, 147
- FortiClient
  - configuring communication settings, 47
- FortiClient group administrators, 51
- FortiGate documentation
  - commenting on, 11
- FortiGate SNMP agent, 144
- FortiGate, IP address, 172
- FortiLog
  - configuring access, 132
- FortiManager
  - rebooting, 206
  - server hostname, 111
  - shutting down, 209
- FortiManager, resetting, 207
- Fortinet customer service, 11
- Fortinet documentation, 11
- Fortinet Knowledge Center, 11

## G

- gateway
  - fmsystem route, 140
- get
  - command in a table shell, 21
  - command in an edit shell, 22
- get fmsystem ha, 115, 117
- get\_configurations
  - execute fortianalyzer, 201
- global
  - fmsystem, 111
- global settings, 111
- group
  - fcdevice, 36
  - for FortiClient group administrator, 51
- group\_admin
  - fmclient, 51
- group\_type
  - fcdevice group, 36

## H

- HA, 113
  - failure detection time, 114
  - synchronization interface, 113
  - synchronization port, 113
- ha
  - fmsystem, 113
  - fmsystem locallog filter, 124, 130

- ha\_role
  - fmsystem ha, 116
- ha\_status
  - fmsystem ha, 116
- hard disk
  - formatting, 200
  - performance status, 139
- hb-interval
  - fmsystem ha, 113
- hb-lost-threshold
  - fmsystem ha, 114
- high availability, 113
- host-name
  - execute traceroute, 213
- hostname
  - fmsystem global, 111
- HTTP, 119
- HTTPS, 119

## I

- ICMP echo request, 204
- image
  - execute restore, 208
- in sync
  - fmsystem ha, 116
- interface
  - bringing up or down, 119
  - configuring, 119
  - fmsystem, 119
  - system snmp community hosts, 142
- International characters, 28
- introduction
  - Fortinet documentation, 11
- ip
  - execute backup, 149
  - fcdevice temp (get), 38
  - fmsystem interface, 119
  - fmsystem log fortianalyzer, 132
  - fmupdate av-ips fgt server-override, 63
  - fmupdate av-ips server-override, 62
  - fmupdate av-ips web-proxy, 67
  - system snmp community hosts, 142
- IP address formats, 29
- ip\_address
  - fcdevice group, 36
- ipsec
  - fmsystem locallog filter, 124, 130

## L

- LCD PIN, setting, 111
- lcdpin
  - fmsystem global, 111
- level
  - fmsystem log setting, 133
- license keys, FortiClient
  - deploying, 181
  - listing, 182
- license, FortiClient enterprise
  - setting validation type, 50
- line continuation, 27

- locallog disk setting
  - fmsystem, 121
- locallog filter
  - fmsystem, 124, 130
- locallog fortianalyzer setting
  - fmsystem, 126
- locallog memory setting
  - fmsystem, 127
- locallog syslogd setting
  - fmsystem, 128
- location
  - system snmp sysinfo, 144
- lockdown
  - fmclient, 55
- log filter settings, 124, 130
- log fortianalyzer
  - fmsystem, 132
- log setting
  - fmsystem, 133
- log settings, 121
  - syslogd, 128
- lrmgr
  - fmsystem locallog filter, 124, 130

## M

- manual, 68
- master
  - fmsystem ha, 116
- max-log-file-size
  - fmsystem locallog, 121
  - fmsystem locallog disk setting, 121
- member
  - fcdevice group, 36
- memory
  - enabling virtual memory, 112
  - sage statistics, 139
- min\_message\_interval
  - fmclient communication\_setting, 47
- mode, 68
- monitor\_port\_status
  - fmsystem ha, 116
- month, setting, 155

## N

- name
  - system snmp community, 142
- newclient\_action
  - fmclient discovery, 48
- next, 22
- ntp
  - fmsystem, 136
- NTP server, configuring, 136

## O

- option access\_ungroup
  - for FortiClient group administrator, 51
- os\_name
  - fcdevice group, 36
- out of sync
  - fmsystem ha, 116

## P

- packet type, 199
- passwd
  - fmsystem backup, 104
  - fmsystem log fortianalyzer, 132
- password
  - execute backup, 149
  - execute restore, 208
  - fmclient lockdown, 55
  - fmsystem admin user, 97
  - fmupdate av-ips web-proxy, 67
  - for backup server, 104
- path
  - execute backup all-settings, 149
- pdmgr
  - fmsystem locallog filter, 125, 130
- performance
  - fmsystem, 139
  - get fmsystem, 139
- performance statistics, 139
- ping, 119
  - execute, 204
- platform
  - in get fmsystem status, 145
- policy
  - fcdevice group, 36
- port
  - bringing up or down, 119
  - configuring, 119
  - fmsystem locallog syslogd setting, 128
  - fmupdate av-ips fct server-override, 62
  - fmupdate av-ips fgt server-override, 63
  - fmupdate av-ips push-override, 64, 65
  - fmupdate av-ips server-override, 62
  - fmupdate av-ips web-proxy, 67
  - fmupdate fct-services, 71
- port\_status
  - fmsystem ha, 116
- primary
  - fmsystem dns, 110
- primary image, 150
- processes, viewing, 212
- profileid
  - fmsystem admin user, 97
- protocol
  - fmsystem backup, 104
- psk
  - fmsystem log fortianalyzer, 132
- purge, 22

## Q

- query-v1-port
  - system snmp community, 142
- query-v1-status
  - system snmp community, 142
- query-v2c-port
  - system snmp community, 142
- query-v2c-status
  - system snmp community, 142

## R

- raid, 205
- reboot
  - execute, 206
- recalling commands, 26
- reset
  - execute, 207
- resources, viewing, 212
- restore, 147
  - execute, 208
- roll-schedule
  - fmsystem locallog, 121
  - fmsystem locallog disk setting, 121
- rotatesize
  - fmsystem log setting, 133
- route
  - fmsystem, 140
- routing
  - configuring for FortiManager, 140
  - gateway, 140
  - ip, 140
  - port, 140
- rtmon
  - fmsystem locallog filter, 125, 131

## S

- secondary
  - fmsystem dns, 110
- secondary image, 150
- send\_all\_configurations
  - execute fortianalyzer, 202
- send\_configurations
  - execute fortianalyzer, 203
- serial connection, 154
- serial number
  - in get fmsystem status, 145
- server
  - fmsystem backup, 104
  - fmsystem locallog syslogd setting, 128
  - fmsystem ntp, 137
- set, 22
- setting administrative access for SSH or Telnet, 19
- severity
  - fmsystem locallog, 122
  - fmsystem locallog disk setting, 122, 129
  - fmsystem locallog fortianalyzer setting, 126
  - fmsystem locallog memory setting, 127
  - fmsystem locallog syslogd, 129
- shutdown
  - execute, 209
- singleton
  - fmsystem ha, 116
- slave
  - fmsystem ha, 116
- SNMP
  - v1, 142
  - v2c, 142
- snmp community
  - system, 141

- snmp sysinfo
  - system, 144
- software upgrade packages, FortiClient
  - deleting, 184
- spaces, entering in strings, 28
- special characters, where they are allowed, 29
- ssh, 119
- ssh-public-key
  - fmsystem admin user, 98
- status
  - fmclient lockdown, 55
  - fmsystem, 145
  - fmsystem backup, 104
  - fmsystem interface, 119
  - fmsystem locallog, 122, 129
  - fmsystem locallog disk setting, 122, 129
  - fmsystem locallog fortianalyzer setting, 126
  - fmsystem locallog memory setting, 127
  - fmsystem log fortianalyzer, 132
  - fmsystem ntp, 137
  - fmupdate av-ips fct server-override, 62
  - fmupdate av-ips fgt server-override, 63
  - fmupdate av-ips push-override, 64, 65
  - fmupdate av-ips web-proxy, 67
  - fmupdate fct-services, 71, 72
  - system snmp community, 142
  - system snmp sysinfo, 144
- swapmem
  - fmsystem global, 112
- sync\_interval
  - fmsystem ntp, 137
- sync\_status
  - fmsystem ha, 116
- synchronization interface
  - HA, 113
- synchronization port
  - HA, 113
  - See also synchronization interface, 113
- syncing
  - fmsystem ha, 116
- system
  - fmsystem locallog filter, 125, 131

## T

- technical support, 11
- temp
  - fcdevice, 38
- time, 147
  - execute, 211
  - fmsystem backup, 104
  - setting automatically, 136
- time zone, setting, 112
- timezone
  - fmsystem global, 112
- toconsole
  - fmsystem log setting, 133
- top
  - execute, 212
- traceroute, 147
  - execute, 213
- trap-v1-rport
  - system snmp community, 142

- trap-v1-status
  - system snmp community, 142
- trap-v2c-rport
  - system snmp community, 142
- trap-v2c-status
  - system snmp community, 142
- trusted hosts
  - administrator, 98
  - security issues, 98
- trusthost
  - fmsystem admin user, 98
- type
  - execute fupdate, 199
  - fcdevice group, 36

## U

- uid
  - fcdevice temp (get), 38
- ungroup
  - fcdevice, 39
- unit
  - fcdevice, 40
- unset, 22
- updmgr
  - fmsystem locallog filter, 125, 131
- upload
  - fmsystem locallog, 122
  - fmsystem locallog setting, 122
- upload-delete-files
  - fmsystem locallog disk setting, 122
- uploaddir
  - fmsystem locallog disk setting, 122
- uploadip
  - fmsystem locallog disk setting, 122
- uploadpass
  - fmsystem locallog disk setting, 122
- uploadport
  - fmsystem locallog disk setting, 122
- uploadsched
  - fmsystem locallog disk setting, 122
- upload-time
  - fmsystem locallog disk setting, 122
- uploadtype
  - fmsystem locallog disk setting, 122
- uploaduser
  - fmsystem locallog disk setting, 122
- uploadzip
  - fmsystem locallog disk setting, 122
- urlog
  - fupdate av-ips push-override, 64, 65
- user
  - fmsystem backup, 104
- username
  - execute backup, 149
  - execute fgt-cli-access, 172
  - execute restore, 208
  - fmsystem log fortianalyzer, 132
  - fupdate av-ips web-proxy, 67
- using the CLI, 17

## V

- validation\_type
  - fmclient, 50
- verify\_serial\_number
  - fmsystem admin setting, 96
- version
  - in get fmsystem status, 145
- virtual memory, 112
- vpn, 106
- vpnmgr
  - fmsystem locallog filter, 125, 131

## W

- week\_days
  - fmsystem backup, 104
- windows\_group
  - fcdevice group, 36

## Y

- year, setting, 155







