



FortiManager™

Version 4.0

CLI Reference

FortiManager CLI Reference

Version 4.0

21 April 2009

02-400-92967-20090421

© Copyright 2009 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

Introduction	9
FortiManager Server	9
Web-based manager	10
FortiManager System product life cycle	10
Registering your Fortinet product.....	11
Customer service and technical support.....	11
Fortinet documentation	11
Fortinet Tools and Documentation CD	11
Fortinet Knowledge Center	11
Comments on Fortinet technical documentation	11
Conventions	12
IP addresses.....	12
CLI constraints.....	12
Notes, Tips and Cautions	12
Typographical conventions	13
What's new	15
Using the CLI.....	23
CLI command syntax	23
Connecting to the CLI.....	24
Connecting to the FortiManager console.....	24
Setting administrative access on an interface	25
Connecting to the FortiManager CLI using SSH.....	26
Connecting to the FortiManager CLI using the web-based manager	26
CLI objects.....	26
CLI command branches	27
config branch	27
get branch.....	29
show branch	30
execute branch	30
diagnose branch	31
Example command sequences.....	31
CLI basics	32
Command help	32
Command completion.....	32
Recalling commands	32
Editing commands	33
Line continuation.....	33

Command abbreviation.....	33
Environment variables	33
Encrypted password support	34
Entering spaces in strings.....	34
Entering quotation marks in strings	34
Entering a question mark (?) in a string.....	34
International characters	35
Special characters	35
IP address formats.....	35
Editing the configuration file.....	35
Changing the baud rate	35
Administrative Domains (ADOMs).....	37
ADOMs overview.....	37
Configuring ADOMs.....	38
fcdevice.....	39
group	40
temp.....	42
ungroup.....	43
unit.....	44
unlicensed	45
fcpolicy.....	47
antileak option.....	48
antileak sensword	49
antispam bannedword	50
antispam blackwhitelist.....	51
antispam option	52
antivirus scheduledscan	53
antivirus setting email	54
antivirus setting realtime.....	55
antivirus setting scheduledscan	57
firewall address	59
firewall addrgrp	60
firewall apppolicy	61
firewall option.....	63
firewall pingserver	65
firewall policy	66
firewall protocol	68
firewall protocolgrp.....	69

firewall schedule recurring	70
firewall schedulegrp	71
firewall service	72
firewall trustedip address.....	73
firewall zone <security_level>.....	74
log setting	75
system settings	77
system trustedfortimanager.....	78
system wan_optimization.....	79
vpn download	80
vpn security_policy.....	81
webfilter option	82
webfilter profile	83
fmclient	85
client_license.....	86
cluster secondary	87
cluster setting.....	88
communication_setting.....	89
discovery	90
emailalert	91
enterprise_license.....	92
group_admin	93
Syntax.....	93
ldap_users	94
ldapsetting	95
license_key	96
lockdown.....	97
systemsetting	98
webfilter_profile	99
fmsystem	101
admin profile.....	102
admin radius.....	106
admin setting.....	107
admin user	109
alertemail	112
backup all-settings.....	113

certificate ca	115
certificate local	116
dm	117
dns	119
global	120
ha	122
General FortiManager HA configuration steps	123
interface	125
locallog disk setting	126
locallog filter	129
locallog fortianalyzer setting	131
locallog memory setting	132
locallog syslogd (syslogd2, syslogd3) setting	133
log fortianalyzer	135
log setting	137
metadata	138
ntp	139
performance	140
route	141
snmp community	142
snmp sysinfo	145
status	146
fmupdate	147
analyzer virusreport	148
av-ips advanced-log	149
av-ips fct server-override	150
av-ips fgt server-override	151
av-ips push-override	152
av-ips update-schedule	153
av-ips web-proxy	154
disk-quota	155
device-version	156
fct-services	157
server-access-priorities	158
config private-server	158
service	160

web-spam fct server-override	161
web-spam fgd-log	162
web-spam fgt server-override	163
web-spam poll-frequency	164
web-spam web-proxy	165
execute	167
backup	168
bootimage	169
certificate ca	170
certificate local	171
certificate local generate	172
console baudrate	173
date	174
dmserver delrev	175
dmserver showconfig	176
dmserver showdev	177
dmserver showrev	178
dmserver revlist	179
fcdevice addtomanaged	180
fcdevice search	181
fcpolicy deploy	182
fcpolicy grant unlicensed	183
fcpolicy group	184
fcpolicy retrieve	185
fcpolicy revoke unit	186
fcpolicy unit	187
fgt-cli-access	188
fmclient apply-lockdown	189
fmclient client_license list	190
fmclient client_license list_device	191
fmclient cluster	192
fmclient enterprise_license download	193
fmclient enterprise_license list	194
fmclient group refresh	195
fmclient license_key deploy	196
fmclient license_key list	197

fmclient optimize-fcm-database	198
fmclient package delete.....	199
fmclient package deploy	200
fmclient package download	201
fmclient package list.....	202
fmclient sync-ldap.....	203
fmpolicy print-global-database	204
fmscript delete.....	205
fmscript import.....	206
fmscript list.....	207
fmscript run	208
fmscript showlog	209
fmupdate {ftp tftp} import.....	210
format disk.....	211
fortianalyzer get_configurations	212
fortianalyzer send_all_configurations	213
fortianalyzer send_configurations	214
ping.....	215
reboot	216
reset.....	217
restore	218
shutdown	219
ssh	220
time	221
top.....	222
tracert.....	223
Index.....	225

Introduction

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

The FortiManager System is an integrated platform for centralized management of FortiGate Antivirus Firewalls.

Using the FortiManager System, you can:

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

The FortiManager System scales to manage up to a thousand FortiGate devices 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 the following topics:

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

FortiManager Server

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

The FortiManager Server manages communication between FortiGate devices and the web-based management console.

The FortiManager Server stores and manages all FortiGate device configurations.

It can also act as a on-site FDN server for the FortiGate devices to download virus and attack signatures, to use the web filtering and antispam service. This will significantly reduce the network delay and usages, compared with the FortiGate devices' connection to an FDN server over the Internet.

Web-based manager

You can use the FortiManager Console to configure FortiGate devices and to view FortiGate 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 FortiGate devices assigned to them. The FortiManager Console also allows these users to remotely upgrade FortiGate device firmware, and virus and attack definitions.

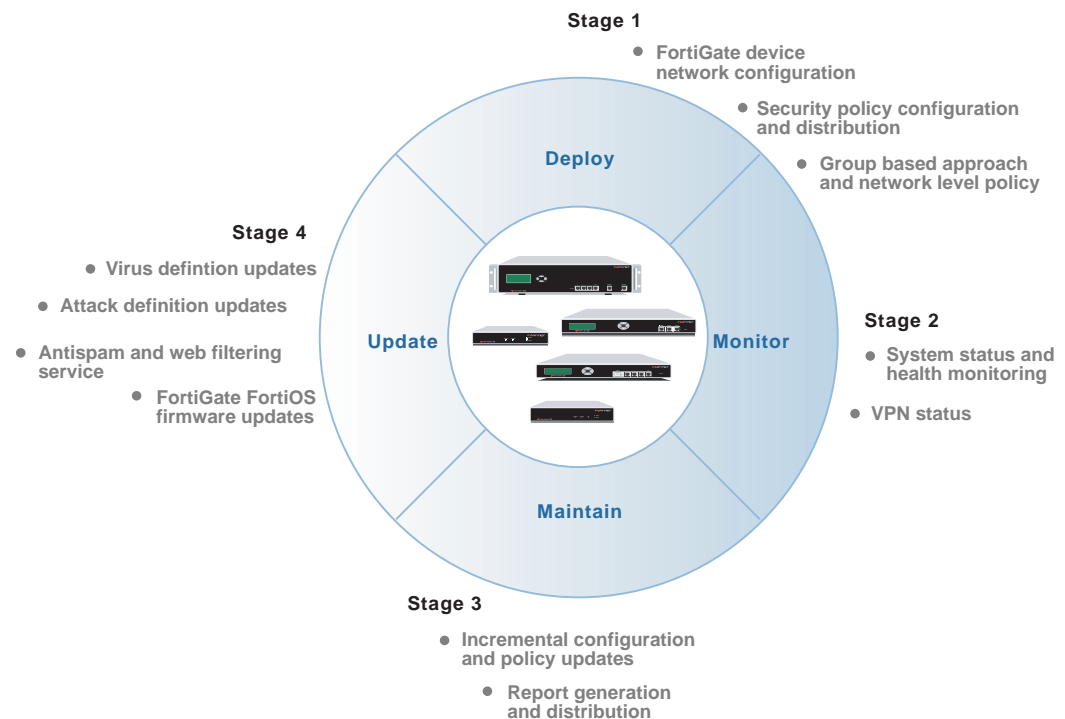
Administrators with read only access can view the configuration, device status, system health, real time logs, and historical logs of the FortiGate devices assigned to them.

FortiManager System product life cycle

The FortiManager System allows you to manager FortiGate devices through their entire product life cycle:

Deployment	Complete FortiGate device configuration after initial installation.
Monitoring	Real-time monitoring of FortiGate system status and health.
Maintenance	Continuous, incremental configuration and updates.
Updates	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.

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 23](#).

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 <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as Central_Office_1.
Navigation	Go to <i>VPN > IPSEC > Auto Key (IKE)</i> .
Publication	For details, see the FortiGate Administration Guide .

What's new

The tables below list commands which have changed since the previous release, FortiManager v3.0 MR7.

Command	Change
config <code>fcdevice group</code> edit <name> set enterprise_client_license set policy enterprise_client_license	New keyword. Sets enterprise client license for group. New keyword. Sets enterprise license as basis for group membership.
get <code>fcdevice unlicensed</code>	New command. Lists unlicensed FortiClient PCs.
config <code>fcpolicy antivirus setting scheduledscan</code> set pause-scan-on-ups	New keyword. Pauses AV scanning if computer switches to battery power or UPS.
config <code>fcpolicy firewall ...</code>	Note: FortiManager 4.0 settings for the FortiClient firewall are compatible with FortiClient version 4.0 only.
config <code>fcpolicy firewall address</code> edit <name> set type fqdn set fqdn <fqdn>	New option. Defines an FQDN as an address. New keyword. Specifies the fully-qualified domain name.
config <code>fcpolicy firewall addrgrp</code> edit <name>	There are now built-in address groups that correspond to the security zones: Blocked, Public and Trusted. You can modify these address groups, but you cannot delete them.
config <code>fcpolicy firewall apppolicy</code>	New command. Configures firewall policies for applications.
config <code>fcpolicy firewall option</code> set firewall-default-action set launch-new-application set ping-server set public-zone-level set trusted-zone-level set trustip-status	Keyword removed. New keyword. Selects the firewall action when an unknown application tries to communicate through the firewall. New keyword. Enables the FortiClient application to check ping servers when it is connected to a new network to determine the trustworthiness of the network. New keyword. Sets the security level for the Public zone. New keyword. Sets the security level for the Trusted zone. New keyword. Exempts the addresses defined in <code>fcpolicy firewall trustedip</code> from intrusion prevention scanning.
config <code>fcpolicy firewall pingserver</code>	New command. Configures ping servers to use with the <code>ping-server</code> option in <code>fcpolicy firewall option</code> .

Command	Change
config <code>fcpolicy firewall policy</code> edit <policy_num> set address set destination set direction set protocol set source	<p>Keyword removed. Use <code>destination</code> and <code>source</code>.</p> <p>New keyword. Specifies the destination address or address group to which the policy applies. Available addresses include built-in address groups Blocked, Trusted, and Public, corresponding to the security zones.</p> <p>Keyword removed. Set <code>source</code> and <code>destination</code> addresses.</p> <p>New keyword. Selects the network protocols to which this policy applies.</p> <p>New keyword. Specifies the source address or address group to which the policy applies. Available addresses include built-in address groups Blocked, Trusted, and Public, corresponding to the security zones.</p>
config <code>fcpolicy firewall protocol</code>	New command. Defines protocols for use in firewall policies.
config <code>fcpolicy firewall protocolgrp</code>	New command. Defines protocol groups for use in firewall policies.
config <code>fcpolicy firewall schedulegrp</code>	New command. Defines schedule groups.
config <code>fcpolicy firewall service</code> edit <name> set destinationport set sourceport set type	<p>Keyword removed. Configure <code>destport</code> in <code>fcpolicy firewall protocol</code>.</p> <p>Keyword removed. Configure <code>srcport</code> in <code>fcpolicy firewall protocol</code>.</p> <p>Keyword removed. Configure <code>type</code> in <code>fcpolicy firewall protocol</code>.</p>
config <code>fcpolicy firewall svcgrp</code>	Command removed.
config <code>fcpolicy firewall trustedip setting</code>	Command removed. Enable trusted IP addresses in the <code>fcpolicy firewall option</code> command using the <code>trustip-status</code> keyword.
config <code>fcpolicy firewall zone <security_level></code>	New command. Configures the settings for the high and medium security levels of the Public and Trusted zones.
config <code>fcpolicy log setting</code> set custom_field enable set custom_field_name set custom_field_value	These new keywords configure a custom log field to be included in all logs from a FortiClient PC.
config <code>fcpolicy system wan_optimization</code>	New command. Configures WAN optimization settings.
config <code>fcpolicy system wan_optimization</code> set webfilter-dont-rate-ip	New keyword. Enables filtering by domain rating only, not by IP address.
config <code>fmclient communication_setting</code> set action_queue_length	Default value changed from 200,3000,120,120 to 300,1500, 60,60
config <code>fmclient emailalert</code>	New command. Configures the sending of email alerts for FortiClient Manager management alerts and events.
config <code>fmclient systemsetting</code> set monitor_eventlogging_duration	New keyword. Sets the number of days that management event logs are retained before automatic deletion.
config <code>fmdevice ...</code>	Commands removed.

Command	Change
config fmfwm ...	Commands removed.
config fmpolicy ...	Commands removed.
config fmrtm ...	Commands removed.
config fmscript ...	Commands removed.
config fmsystem admin profile	
edit <profile_name>	
set av_read	Keyword removed.
set av_write	Keyword removed.
set deploy-management	New keyword. Sets level of access to the deployment management configuration settings.
set devcfg-adminuser	New keyword. Sets level of access to admin user configuration.
set devcfg-authuser	New keyword. Sets level of access to authenticated user configurations.
set devcfg-avconfig	New keyword. Sets level of access to antivirus configuration settings.
set devcfg-fgupdate	New keyword. Sets level of access to FortiGuard update configurations.
set devcfg-fw-address	New keyword. Sets level of access to firewall address configuration settings.
set devcfg-fw-other	New keyword. Sets level of access to configuration settings such as the VPN console, FortiClient manager, and Script manager.
set devcfg-fw-policy	New keyword. Sets level of access to firewall policy configuration settings.
set devcfg-fw-profile	New keyword. Sets level of access to firewall profile configuration settings.
set devcfg-fw-schedule	New keyword. Sets level of access to firewall schedule configuration settings.
set devcfg-fw-service	New keyword. Sets level of access to firewall service configuration settings.
set devcfg-ipsconfig	New keyword. Sets level of access to IPS configuration settings.
set devcfg-logreport	New keyword. Sets level of access to log reporting configuration settings.
set devcfg-maintenance	New keyword. Sets level of access to device maintenance details.
set devcfg-netconfig	New keyword. Sets level of access to network configuration settings.
set devcfg-routerconfig	New keyword. Sets level of access to router configuration settings.
set devcfg-spamfilter	New keyword. Sets level of access to spam filter configuration settings.
set devcfg-sysconfig	New keyword. Sets level of access to system configuration settings.
set devcfg-vpnconfig	New keyword. Sets level of access to VPN configuration settings.
set devcfg-webfilter	New keyword. Sets level of access to web filter configuration settings.
set device-op	New keyword. Adds the capability to add, delete, and edit devices.
set device-summary	New keyword. Sets level of access to device summary details.
set faz-management	New keyword. Sets level of access to FortiAnalyzer configuration management settings.
set fct-manager	New keyword. Sets level of access to FortiClient manager configuration settings.

Command	Change
config fmsystem admin profile (continued)	
edit <profile_name>	
set fgd-center	New keyword. Sets level of access to FortiGuard Center.
set firewall_read	Keywords removed. Use new devcfg-fw- keywords.
set firewall_write	
set firmware-management	New keyword. Sets level of access to firmware management configuration settings.
set fullaccess	Keyword removed.
set fwimage-database	New keyword. Sets level of access to firmware images.
set global_privileges	Keyword removed.
set global-storage	New keyword. Sets level of access to global object storage configuration settings.
set group-op	New keyword. Adds the capability to add, delete, and edit groups.
set imp2p_read	Keywords removed.
set imp2p_write	
set ips_read	Keywords removed. Use new devcfg-ipsconfig keyword.
set ips_write	
set logrep_read	Keywords removed. Use new devcfg-logreport keyword.
set logrep_write	
set logrepmgr_read	
set logrepmgr_write	
set other_read	Keywords removed. Use new devcfg-fw-other keyword.
set other-write	
set read-passwd	New keyword. Adds the capability to view the authentication password in clear text.
set realtime-monitor	New keyword. Sets level of access to the Real-Time monitor configuration settings.
set realtime_read	Keywords removed. Use new realtime-monitor keyword.
set realtime_write	
set router_read	Keywords removed. Use new devcfg-routerconfig keyword.
set router_write	
set script-database	New keyword. Sets level of access to script databases.
set script-management	New keyword. Sets level of access to the Script manager configuration settings.
set security-console	New keyword. Sets level of access to security console configuration settings.
set service-usage	New keyword. Sets level of access to the service usage configuration settings.
set spamf_read	Keywords removed. Use new devcfg-spamfilter keyword.
set spamf_write	
set system_read	Keywords removed. Use new devcfg-sysconfig keyword.
set system_write	
set system-setting	New keyword. Sets level of access to system settings.
set user_read	Keywords removed. Use new devcfg-authuser keyword.
set user_write	
set vpn-manager	New keyword. Sets level of access to VPN console configuration settings.

Command	Change
config <code>fmsystem admin profile</code> (continued)	
set vpn_read	Keywords removed. Use new <code>devcfg-vpnconfig</code> keyword.
set vpn_write	
set webf_read	Keywords removed. Use new <code>devcfg-webfilter</code> keyword.
set webf_write	
set web-portal	New keyword. Sets level of access to web portal configuration settings.
config <code>fmsystem admin radius</code>	
set auth-type	New keyword. Sets authentication protocol for RADIUS server.
config <code>fmsystem admin setting</code>	
set admin_server_cert	New keyword. Sets the name of an https server certificate to use for secure connections.
set allow_register	New keyword. Enables unregistered devices to register.
set offline_mode	New keyword. Shuts down the protocol used to communicate with managed devices.
set register_passwd	New keyword. Sets the password to use when registering a device.
set unreg_dev_opt	New keyword. Select action to take when an unregistered device connects to FortiManager.
config <code>fmsystem admin user</code>	
edit <name_str>	
set adom	New keyword. Assigns the administrator to an ADOM.
config meta-data	New subcommand. Sets the value of a metadata field. To create metadata fields, use the <code>config fmsystem metadata</code> command.
config <code>fmsystem certificate ca</code>	New command. Installs Certificate Authority (CA) certificates.
config <code>fmsystem certificate local</code>	New command. Installs local certificates.
config <code>fmsystem dm</code>	
set fgfm_keepalive_itvl	New keyword. Sets the interval at which the FortiManager will send a FortiManager/FortiGate protocol keepalive signal to a FortiGate unit.
set rollback-allow-reboot	New keyword. Allows FortiGate units to reboot when installing a script or configuration.
config <code>fmsystem global</code>	
set adom-status	New keyword. Enables Administrative Domains (ADOMs).
set global-custom-service	Keyword removed.
set install-used-objs-only	Keyword removed.
set reload-service-overwrite	Keyword removed.
set remoteauthtimeout	Keyword removed.
set revision-control	Keyword removed.
config <code>fmsystem ha</code>	Command extensively revised. Peer configuration added.
config <code>fmsystem interface</code>	
set speed	New keyword. Sets speed and half/full duplex for interface.

Command	Change
<code>config fmsystem locallog filter</code>	
<code>set devcfg</code>	New keyword. Enable to log device configuration messages.
<code>set epmgr</code>	New keyword. Enable to log endpoint manager messages.
<code>set fgd</code>	New keyword. Enable to log FortiGuard service messages.
<code>set fgfm</code>	New keyword. Enable to log FortiGate/FortiManager communication protocol messages.
<code>set fmwmgr</code>	New keyword. Enable to log firmware manager messages.
<code>set glbcfg</code>	New keyword. Enable to log global database messages.
<code>set ipsec</code>	Keyword removed.
<code>set pdmgr</code>	Keyword removed.
<code>set rev</code>	New keyword. Enable to log revision history messages.
<code>set scfw</code>	New keyword. Enable to log firewall objects messages.
<code>set scply</code>	New keyword. Enable to log policy console messages.
<code>set scrmgr</code>	New keyword. Enable to log script manager messages.
<code>set scvpn</code>	New keyword. Enable to log VPN console messages.
<code>set updmgr</code>	Keyword removed.
<code>set vpnmgr</code>	Keyword removed.
<code>set webport</code>	New keyword. Enable to log web portal messages.
<code>config fmsystem log fortianalyzer</code>	
<code>set auto_install</code>	New keyword. Enables automatic update of FortiAnalyzer settings as they are changed on the FortiManager unit.
<code>config fmsystem metadata addresses</code>	Command removed.
<code>config fmsystem metadata addrgroups</code>	Command removed.
<code>config fmsystem metadata fwpolicies</code>	Command removed.
<code>config fmsystem metadata servgroups</code>	Command removed.
<code>config fmsystem metadata services</code>	Command removed.
<code>config fmsystem peer</code>	Command removed. Use <code>config fmsystem ha</code> command.
<code>config fmsystem snmp community</code>	Command renamed from <code>config fmrtm snmp community</code> . Configures SNMP communities on your FortiManager unit.
<code>config fmsystem snmp sysinfo</code>	Command renamed from <code>config fmrtm snmp sysinfo</code> . Configures the FortiManager SNMP agent.
<code>config fmupdate device-version</code>	New command. Sets the firmware version devices connecting to the FortiManager unit will use.
<code>config fmupdate server-access-priorities</code>	
<code>config private-server</code>	
<code>edit <id></code>	
<code>set time_zone</code>	New keyword. Sets the time zone of the private server.
<code>execute backup</code>	<code>dpm</code> , <code>sm</code> , <code>full</code> , and <code>basic</code> backup types removed. Only <code>all-settings</code> backup is supported.
<code>execute device ...</code>	Commands removed.
<code>execute dmserver backuplog</code>	Command removed.
<code>execute dmserver delrev <startrev> <endrev></code>	New options <code><startrev></code> and <code><endrev></code> . Specify first and last revision to delete.

Command	Change
<code>execute dmserver delrev <conftype> <rev></code>	Options <conftype> and <rev> removed.
<code>execute dmserver install</code>	Command removed.
<code>execute dmserver revlist</code>	Command renamed from <code>execute dmserver showrevlist</code> .
<code>execute dmserver showconfig <devicename></code>	Options <configtype> and <revno> removed. Command now shows only current device configuration. To view a particular revision, use <code>execute dmserver showrev</code> .
<code>execute dmserver showdelta</code>	Command removed.
<code>execute dmserver showdev</code>	Command renamed from <code>execute dmserver showinfo</code> .
<code>execute dmserver showdevice</code>	Command removed. Use <code>execute dmserver showdev</code> .
<code>execute dmserver showlog</code>	Command removed.
<code>execute dmserver showinfo</code>	Command renamed to <code>execute dmserver showdev</code> .
<code>execute dmserver showrevdiff</code>	Command removed.
<code>execute dmserver showrevlist</code>	Command renamed to <code>execute dmserver revlist</code> .
<code>execute fcpolicy deploy group_child</code>	New option <code>group_child</code> deploys configuration changes to the specified FortiClient group and its child groups.
<code>execute fcpolicy grant unlicensed</code>	New command. Grants a license to a client that is in the Unlicensed Client list.
<code>execute fcpolicy revoke unit</code>	New command. Revokes a managed client's enterprise license key.
<code>execute fmclient client_license list_device</code>	New command. Lists the clients using a specified client license.
<code>execute fmpolicy ...</code>	Existing commands removed.
<code>execute fmpolicy print-global-database</code>	New command. Displays the global database configuration for an ADOM.
<code>execute fmscript import</code>	New command. Imports a script from an FTP server.
<code>execute fmscript list</code>	New command. Lists the scripts on the FortiManager device.
<code>execute fmscript run</code>	Command can now run scripts on the database. Keywords used to specify script and devices have changed.
<code>execute fmscript show-log</code>	Command renamed to <code>execute fmscript showlog</code> .
<code>execute fmscript showlog</code>	Command renamed from <code>execute fmscript show-log</code> .
<code>execute reset</code>	<code>data <database></code> option removed.
<code>execute restore</code>	<code>config</code> , <code>database</code> , <code>dpm</code> , <code>fortianalyzer_package</code> , and <code>sm</code> options removed.

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

fcdevice	Configures FortiClient PCs and client groups.
fcpolicy	Configures the settings of FortiClient PCs or client groups.
fmclient	Configures the FortiManager settings used to manage clustering, discovering and adding FortiClient PCs, licenses, client lockdown, and web filtering for managed FortiClient PCs.
fmsystem	Configures options related to the overall operation of the FortiManager unit, such as interfaces, virtual domains, and administrators.
fmupdate	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 31](#).

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 now in the admin shell.

```
(user)#
```

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

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

purge Remove all entries configured in the current shell. For example in the `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:

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

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

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

An Administrative Domain (ADOM) defines a set of devices to be controlled by one or more administrators. On a FortiGate unit with multiple VDOMs, each VDOM is managed as separate logical device. VDOMs on the same FortiGate unit can belong to different FortiManager ADOMs.

ADOMs are particularly useful when the FortiManager unit provides management services for several different clients. In previous releases of FortiManager, individual devices were assigned to administrator profiles. In FortiManager 4.0, devices belong to ADOMs and each administrator is assigned an ADOM.

In the initial FortiManager configuration, there is only a root ADOM and one administrator. Administrators other than the `admin` administrator cannot enable, disable, or configure ADOMs.

When ADOMs are enabled, each ADOM (except root) can operate in one of two modes:

Element Management System (EMS) mode is suited to environments with diverse device configurations, including MSSP applications where a single FortiManager unit serves several customers. You can define a custom Web portal for your customers' administrators. When ADOMs are not enabled, the FortiManager unit operating mode is EMS.

Global Management System (GMS) mode is intended for large enterprise users who want to manage device configurations in a highly centralized way with a single set of policies that are pushed out to the devices. You use the Security Console to configure all firewall policies and VPNs.

The root ADOM can operate in EMS mode only. The root ADOM administrator can switch to another ADOM, but cannot log into the ADOM directly. You need to create a specific administrator account for each non-root ADOM.

By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all devices in the device list. By creating ADOMs 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 ADOM.

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 the 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 enterprise client license <license_key>
    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 | enterprise client license | 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.
enterprise client license <license_key>	If policy is enterprise client license, enter the client license key.	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 enterprise client license ip_address os windows_group}	If type is dynamic, select criterion for group membership: dnsdomain — DNS domain enterprise client license — Enterprise Client License 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.

Keywords and variables	Description	Default
<code>type {dynamic static}</code>	Select a group type. static - specify members by name dynamic - define membership by DNS domain, IP address, OS type or Windows group.	static
<code>windows_group <wingrpname></code>	If <code>policy</code> is <code>windows_group</code> , enter the Windows workgroup or domain name.	No default.

History

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

- [execute 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

FortiManager v4.0	New.
--------------------------	------

fcpolicy

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

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

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

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

This chapter contains the following sections:

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

antileak option

Use this command to configure antileak options.

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

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

Syntax

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

Keywords and variables	Description	Default
action {block log}	Set action to take when leakage detected: block - block sending of email suspected of leakage log - log leakage incident	log
enable {enable disable}	Enable or disable Antileak feature.	disable
override {yes no}	Enter yes to configure options for a unit that differ from the group configuration.	no

History

FortiManager v3.0 MR6 New.

Related topics

- [fcpolicy antileak sensword](#)

antileak sensword

Use this command to configure the antileak sensitive word list.

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

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

Syntax

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

Keywords and variables	Description	Default
edit <senswordid>	Enter an integer ID to identify the entry.	No default
sensword <string>	Enter the sensitive word.	No default
override {yes no}	Enter yes to configure options for a unit that differ from the group configuration.	no

History

FortiManager v3.0 MR6 New.

Related topics

- [fcpolicy antileak option](#)

antispam bannedword

Use this command to configure the antispam banned word list.

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

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

Syntax

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

Keywords and variables	Description	Default
bannedword <string>	Enter the sensitive word.	No default
override {yes no}	Enter <i>yes</i> to configure options for a unit that differ from the group configuration.	no

History

FortiManager v3.0 MR6 New.

Related topics

- [fcpolicy antispam blackwhitelist](#)
- [fcpolicy antispam option](#)

antispam blackwhitelist

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

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

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

Syntax

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

Keywords and variables	Description	Default
emailaddress <emailaddr>	Enter the email address.	No default
override {yes no}	Enter <code>yes</code> to configure options for a unit that differ from the group configuration.	no
status {allow block}	Enter <code>allow</code> to add to whitelist. Enter <code>block</code> to add to blacklist.	block

History

FortiManager v3.0 MR6 New.

Related topics

- [fcpolicy antispam bannedword](#)
- [fcpolicy antispam option](#)

antispam option

Use this command to configure antispam options.

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

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

Syntax

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

Keywords and variables	Description	Default
antispam-port <portnum>	Enter the override Antispam server port number.	No default
antispam-server <srv_ip>	Enter the override Antispam server IP address.	No default
antispam-using-override-server {enable disable}	Enable or disable use of override antispam server.	disable
auto_submit {enable disable}	Enable or disable auto-submission of misclassified email to Fortinet.	disable
dont_prompt {enable disable}	Enable if you do not want users prompted to submit misclassified email to Fortinet.	disable
enable_antispam {enable disable}	Enable or disable the antispam feature.	disable
override {yes no}	Enter yes to configure options for a unit that differ from the group configuration.	no

History

FortiManager v3.0 MR6 New.

Related topics

- [fcpolicy antispam bannedword](#)
- [fcpolicy antispam blackwhitelist](#)

antivirus scheduledscan

Use this command to configure antivirus scheduled scan.

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

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

Syntax

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

Keywords and variables	Description	Default
edit <name>	Create or edit a scheduled scan.	
comments <string>	Comments on the scheduled scan.	No default.
day {sunday monday ...}	For weekly scan, enter the days on which the scan runs.	sunday
override {no yes}	Select <code>yes</code> to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no
scan_level {basic full}	Select the scan level.	basic
time {hh:mm}	Enter the scheduled hour and minute.	
type {daily one-time weekly}	Select the scan frequency.	daily

History

FortiManager v3.0 New.

antivirus setting email

Use this command to configure antivirus email scan settings.

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

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

Syntax

```
config fcpolicy antivirus setting email
  set action <action>
  set heuristic <disable | enable>
  set override {no | yes}
  set status {disable | enable}
  set worm-scan <disable | enable>
end
```

Keywords and variables	Description	Default
action <action>	Select <action> when a virus is found in email: log-alert — Log the virus. Send an email alert. strip-quarantine — Quarantine virus email attachment.	log-alert
heuristic <disable enable>	Disable or enable heuristic scan of email attachments.	disable
override {no yes}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no
status {disable enable}	Disable or enable email scanning.	disable
worm-scan <disable enable>	Disable or enable preventing worms from spreading with emails.	disable

History

FortiManager v3.0 New.

antivirus setting realtime

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

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

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

Syntax

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

Keywords and variables	Description	Default
action {clean deny quarantine}	clean — The FortiClient agent attempts to remove the virus from the infected file. If FortiClient cannot clean an infected file, it quarantines the file automatically. deny — You cannot open, run or modify the file until it is cleaned. Quarantine — Move the file to a quarantine directory.	deny
exempt-files <string>	Enter a comma-separated list of file names to exclude from real-time antivirus checking.	No default.
exempt-folders <string>	Enter a comma-separated list of folder names to exclude from real-time antivirus checking.	No default.
exempt-types <string>	Add the file types that you do not want to scan.	No default.
heuristic {disable enable}	Disable or enable heuristic scanning.	disable
max-compress-file-size <integer>	Specify the file size scan limit.	0
override {no yes}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no
scan-compress {no yes}	Specify whether to scan the compressed files.	no
scan-grayware {adware dialer keylogger spyware none}	Specify which grayware to scan.	No default.

Keywords and variables	Description	Default
scan-options <options>	Enter one or more of the following options: network_drives — Scan network drives. reading_from_disk — Scan when reading from disk. writing_to_disk — Scan when writing to disk. none — No scan. To clear all options, enter unset scan-options.	No default.
status <rtstatus>	Set realtime protection status to one of: disable — No realtime protection enable_monitor_startup — Monitor program startup list. enable_realtime_protection — Realtime protection enabled.	No default.

History

FortiManager v3.0

New.

FortiManager v3.0 MR5

Added none option for scan-grayware keyword. Added enable_monitor_startup and enable_realtime_protection options to status.

antivirus setting scheduledscan

Use this command to configure advanced antivirus scheduled scan settings.

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

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

Syntax

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

Keywords and variables	Description	Default
action {clean deny quarantine}	clean — The FortiClient agent attempts to remove the virus from the infected file. If FortiClient cannot clean an infected file, it quarantines the file automatically. deny — You cannot open, run or modify the file until it is cleaned. quarantine — Move the file to a quarantine directory.	
exempt-files <string>	Enter a comma-separated list of file names to exclude from real-time antivirus checking.	No default.
exempt-folders <string>	Enter a comma-separated list of folder names to exclude from real-time antivirus checking.	No default.
exempt-types <string>	Add the file types that you do not want to scan.	No default.
heuristic {disable enable}	Disable or enable heuristic scanning.	disable
max-compress-file-size <integer>	Specify the file size scan limit.	0
override {no yes}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no
pause-scan-on-ups {enable disable}	Pause AV scanning if computer switches to battery power or UPS.	enable
scan-compress {enable disable}	Specify whether to scan the compressed files.	disable
scan-grayware {adware dialer keylogger spyware}	Specify which greyware to scan.	No default.

Keywords and variables	Description	Default
scan-on-insertion {enable disable}	Enable or disable scanning of removable media on insertion.	disable
shellintegrate {enable disable}	Enable or disable integration with Windows Explorer.	disable
signature-warning {enable disable}	Enable or disable notification when virus signature is out-of-date.	disable

History

FortiManager v3.0 New.

FortiManager v4.0 Added pause-scan-on-ups keyword.

firewall address

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

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

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

Syntax

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

Keywords and variables	Description	Default
edit <name>	Create or edit a firewall address.	No default.
comment <string>	Add comments for the firewall address.	No default.
end_ip <ip>	Enter the firewall address' end IP if type is iprange.	No default.
fqdn <fqdn>	Enter the fully-qualified domain name if type is fqdn.	No default.
ip_address <ip>	Enter the IP address. The is available when type is ip.	No default.
ip_mask <ip&netmask>	Enter the firewall IP address and subnet mask. Format: xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx This is available when type is subnet.	No default.
override {no yes}	Select yes if you want this FortiClient PC uses its own firewall address instead of inheriting the address from a group in which this FortiClient PC is a member. Otherwise select no.	no
start_ip <ip>	Enter the firewall address' start IP if type is iprange.	No default.
type {ip iprange subnet fqdn}	Select the firewall address type: ip — single IP address iprange — range of IP addresses subnet — subnet address fqdn — fully-qualified domain name	ip

History

FortiManager v3.0	New.
FortiManager v3.0 MR4	Added ip to type. Added ip_address. Changed subnet to ip_mask.
FortiManager v4.0	Added fqdn option to type. Added fqdn keyword.

firewall addrgrp

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

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

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

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

Syntax

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

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

History

FortiManager v3.0 New.

FortiManager v4.0 Added three built-in address groups: Blocked, Public, and Trusted.

firewall apppolicy

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

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

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

Syntax

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

Keywords and variables	Description	Default
edit <app_policy_id>	Enter a policy ID for this firewall application policy.	No default.
action {allow block}	Select how to respond to the application's connection attempt.	allow
comments <string>	Optionally enter a descriptive comment.	No default.
destination <address_name>	Enter the destination address or address group to which the policy applies. Available addresses include Blocked, Trusted, and Public zones. Use the <code>fcpolicy firewall address</code> command to define addresses.	No default.
override {no yes}	Select <code>yes</code> if you want this FortiClient PC uses its own firewall policy settings instead of inheriting the settings from a group in which this FortiClient PC is a member. Otherwise, select <code>no</code> .	no
protocol <protocol_name>	Select the network protocols to which this policy applies.	<any>
schedule <sched_name>	Select the firewall schedule that controls when the policy should be active.	No default.
service <service_name>	Select the service/application to which the policy applies.	No default.
source <address_name>	Enter the destination address or address group to which the policy applies. Available addresses include Blocked, Trusted, and Public zones. Use the <code>fcpolicy firewall address</code> command to define addresses.	No default.
status {enable disable}	Enable or disable this policy.	disable

History

FortiManager v4.0 MR4 New.

Related topics

- [fcpolicy firewall address](#)
- [fcpolicy firewall addrgrp](#)
- [fcpolicy firewall protocol](#)
- [fcpolicy firewall protocolgrp](#)
- [fcpolicy firewall schedule recurring](#)
- [fcpolicy firewall service](#)

firewall option

Use this command to:

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

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

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

Syntax

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

Keywords and variables	Description	Default
disable-firewall-notify {yes no}	Enter yes to disable FortiTray notification of blocked traffic on the FortiClient PC.	no
firewall-profile <profile_name>	Enter the firewall profile to use: basic_business — Allow all outgoing traffic, allow all incoming traffic from the trusted zone, and deny all incoming traffic from the public zone. basic_home — Allow all outgoing traffic and deny all incoming traffic cust_profile — You can configure firewall policies to control application access to the network and to control traffic between address groups.	basic_home
launch-new-application {allow follow_default}	Select the firewall action when an unknown application tries to communicate through the firewall: allow — Allow the application to communicate, but raise a firewall violation alert. follow_default — Follow the firewall-profile setting. Note: The FortiClient application can be installed with the DEFAULTACTION=1 option, which causes it to always block an unknown application and raise a firewall violation alert.	follow_default
override {no yes}	Select yes if you want this FortiClient PC to use its own firewall option settings instead of inheriting the settings from the group in which this FortiClient PC is a member. Otherwise select no.	no

Keywords and variables	Description	Default
ping-server {enable disable}	Enable the FortiClient application to check ping servers when it is connected to a new network, such as a wireless access point. For information about defining the ping servers, see “fcpolicy firewall pingserver” on page 65	disable
public-zone-level {high medium low}	Set the security level for the public zone. high — Block ICMP, NetBIOS, but allow other traffic coming from this zone. medium — Block ICMP and NetBIOS from this zone, but allow other traffic. Allow NetBIOS to this zone. low — Allow all traffic, except where disallowed by application policies.	high
trusted-zone-level {high medium low}	Set the security level for the trusted zone. high — Block ICMP, NetBIOS, but allow other traffic coming from this zone. medium — Allow all traffic to and from this zone. low — Allow all traffic, except where disallowed by application policies.	medium
trustip-status {enable disable}	Select enable to exempt the addresses defined in fcpolicy firewall trustedip from intrusion prevention scanning.	disable

History

FortiManager v3.0 MR4	New.
FortiManager v3.0 MR5	firewall-default-notice changed to firewall-default-action.
FortiManager v3.0 MR6	Added firewall-profile keyword.
FortiManager v4.0	Removed firewall-default-action. Added launch-new-application, ping-server, public-zone-level, trusted-zone-level, trustip-status keywords.

Related topics

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

firewall pingserver

Use this command to configure ping servers to use with the `ping-server` option in [fcpolicy firewall option](#).

Syntax

```
config fcpolicy firewall pingserver
  edit <pingserver_name>
    set ip_fqdn <ip_fqdn>
  end
```

Variables	Description	Default
edit <pingserver_name>	Enter a name for the ping server.	No default.
ip_fqdn <ip_fqdn>	Enter the IP address or FQDN of the ping server.	No default.

History

FortiManager v4.0 New.

Related topics

- [fcpolicy firewall option](#), see `ping-server {enable | disable}`

firewall policy

Use this command to configure firewall policies.

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

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

Syntax

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

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

History

FortiManager v3.0	New.
FortiManager v3.0 MR4	Added <code>status</code> keyword.
FortiManager v4.0	<code>address</code> replaced by <code>destination</code> and <code>source</code> . <code>direction</code> keyword removed. Added <code>protocol</code> keyword.

Related topics

- [fcpolicy firewall address](#)
- [fcpolicy firewall addrgrp](#)
- [fcpolicy firewall protocol](#)
- [fcpolicy firewall protocolgrp](#)
- [fcpolicy firewall schedule recurring](#)
- [fcpolicy firewall service](#)

firewall protocol

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

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

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

Syntax

```
config fcpolicy firewall protocol
  edit <protocol_name>
    set comment <string>
    set destport <portnum>
    set srcport <portnum>
    set type {tcp | udp | tcpudp | icmp}
  end
```

Variables	Description	Default
edit <protocol_name>	Enter a name for the protocol.	No default.
comment <string>	Optionally, enter a descriptive comment.	No default.
destport <portnum>	Enter the destination port for the protocol.	0
srcport <portnum>	Enter the source port for the protocol.	0
type {tcp udp tcpudp icmp}	Select the type of protocol: TCP, UDP, TCP/UDP or ICMP	tcp

History

FortiManager v4.0 New.

Related topics

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

firewall protocolgrp

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

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

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

Syntax

```
config fcpolicy firewall protocol
  edit <protocol_grp_name>
    set comments <string>
    set member {prot1 prot2 ...}
  end
```

Variables	Description	Default
edit <protocol_grp_name>	Enter a name for this protocol group.	No default.
comments <string>	Optionally, enter a descriptive comment.	No default.
member {prot1 prot2 ...}	Enter the names of the protocols that belong to this group. Use the fcpolicy firewall protocol command to define protocols.	No default.

History

FortiManager v4.0 New.

Related topics

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

firewall schedule recurring

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

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

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

Syntax

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

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

History

FortiManager v3.0 New.

Related topics

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

firewall schedulegrp

Use this command to configure firewall schedule groups.

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

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

Syntax

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

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

History

FortiManager v4.0 New.

Related topics

- [fcpolicy firewall schedule recurring](#)
- [fcpolicy firewall policy](#)
- [fcpolicy firewall apppolicy](#)

firewall service

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

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

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

Syntax

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

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

History

FortiManager v3.0	New.
FortiManager v3.0 MR4	Added ICMP and NETBIOS to <code>type</code> .
FortiManager v4.0	Keywords <code>destinationport</code> , <code>sourceport</code> , and <code>type</code> removed. Configure these in fcpolicy firewall protocol .

Related topics

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

firewall trustedip address

Use this command to define trusted IP addresses, ranges or subnets that are exempt from intrusion detection. Use the [fcpolicy firewall option](#) command to enable trusted IPs.

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

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

Syntax

```
config fcpolicy firewall trustedip address
  edit <addr_name>
    set end_ip <ipv4>
    set ip_address <ipv4>
    set ip_mask <ipv4mask>
    set start_ip <ipv4>
    set type <addr_type>
  end
```

Keywords and variables	Description	Default
edit <addr_name>	Enter a name for the trusted address.	
end_ip <ipv4>	If type is iprange, enter the range end IP address.	0.0.0.0
ip_address <ipv4>	If type is ip, enter the IP address.	0.0.0.0
ip_mask <ipv4mask>	If type is subnet, enter the IP address and netmask.	0.0.0.0 0.0.0.0
start_ip <ipv4>	If type is iprange, enter the range start IP address.	0.0.0.0
type <addr_type>	Select the trusted IP address type: ip — single IP address iprange — range of IP addresses subnet — subnet address	ip

History

FortiManager v3.0 MR5 New.

Related topics

- [fcpolicy firewall option](#)

firewall zone <security_level>

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

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

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

Syntax

```
config fcpolicy firewall <security_level>
  set allow_icmp_in {true | false}
  set allow_netbios_in {true | false}
  set allow_netbios_out {true | false}
  set data_from_zone {allow | deny}
end
```

Keywords and variables	Description	Default
<security_level>	One of: public_high_level — Public zone high security level public_medium_level — Public zone medium security level trusted_high_level — Trusted zone high security level trusted_medium_level — Trusted zone medium security level	
allow_icmp_in {true false}	Allow incoming ICMP traffic.	See table below.
allow_netbios_in {true false}	Allow incoming NETBIOS traffic.	
allow_netbios_out {true false}	Allow outgoing NETBIOS traffic.	
data_from_zone {allow deny}	Allow other traffic from this zone. This is available only for the high security levels. At medium security level, FortiClient always allows this traffic.	

Table 4: Default values for firewall zone security levels

Setting	Public-High	Public-Medium	Trusted-High	Trusted-Medium
allow_icmp_in	false	false	false	true
allow_netbios_in	false	false	false	true
allow_netbios_out	false	true	false	true
data_from_zone	allow	Not applicable	allow	Not applicable

History

FortiManager v4.0

New.

Related topics

- [fcpolicy firewall option](#)

log setting

Use this command to configure logging settings for FortiClient PCs.

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

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

Syntax

```
config fcpolicy log setting
  set custom_field {enable | disable}
  set custom_field_name
  set custom_field_value
  set local_level {error | information | warning}
  set local_maxfilesize <integer>
  set remote_facility <facility>
  set remote_level {error | information | warning}
  set remote_logging {enable | disable}
  set remote_server <serv_addr>
  set remote_server_port <portnum>
  set remote_type {fortianalyzer | syslog}
end
```

Keywords and variables	Description	Default
custom_field {enable disable}	Enable a custom log field to be included in all logs from this FortiClient PC. This field can appear in reports generated on the FortiAnalyzer unit. custom_field_name and custom_field_value define the field name and its value.	disable
custom_field_name	If custom_field is enabled, this is the name of the custom log field.	No default.
custom_field_value	If custom_field is enabled, this is the value of the custom log field.	No default.
local_level {error information warning}	Select the minimum severity of message to log locally.	warning
local_maxfilesize <integer>	Set the log file maximum size (5120 - 3530944 KB).	5120
remote_facility <facility>	Select the facility name to use on the remote log device. To list the facility names, enter set remote_facility ?	local7
remote_level {error information warning}	Select the minimum severity of message to log remotely.	warning
remote_logging {enable disable}	Enable or disable remote logging.	disable
remote_server <serv_addr>	Enter the IP address or hostname of logging server.	No default.
remote_server_port <portnum>	Enter the remote server port number. 0 means default.	0
remote_type {fortianalyzer syslog}	Select the type of logging server: FortiAnalyzer or syslog.	fortianalyzer

History

- FortiManager v3.0 MR5** New. Replaces `fcpolicy log local`, `fcpolicy log remote fortianalyzer`, and `fcpolicy log remote syslog` commands.
- FortiManager v4.0** Added `custom_field`, `custom_field_name`, and `custom_field_value` keywords.

system settings

Use this command to configure FortiClient system settings.

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

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

Syntax

```
config fcpolicy system settings
  set load_at_startup {enable | disable}
  set lockdown_status {enable | disable}
  set raise_alert_to_fmng {enable | disable}
  set override {yes | no}
  set update_server {FortiManager | public | server}
  set update_server_address {ip_address | FQDN}
  set update_server_port <port>
end
```

Keywords and variables	Description	Default
load_at_startup {enable disable}	Enable to load FortiClient Console at startup.	disable
lockdown_status {enable disable}	Enable to lock down FortiClient configuration.	disable
raise_alert_to_fmng {enable disable}	Enable to raise AV alerts to the FortiManager unit.	disable
override {yes no}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no
update_server {FortiManager public server}	Select the source for FortiClient AV/Web Filter/Antispam updates.	public
update_server_address {ip_address FQDN}	Enter the IP address or FQDN of the FDS update server. This is available when update_server is server.	No default.
update_server_port <port>	Enter the port number for updates. This is available when update_server is server.	0

History

FortiManager v3.0 MR4 New.

FortiManager v3.0 MR7 Removed use_fmng_as_update_server. Added update_server, update_server_address and update_server_port.

Related topics

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

system trustedfortimanager

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

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

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

Syntax

```
config fcpolicy system trustedfortimanager
  edit <name>
    set address <ip>
    set comments <string>
    set fqdn <fqdn>
    set type {fqdn | ipmask | iprange | singleip}
    set subnet <ip&netmask>
    set start_ip <ip>
    set end_ip <ip>
  end
```

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

History

FortiManager v3.0	New.
FortiManager v3.0 MR5	Command name changed from <code>misc trustedFMGs</code> .

Related topics

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

system wan_optimization

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

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

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

Syntax

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

Keywords and variables	Description	Default
cache_size <MBytes>	Set maximum disk cache size in MBytes. Range is 256 to 32 768 MBytes. Entry is rounded to nearest 64MBytes (values 256, 320, 384, and so on). If your hard disk can accommodate a larger cache, better optimization performance is possible.	256
override {yes no}	Select <code>yes</code> to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no
protocols {http cifs mapi ftp}	Select the protocols to optimize: HTTP, CIFS, MAPI, or FTP.	No default.
status {enable disable}	Enable or disable WAN optimization.	disable

History

FortiManager v4.0 New.

vpn download

Use this command to configure the FortiClient PC to download VPN configurations from a FortiGate unit running FortiOS 3.0 or 4.0.

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

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

Syntax

```
config fcpolicy vpn download
  edit <name>
    set policy server <string>
    set type automatic
  end
```

Keywords and variables	Description	Default
<code>edit <name></code>	Create or edit a VPN.	No default.
<code>policy server <string></code>	Enter the IP address of the VPN gateway, that is, the FortiGate unit running FortiOS 3.0 that the FortiClient PC connects to.	No default.
<code>type automatic</code>	Select the type of methods used to create VPNs. In this release, only the automatic method is supported.	No default.

History

FortiManager v3.0	New (as <code>fcpolicy vpn</code>).
FortiManager v3.0 MR7	Renamed from <code>fcpolicy vpn</code> .

vpn security_policy

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

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

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

Syntax

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

Keywords and variables	Description	Default
check_antispam {enable disable}	Enable to require that AntiSpam is enabled.	disable
check_firewall {enable disable}	Enable to require that Firewall is enabled.	disable
check_realtime_av {enable disable}	Enable to require that Realtime Protection is enabled.	disable
check_webfilter {enable disable}	Enable to require that WebFilter is enabled.	disable
override {yes no}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no

History

FortiManager v3.0 MR7 New.

webfilter option

The FortiManager unit can act as the local FortiGuard webfilter and antispam service center. As a result, the FortiClient PCs can get the webfiltering and antispam settings from the FortiManager unit instead of from the FortiGuard server through the Internet. If you have a large number of FortiClient PCs, using this feature speeds up the installation of the webfilter and antispam settings.

Use this command to configure the global webfiltering and antispam settings for FortiClient Manager.

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

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

Syntax

```
config fcpolicy webfilter option
  set webfilter-default-action {allow | block}
  set webfilter-dont-rate-ip {enable | disable}
  set webfilter-log-all-urls {enable | disable}
  set webfilter-port <port_num>
  set webfilter-server <fmgi_ip>
  set webfilter-status {enable | disable}
  set webfilter-using-override-server {enable | disable}
end
```

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

History

FortiManager v3.0 MR4	New.
FortiManager v3.0 MR5	Added antispam-using-override-server, webfilter-using-override-server keywords. Removed antispam-status keyword.
FortiManager v3.0 MR6	Moved antispam-port, antispam-server and antispam-using-override-server to fcpolicy antispam option. Added webfilter-log-all-urls keyword.
FortiManager v4.0	Added webfilter-dont-rate-ip keyword.

webfilter profile

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

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

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

Syntax

```
config fcpolicy webfilter profile
  set peruser-status {enable | disable}
  set profile-name <name>
end
```

Keywords and variables	Description	Default
override {yes no}	Select yes to enable modification of settings, otherwise unit uses group settings. This is available only when configuring a unit that belongs to a group.	no
peruser-status {enable disable}	Enable or disable per-user web filtering.	disable
profile-name <name>	Select the webfilter profile to use. The profile must first be configured in fmclient webfilter_profile .	No default.

History

FortiManager v3.0

New.

FortiManager v3.0 MR5Completely re-written. Removed `blocked_categories`, `comments`, `status` keywords. Added `peruser-status` and `profile-name`.

Related topics

- [fmclient webfilter_profile](#)

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 the 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 [execute fmclient enterprise_license download](#) command.

Syntax

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

Keywords and variables	Description	Default
<name>	Enter a name for this client license.	No default.
description <string>	Optionally, enter a description.	null
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
license_key <key_value>	The client license key is generated automatically and is read-only. View it by using the <code>get</code> command.	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
used <seats_used>	The number of client license seats in use. This is read-only. View it by using the <code>get</code> command.	

History

FortiManager v3.0 MR7 New.

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 88](#).

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. q1 — Deploy/retrieve messages q2 — Lockdown/License key messages q3 — Patch update messages q4 — AV update messages	60,60, 120,180
action_queue_length <q1,q2,q3,q4>	Set length of each message queue. q1 — Deploy/retrieve messages q2 — Lockdown/License key messages q3 — Patch update messages q4 — 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 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 emails.	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 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.
validation_type {internal external}	Set validation type for client license key: internal — Validate on FortiManager unit. external — Validate through external facility.	internal

History

FortiManager v3.0 MR7 New.

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 fmclient webfilter_profile .	No default.

The `get` form of the command returns the webfilter 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 webfiltering 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 <grp1_id grp_n_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 <grp1_id grp_n_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

FortiManager v3.0	New.
FortiManager v3.0 MR6	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}
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

History

FortiManager v3.0 MR5 New.

FortiManager v4.0 Added monitor_eventlogging_duration 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 webfilter 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](#)

fmsystem

Use `fmsystem` commands to configure options related to the overall operation of the FortiManager unit. This chapter contains the following sections:

admin profile	global	log fortianalyzer
admin radius	ha	log setting
admin setting	interface	metadata
admin user	locallog disk setting	ntp
alertemail	locallog filter	performance
backup all-settings	locallog fortianalyzer setting	route
certificate ca	locallog memory setting	snmp community
certificate local	locallog syslogd (syslogd2, syslogd3) setting	snmp sysinfo
dm		status
dns		

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

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}
  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.
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.
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.

Keywords and variables	Description
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.
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.

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 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
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.	
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

Keywords and variables	Description	Default
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

FortiManager v3.0	New.
FortiManager v3.0 MR4	Added device_locks, device_sync_status, verify_serial_number.
FortiManager v3.0 MR5	Added japanese option to webadmin_language.
FortiManager v3.0 MR7	device_sync_status default changed to enable.
FortiManager v4.0	Added admin_server_cert, allow_register, offline_mode, register_passwd, unreg_dev_opt.

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 Administrative Domains (ADOMs) .	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.
trusthost1 <ip_mask> trusthost2 <ip_mask> trusthost3 <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 "Using trusted hosts" .	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
Keywords and variables for config meta-data subcommand: Note: 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).

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.

FortiManager v3.0 MR5 Added smtppassword and smtpuser keywords.

Related topics

- [fmsystem backup all-settings](#)

backup all-settings

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

Here is an example of enabling scheduled backups. The backup server is at 172.20.120.11 using the admin account with no password and saving the backup in the /usr/local/backups directory. Backups will be 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/backups
  set week_days monday
  set time 13:00:00
  set protocol ftp
end
```

History

FortiManager v3.0 New.

FortiManager v3.0 MR1 Added crptpasswd variable.

certificate ca

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

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

The process for obtaining and installing certificates is as follows:

- 1 Use the `execute certificate local generate` command to generate a CSR.
- 2 Send the CSR to a CA.

The CA sends you the CA certificate, the signed local certificate and the CRL.

- 3 Use the `fmsystem certificate local` command to install the signed local certificate.
- 4 Use the `fmsystem certificate ca` command to install the CA certificate.

Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

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

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

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

<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](#)
- [execute 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.

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

History

FortiManager v4.0 New.

Related topics

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

dm

Use this command to configure Deployment Manager settings.

Syntax

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

Keywords and variables	Description	Default
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_keepalive_itvl <sec_int>	The interval at which the FortiManager will send a keepalive signal to a FortiGate unit to keep the FortiManager/FortiGate communication protocol active. The interval can be from 30 to 600 seconds.	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

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

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.

global

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

Syntax

```
config fmsystem global
  set fmsystem adom-status {enable | disable}
  set console-output {more | standard}
  set daylightsavetime {enable | disable}
  set hostname <hostname_str>
  set lcdpin <pin_int>
  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 more to pause the output at each full screen until keypress. Select standard 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
hostname <hostname_str>	Enter a name for this FortiManager unit.	FortiManager model name.
lcdpin <pin_int>	Set the 6 digit PIN administrators must enter to use the LCD panel.	No default.
ssl-low-encryption {enable disable}	Enable or disable low-grade (40-bit) encryption.	disable
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

FortiManager v3.0	New. Includes <code>set swapmem</code> and <code>set timezone</code> from v2.8.
FortiManager v3.0 MR1	Added <code>console-output</code> and <code>ssl-low-encryption</code> variables.
FortiManager v3.0 MR3	Added <code>policy-commit-prompt</code> variable.
FortiManager v3.0 MR5	Added <code>global-custom-service</code> , <code>install-used-obj-only</code> , <code>reload-service-overwrite</code> , <code>remoteauthtimeout</code> , <code>revision-control</code> keywords. Removed <code>policy-commit-prompt</code> .
FortiManager v4.0	Added <code>adom-status</code> keyword. Removed <code>global-custom-service</code> , <code>install-used-objs-only</code> , <code>reload-service-overwrite</code> , <code>remoteauthtimeout</code> , and <code>revision-control</code> 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 master to configure the FortiManager unit to be the primary unit in a cluster. Select slave to configure the FortiManager unit to be a backup unit in a cluster. Select standalone to stop operating in HA mode.	
password <password_str>	A group password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.	
config peer	Add peers to the HA configuration of the FortiManager unit. You add all of the backup units as peers to the primary unit (up to 5). For each backup unit you add the primary unit.	
edit <peer_id_int>	Add a peer and add the peer's IP address and serial number.	
ip <peer_ip_ipv4>	Enter the IP address of the peer FortiManager unit.	
serial-number <peer_serial_str>	Enter the serial number of the peer FortiManager unit.	

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.

interface

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 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 — overwrite 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
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.

Related topics

- [fmsystem log setting](#)

locallog filter

Use this command to configure filters for local logs. Enabling a variable logs events in that area. All keywords are visible only when event is enabled.

Syntax

```
config fmsystem locallog 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 rev {disable | enable}
  set rtmon {disable | enable}
  set scfw {disable | enable}
  set scply {disable | enable}
  set scrmgr {disable | enable}
  set scvpn {disable | enable}
  set system {disable | enable}
  set webport {disable | enable}
end
```

Variable	Description	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
lrmgr {disable enable}	Enable to log log and report manager messages.	disable
rev {disable enable}	Enable to log revision history 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

Variable	Description	Default
scvpn {disable enable}	Enable to log VPN console messages.	disable
system {disable enable}	Enable to log system 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 vpnmgr commands. Added devcfg, epmgr, fgd, fgfm, fmwmgr, glbcfg, rev, scfw, scply, scrmgr, scvpn, and webport commands.

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`.

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

Syntax

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

Variable	Description	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 " fmsystem severity {alert critical debug emergency error information notification warning} " on page 127 .	alert
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.

locallog memory setting

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

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 “fmsystem severity {alert critical debug emergency error information notification warning}” on page 127 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.

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

Related topics

- [fmsystem log 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. If you want to use a secure tunnel, you must also enable Secure Connection and configure the FortiManager device's `id` and `psk`, as well as configuring the FortiAnalyzer unit's end of the tunnel.

Syntax

```
config fmsystem log fortianalyzer
  set auto_install {enable | disable}
  set ip <ipv4>
  set localid <id_str>
  set passwd <pass_str>
  set psk <key_str>
  set secure_connection {enable | disable}
  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.
localid <id_str>	Enter the FortiManager unit serial number. This value corresponds to the Local ID field in the GUI. This option is only available when <code>secure_connection</code> is enabled.	No default.
passwd <pass_str>	Enter the FortiAnalyzer administrator password for the account specified in <code>username</code> .	No default.
psk <key_str>	Enter the preshared key which matches the FortiAnalyzer unit's <code>psk</code> . This option is only available when <code>secure_connection</code> is enabled.	No default.
secure_connection {enable disable}	Enable or disable a secure IPSec tunnel for all communications with the FortiAnalyzer unit. If you enable this option, also configure the <code>localid</code> and <code>psk</code> . You must also configure the other endpoint of the tunnel, the FortiAnalyzer unit. For instructions, see the FortiAnalyzer CLI Reference .	disable
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 secure_connection enable
  set localid FMG-3K2404400063
  set psk fGHqm0042x9q
  set username admin
  set passwd wert5W34bNg
end
```

History

FortiManager v3.0	New.
FortiManager v3.0 MR4	Added <code>auto_install</code> .
FortiManager v3.0 MR5	Removed <code>auto_install</code> .
FortiManager v4.0	Added <code>auto_install</code> command.

log setting

Use this command to configure settings for logs.

Syntax

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

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.	10 000 000

Example

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

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

History

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

FortiManager v3.0 MR1 toconsole variable was removed.

FortiManager v3.0 MR3 toconsole variable was added.

FortiManager v3.0 MR4 toconsole variable was removed.

Related topics

- [fmsystem locallog disk setting](#)

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}
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

History

FortiManager v3.0 MR1 New.

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

Related topics

- [execute 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 how often, in minutes, the FortiManager unit synchronizes its time with the NTP server.	60

History

FortiManager v3.0 New.

Related topics

- [execute 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.

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>`.

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
hosts variables		
edit <host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.	
interface <if_name>	Enter the name of the FortiManager unit that connects to the SNMP manager.	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 system 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.

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.

fmupdate

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

This chapter contains the following sections:

- [analyzer virusreport](#)
- [av-ips advanced-log](#)
- [av-ips fct server-override](#)
- [av-ips fgt server-override](#)
- [av-ips push-override](#)
- [av-ips update-schedule](#)
- [av-ips web-proxy](#)
- [disk-quota](#)
- [device-version](#)
- [fct-services](#)
- [server-access-priorities](#)
- [service](#)
- [web-spam fct server-override](#)
- [web-spam fgd-log](#)
- [web-spam fgt server-override](#)
- [web-spam poll-frequency](#)
- [web-spam web-proxy](#)

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-forticlient {enable | disable}
  set log-fortigate {enable | disable}
  set log-server {enable | disable}
end
```

Variables	Description	Default
log-forticlient {enable disable}	Enable or disable logging of FortiGuard Antivirus and IPS service updates of FortiClient installations.	disable
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.

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

FortiManager v3.0 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.

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.

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.

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.

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}	Enable to allow users to permit the FortiGate unit to access public FDS servers.	disable
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
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}
  set web-spam {enable | disable}
end
```

Variables	Description	Default
avips {enable disable}	Enable the built-in FDS to provide FortiGuard Antivirus and IPS updates.	disable
web-spam {enable disable}	Enable FortiGuard Web Filtering and Antispam services for the built-in FDS.	disable

Example

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

History

FortiManager v3.0 MR3 New.

web-spam fct server-override

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

Syntax

```
config fmupdate web-spam 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 server.	disable

Example

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

```
config fmupdate web-spam fct server-override
  set status enable
  set ip 172.16.21.124
  set port 508
end
```

History

FortiManager v3.0 MR4 New.

web-spam fgd-log

Use this command to enable or disable logging of URL and spam lookups (rating queries).

Syntax

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

Variables	Description	Default
spamlog {all nospam}	Select whether to log all spam lookups, or only those where the email rating was not found (it was categorized as "nospam").	nospam
status {enable disable}	Enable or disable logging of FortiGuard Web Filtering and Antispam lookups.	disable
urllog {all miss}	Select whether to log all URL lookups, or only those where the the URL rating was not found (a "miss").	miss

Example

You could configure logging of all URL lookups, but only spam lookups where the resulting category was "nospam".

```
config fmupdate web-spam fgd-log
  set status enable
  set spamlog nospam
  set urllog all
end
```

History

FortiManager v3.0 New.

web-spam fgt server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard Web Filtering and Antispam updates for FortiGate units from the FortiGuard Distribution Network (FDN).

Syntax

```
config fmupdate web-spam 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 server.	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 Web Filtering and Antispam updates for FortiGate units from the FDN.

```
config fmupdate web-spam fgt server-override
  set status enable
  set ip set ip 192.168.22.124
  set port 443
end
```

History

FortiManager v3.0 MR4 New.

web-spam poll-frequency

Use this command to configure the frequency with which the FortiManager unit's built-in FDS should poll the FortiGuard Distribution Network (FDN) for updates to its local copies of the FortiGuard Web Filtering and Antispam rating databases. Up-to-date databases help to ensure rating accuracy and reduce traffic related to rating queries from your network's devices.

Syntax

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

Variables	Description	Default
time <hh:mm>	Enter the FDN polling interval. Hours can be 0-11; minutes can be incremented in ten-minute units, 0 10 20 40 50.	0:10

Example

You could poll the FDN for FortiGuard Web Filtering and antispam updates every two hours and 20 minutes.

```
config fmupdate web-spam poll-frequency
    set time 2:20
end
```

History

FortiManager v3.0 New.

web-spam web-proxy

Use this command to configure a web proxy if the built-in FDS must retrieve FortiGuard Web Filtering and Antispam updates through a web proxy.

Syntax

```
config fmupdate web-spam
  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>	Enter the password of the web proxy.	No default.
port <port_int>	Enter the port of the web proxy.	80
status {enable disable}	Enable or disable the web proxy.	disable
username <username_str>	Enter the user name of the web proxy.	No default.

Example

You could enable the use of FortiGuard Web Filtering and Antispam updates through a web proxy that requires authentication.

```
config fmupdate web-spam web-proxy
  set status enable
  set ip 10.10.10.3
  set port 443
  set username wfasupdates
  set password 123456
end
```

History

FortiManager v3.0 New.

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 the following sections:

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

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

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

Related topics

- [execute 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

- [execute 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

- [execute certificate local](#)

certificate local

Use these commands to list local certificates, and to import or export local certificates. To generate a certificate request, see [“execute certificate local generate” on page 172](#).

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

- [execute certificate local generate](#)
- [execute 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"> the FortiManager unit IP address the fully qualified domain name of the FortiManager unit an email address that identifies the FortiManager unit An IP address or domain name is preferable to an email address.
<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 "Optional information variables" for the list of optional information variables. You must enter the optional variables in the order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list. For example, to enter the 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

- [execute 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 2004:

```
execute date 09/17/2004
```

History

FortiOS v2.80 MR4 New.

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

Related topics

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

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

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

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

FortiManager v3.0 MR1	New.
FortiManager v3.0 MR5	<devicename> replaced <device_name> to identify device.
FortiManager v4.0	<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](#)

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

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

Related topics

- [execute 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

FortiManager v4.0	New.
-------------------	------

Related topics

- [execute 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

- [execute 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

- [execute 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

FortiManager v4.0	New.
--------------------------	------

Related topics

- [execute 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

- [execute fcpolicy group](#)

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

- [execute 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

- [execute 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

FortiManager v4.0	New.
--------------------------	------

Related Topics

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

FortiManager v3.0 MR5	New.
FortiManager v3.0 MR6	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

- [execute 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

- [execute 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 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

- [execute fmclient license_key list](#)
- `config` [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

- [execute fmclient license_key deploy](#)
- [config 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 [execute fmclient package list](#) command to determine the value of <package_version_id>.

History

FortiManager v3.0 MR7 New.

Related commands

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

- [execute fmclient package list](#)
- [execute 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 [execute fmclient package list](#) command to determine the value of <package_id>.

History

FortiManager v3.0 MR6 New.

Related commands

- [execute fmclient package list](#)
- [execute 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.

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 v4.0

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> { 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.
{ 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

FortiManager v4.0	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 FortiGuard service packages to the built-in FDS, including initializing the databases required by the FortiManager unit's built-in FDS to provide FortiGuard Web Filtering and Antispam to requesting devices.

You will be asked to confirm the command.

Syntax

```
execute fmupdate {ftp | tftp} import {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.
{fct fds spam url}	Select the type of file to import.
<filename_str>	Enter the name of the file to download.
<server_ipv4>	Enter the FQDN or IP address of the FTP or TFTP server
<path_str>	Enter the directory of the file to download (FTP server only). If the directory name includes spaces, use quotes around it.
<user_str>	Enter the user name to use to log into the server (FTP server only).
<password_str>	Enter the password to use to log into the server (FTP server only).

Example

You might initialize your FortiManager unit by importing a file called FMGWFASDBbackup located on the server 172.31.22.124 in /usr/local/backups/ using the protocol ftp, a user name of admin and a password of adminpwd.

```
execute fmupdate ftp import fds FMGWFASDBbackup 172.31.22.124
/usr/local/backups/ admin adminpwd
```

History

FortiManager v3.0 New.

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

- [execute 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

FortiManager v3.0	New.
FortiManager v3.0 MR5	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

FortiManager v3.0	New.
FortiManager v3.0 MR5	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

- [execute traceroute](#)

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

- [execute reset](#)
- [execute restore](#)
- [execute 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

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

Related topics

- [execute restore](#)
- [execute 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>
    <password_str>

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

FortiManager v3.0 New.

FortiManager v3.0 MR5 Added `dpm`, `fortianalyzer_package`, `sm`, and `<backuptype>` keywords.

FortiManager v4.0 Removed the `config`, `database`, `dpm`, `fortianalyzer_package`, and `sm` 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

- [execute reboot](#)
- [execute 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

- [execute 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

- [execute 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	bdfldush
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

- [execute ping](#)

Index

A

- accept_ports
 - fmclient discovery, 90
- accepting FortiClient requests for management, 90
- accprofile
 - fmsystem admin, 109
- action
 - fcpolicy antivirus setting realtime, 55
 - fcpolicy antivirus setting scheduledscan, 57
 - fcpolicy firewall policy, 61, 66
- action_queue_interval
 - fmclient communication_setting, 89
- action_queue_length
 - fmclient communication_setting, 89
- address
 - fcpolicy misc trustedFMGs, 78
- address_ipv4
 - execute traceroute, 223
- address, destination in FCM firewall policy, 61, 66
- admin profile
 - fmsystem, 102, 142
- admin user
 - fmsystem, 109
- administrative access, 125
- administrator accounts, 109
- administrator profile, 102, 142
- allowaccess
 - fmsystem interface, 125
- all-settings
 - execute restore, 218
- antispam-port
 - fcpolicy antispam option, 52
- antispam-server
 - fcpolicy antispam option, 52
- antispam-using-override-server
 - fcpolicy antispam option, 52
- antivirus scheduledscan
 - fcpolicy, 53
- antivirus setting email
 - fcpolicy, 54
- antivirus setting realtime
 - fcpolicy, 55
- antivirus setting scheduledscan
 - fcpolicy, 57
- archiving, 168
- auto_submit
 - fcpolicy antispam option, 52
- av-ips fct server-override
 - fmupdate, 150
- av-ips fgt server-override
 - fmupdate, 151
- av-ips push-override
 - fmupdate, 152
- av-ips web-proxy
 - fmupdate, 154

B

- backing up
 - on demand, 168
- backup
 - execute, 168
- bootimage
 - execute, 169

C

- certificate
 - vpn ca, 115
 - vpn local, 116
- checksum
 - fcpolicy firewall service, 72
- CLI basics, 32
- CLI session, 188
- CLI structure, 27
- client licenses, FortiClient
 - listing, 190
- cluster, 122
- cluster secondary
 - fmclient, 87
- cluster setting
 - fmclient, 88
- command abbreviation, 33
- command completion, 32
- command help, 32
- comments, documentation, 11
- communication_setting
 - fmclient, 89
- compression
 - fmsystem log settings, 137
- config, 28
- config router, 15, 147
- configuration file, 210
- configuration file, importing, 210
- connecting
 - to the CLI, 24
 - to the CLI using SSH, 26
 - to the FortiManager console, 24
- connection
 - ping test, 215
 - traceroute test, 223
- console baudrate
 - execute, 173
- contact-info
 - system snmp sysinfo, 145
- CPU, 140
- CPU usage, SNMP event, 142
- cryptpasswd
 - execute backup all-settings, 168
- csv
 - fmsystem locallog syslogd setting, 133
- customer service, 11

D

- database configuration, restoring, 218
- date
 - execute, 174
- date_str
 - execute date, 174
- Daylight Saving Time, 120
- daylightsavetime
 - fmsystem global, 120
- delete, table shell command, 27
- Deployment Manager, 117
- description
 - fcdevice ungroup, 43
 - fmsystem admin user, 109, 112
 - system snmp sysinfo, 145
- destination
 - fcpolicy firewall policy, 61, 66
- device
 - fmsystem route, 141
- device lock enable, 107
- device_locks
 - fmsystem admin setting, 107
- device_name
 - execute fgt-cli-access, 188
- device_sync_status
 - fmsystem admin setting, 107
- directory
 - fmsystem backup, 113
- disable_auto_vacuum
 - fmclient communication_setting, 89
- disable-firewall-notify
 - fcpolicy firewall option, 63
- discovery
 - fmclient, 90
- diskfull
 - fmsystem locallog, 126
 - fmsystem locallog disk setting, 126
- dm
 - fmsystem locallog filter, 129
- dns
 - fmsystem, 117
- DNS servers, 119
- dns_domain
 - fcdevice group, 40
 - fcdevice temp (get), 42
- documentation
 - commenting on, 11
 - Fortinet, 11
- dont_prompt
 - fcpolicy antisipam option, 52
- dst
 - fmsystem route, 141

E

- edit
 - fcdevice group, 40
 - fcdevice ungroup, 43
- edit, table shell command, 27
- editing commands, 33
- editing the configuration file, 35

- enable_antisipam
 - fcpolicy antisipam option, 52
- encrypted password support, 34
- end
 - command in a table shell, 27
 - command in an edit shell, 28
- end_ip
 - fcpolicy firewall address, 59
 - fcpolicy misc trustedFMGs, 78
- enterprise license, FortiClient
 - downloading, 193
 - listing, 194
- enterprise_license
 - fmclient, 92
- event
 - fmsystem locallog filter, 129
- events
 - system snmp communities, 142
- example command sequences, 31
- executable
 - fcpolicy firewall service, 72
- execute, 167
- exempt-files
 - fcpolicy antivirus setting realtime, 55
 - fcpolicy antivirus setting schedulescan, 57
- exempt-folders
 - fcpolicy antivirus setting realtime, 55
 - fcpolicy antivirus setting schedulescan, 57
- exempt-types
 - fcpolicy antivirus setting realtime, 55
 - fcpolicy antivirus setting scheduledscan, 57

F

- facility
 - fmsystem locallog syslogd setting, 133
- failure detection time
 - HA, 123
- fcdevice search
 - execute, 181
- fcpolicy deploy
 - execute, 182
- fcpolicy group
 - execute, 184
- fcpolicy retrieve
 - execute, 185
- fcpolicy unit
 - execute, 187
- fct ip address
 - fmupdate av-ips fct server-override, 150
- fct-services
 - fmupdate, 157
- fgt ip address
 - fmupdate av-ips fgt server-override, 151
- fgt-cli-access
 - execute, 188
- file
 - execute fmupdate, 210
- filename
 - execute backup, 168
 - execute restore, 218

- filesize
 - fcpolicy firewall service, 72
- firewall address
 - fcpolicy, 59
- firewall addrgrp
 - fcpolicy, 60
- firewall policy
 - fcpolicy, 66
- firewall schedule recurring
 - fcpolicy, 70
- firewall service
 - fcpolicy, 72
- firmware image, uploading, 218
- flash disk, 140
- fmclient apply-lockdown
 - execute, 189
- fmclient client_license list
 - execute, 190
- fmclient cluster
 - execute, 192
- fmclient enterprise_license download
 - execute, 193
- fmclient enterprise_license list
 - execute, 194
- fmclient group refresh
 - execute, 195
- fmclient license_key deploy
 - execute, 196
- fmclient license_key list
 - execute, 197
- fmclient package delete
 - execute, 199
- fmclient package deploy
 - execute, 200
- fmclient package download
 - execute, 201
- fmclient package list
 - execute, 202
- fmupdate
 - execute, 210
 - server-access-priorities, 158
- fmwmgr
 - fmsystem locallog filter, 129
- format disk
 - execute, 211
- FortiAnalyzer
 - configuring, 135
- FortiClient
 - configuring communication settings, 89
- FortiClient group administrators, 93
- FortiGate documentation
 - commenting on, 11
- FortiGate SNMP agent, 145
- FortiGate, IP address, 188
- FortiLog
 - configuring access, 135
- FortiManager
 - rebooting, 216
 - server hostname, 120
 - shutting down, 219
 - trustedfortimanager setting, 78

- FortiManager, resetting, 217
- Fortinet customer service, 11
- Fortinet documentation, 11
- Fortinet Knowledge Center, 11
- fqdn
 - fcpolicy misc trustedFMGs, 78

G

- gateway
 - fmsystem route, 141
- get
 - command in a table shell, 27
 - command in an edit shell, 28
- get_configurations
 - execute fortianalyzer, 212
- global
 - fmsystem, 120
- global settings, 120
- group
 - fcdevice, 40
 - for FortiClient group administrator, 93
- group_admin
 - fmclient, 93
- grouptype
 - fcdevice group, 41

H

- HA, 122
 - failure detection time, 123
 - synchronization interface, 122
 - synchronization port, 122
- ha
 - fmsystem, 122
 - fmsystem locallog filter, 129
- hard disk
 - formatting, 211
 - performance status, 140
- hb-interval
 - fmsystem ha, 122
- hb-lost-threshold
 - fmsystem ha, 123
- heuristic
 - fcpolicy antivirus setting email, 54
 - fcpolicy antivirus setting realtime, 55
 - fcpolicy antivirus setting scheduledscan, 57
- high availability, 122
- host-name
 - execute traceroute, 223
- hostname
 - fmsystem global, 120
- HTTP, 125
- HTTPS, 125

I

- ICMP echo request, 215
- image
 - execute restore, 218

- interface
 - bringing up or down, 125
 - configuring, 125
 - fmsystem, 125
 - system snmp community hosts, 143
- International characters, 35
- introduction
 - Fortinet documentation, 11
- ip
 - execute backup, 168
 - fcdevice temp (get), 42
 - fmsystem interface, 125
 - fmsystem log fortianalyzer, 135
 - fmupdate av-ips fgt server-override, 151
 - fmupdate av-ips server-override, 150
 - fmupdate av-ips web-proxy, 154
 - fmupdate web-spam web-proxy, 165
 - system snmp community hosts, 143
- IP address formats, 35
- ip_address
 - fcdevice group, 40
 - fcpolicy firewall address, 59
- L**
- LCD PIN, setting, 120
- lcdpin
 - fmsystem global, 120
- level
 - fmsystem log setting, 137
- license keys, FortiClient
 - deploying, 196
 - listing, 197
- license, FortiClient enterprise
 - setting validation type, 92
- line continuation, 33
- load_at_startup
 - fcpolicy system settings, 77
- local_level
 - fcpolicy log setting, 75
- local_maxfilesize
 - fcpolicy log setting, 75
- localid
 - fmsystem log fortianalyzer, 135
- locallog disk setting
 - fmsystem, 126
- locallog filter
 - fmsystem, 129
- locallog fortianalyzer setting
 - fmsystem, 131
- locallog memory setting
 - fmsystem, 132
- locallog syslogd setting
 - fmsystem, 133
- location
 - system snmp sysinfo, 145
- lockdown
 - fmclient, 97
- lockdown_status
 - fcpolicy system settings, 77

- log filter settings, 129
- log fortianalyzer
 - fmsystem, 135
- log setting
 - fmsystem, 137
- log settings, 126
 - syslogd, 133
- log-alert
 - action for fcpolicy antivirus setting email, 54
- lrmgr
 - fmsystem locallog filter, 129

M

- max-log-file-size
 - fmsystem locallog, 126
 - fmsystem locallog disk setting, 126
- member
 - fcdevice group, 40
 - fcpolicy firewall addrgrp, 60
 - fcpolicy firewall svcgrp, 71
- memory
 - enabling virtual memory, 120
 - sage statistics, 140
- min_message_interval
 - fmclient communication_setting, 89
- month, setting, 174

N

- name
 - system snmp community, 143
- newclient_action
 - fmclient discovery, 90
- next, 28
- ntp
 - fmsystem, 138
- NTP server, configuring, 138

O

- option access_ungroup
 - for FortiClient group administrator, 93
- os_name
 - fcdevice group, 40
- override
 - fcpolicy antivirus scheduledscan, 53, 54, 55, 57
 - fcpolicy firewall address, 59
 - fcpolicy firewall addrgrp, 60, 63
 - fcpolicy firewall policy, 61, 66
 - fcpolicy firewall service, 72
 - fcpolicy firewall svcgrp, 71

P

- packet type, 210
- passwd
 - fmsystem backup, 113
 - fmsystem log fortianalyzer, 135

- password
 - execute backup, 168
 - execute restore, 218
 - fmclient lockdown, 97
 - fmsystem admin user, 109
 - fmupdate av-ips web-proxy, 154
 - fmupdate web-spam web-proxy, 165
 - for backup server, 113
- path
 - execute backup all-settings, 168
 - execute fmupdate, 210
- performance
 - fmsystem, 140
 - get fmsystem, 140
- performance statistics, 140
- ping, 125
 - execute, 215
- platform
 - in get fmsystem status, 146
- policy
 - fcdevice group, 40
 - fcpolicy vpn, 80
- port
 - bringing up or down, 125
 - configuring, 125
 - fmsystem locallog syslogd setting, 133
 - fmupdate av-ips fct server-override, 150
 - fmupdate av-ips fgt server-override, 151
 - fmupdate av-ips push-override, 152
 - fmupdate av-ips server-override, 150
 - fmupdate av-ips web-proxy, 154
 - fmupdate fct-services, 157
 - fmupdate web-spam web-proxy, 165
- primary
 - fmsystem dns, 119
- primary image, 169
- processes, viewing, 222
- profileid
 - fmsystem admin user, 109
- protocol
 - fmsystem backup, 113
- psk
 - fmsystem log fortianalyzer, 135
- psk, preshared key
 - for FortiAnalyzer, 135
- purge, 28

Q

- query-v1-port
 - system snmp community, 143
- query-v1-status
 - system snmp community, 143
- query-v2c-port
 - system snmp community, 143
- query-v2c-status
 - system snmp community, 143

R

- raise_alert_to_fmg
 - fcpolicy system settings, 77
- reboot
 - execute, 216
- recalling commands, 32
- remote_facility
 - fcpolicy log setting, 75
- reset
 - execute, 217
- resources, viewing, 222
- restore
 - execute, 218
- roll-schedule
 - fmsystem locallog, 126
 - fmsystem locallog disk setting, 126
- rotatesize
 - fmsystem log setting, 137
- route
 - fmsystem, 141
- routing
 - configuring for FortiManager, 141
 - gateway, 141
 - ip, 141
 - port, 141
- rtmon
 - fmsystem locallog filter, 129

S

- scan_level
 - fcpolicy antivirus scheduledscan, 53
- scan-compress
 - fcpolicy antivirus setting realtime, 55
 - fcpolicy antivirus setting scheduledscan, 57
- scan-grayware
 - fcpolicy antivirus setting realtime, 55
 - fcpolicy antivirus setting scheduledscan, 57
- schedule
 - fcpolicy firewall policy, 61, 66
- secondary
 - fmsystem dns, 119
- secondary image, 169
- secure_connection
 - fmsystem log fortianalyzer, 135
- send_all_configurations
 - execute fortianalyzer, 213
- send_configurations
 - execute fortianalyzer, 214
- serial connection, 173
- serial number
 - in get fmsystem status, 146
- server
 - fmsystem backup, 113
 - fmsystem locallog syslogd setting, 133
 - fmsystem ntp, 139
- service
 - fcpolicy firewall policy, 61, 66
- set, 28
- setting administrative access for SSH or Telnet, 25

- severity
 - fmsystem locallog, 127
 - fmsystem locallog disk setting, 127, 134
 - fmsystem locallog fortianalyzer setting, 131
 - fmsystem locallog memory setting, 132
 - fmsystem locallog syslogd, 134
- shutdown
 - execute, 219
- SNMP
 - v1, 143
 - v2c, 143
- snmp community
 - system, 142
- snmp sysinfo
 - system, 145
- software upgrade packages, FortiClient
 - deleting, 199
- spaces, entering in strings, 34
- spamlog
 - fmupdate web-spam fgd-log, 162
- special characters, where they are allowed, 35
- ssh, 125
- ssh-public-key
 - fmsystem admin user, 110
- start_ip
 - fcpolicy firewall address, 59
 - fcpolicy misc trustedFMGs, 78
- status
 - fcpolicy antivirus setting email, 54
 - fcpolicy antivirus setting realtime, 56
 - fmclient lockdown, 97
 - fmsystem, 146
 - fmsystem backup, 113
 - fmsystem interface, 125
 - fmsystem locallog, 127, 134
 - fmsystem locallog disk setting, 127, 134
 - fmsystem locallog fortianalyzer setting, 131
 - fmsystem locallog memory setting, 132
 - fmsystem log fortianalyzer, 135
 - fmsystem ntp, 139
 - fmupdate av-ips fct server-override, 150
 - fmupdate av-ips fgt server-override, 151
 - fmupdate av-ips push-override, 152
 - fmupdate av-ips web-proxy, 154
 - fmupdate fct-services, 157
 - fmupdate web-spam fgd-log, 162
 - fmupdate web-spam web-proxy, 165
 - system snmp community, 143
 - system snmp sysinfo, 145
- strip-quarantine
 - action for fcpolicy antivirus setting email, 54
- subnet
 - fcpolicy firewall address, 59
 - fcpolicy misc trustedFMGs, 78
- swapmem
 - fmsystem global, 120
- sync_interval
 - fmsystem ntp, 139
- synchronization interface
 - HA, 122
- synchronization port
 - HA, 122
 - See also synchronization interface, 122

- system
 - fmsystem locallog filter, 130
- system settings
 - fcpolicy, 77
- system trustedfortimanager
 - fcpolicy, 78

T

- technical support, 11
- temp
 - fcdevice, 42
- time
 - execute, 221
 - fcpolicy antivirus scheduledscan, 53
 - fmsystem backup, 113
 - fmupdate web-spam poll-frequency, 164
 - setting automatically, 138
- time zone, setting, 120
- timezone
 - fmsystem global, 120
- top
 - execute, 222
- traceroute
 - execute, 223
- trap-v1-rport
 - system snmp community, 143
- trap-v1-status
 - system snmp community, 143
- trap-v2c-rport
 - system snmp community, 143
- trap-v2c-status
 - system snmp community, 143
- trusted FortiManager
 - setting, 78
- trusted hosts
 - administrator, 110
 - security issues, 110
- trusthost
 - fmsystem admin user, 110
- type
 - execute fmupdate, 210
 - fcdevice group, 41
 - fcpolicy antivirus scheduledscan, 53
 - fcpolicy firewall address, 59
 - fcpolicy misc trustedFMGs, 78
- type automatic
 - fcpolicy vpn, 80

U

- uid
 - fcdevice temp (get), 42
- ungroup
 - fcdevice, 43
- unit
 - fcdevice, 44
- unset, 28
- update_server
 - fcpolicy system settings, 77
- update_server_address
 - fcpolicy system settings, 77

- update_server_port
 - fcpolicy system settings, 77
- upload
 - fmsystem locallog, 127
 - fmsystem locallog setting, 127
- upload-delete-files
 - fmsystem locallog disk setting, 127
- uploadaddr
 - fmsystem locallog disk setting, 127
- uploadip
 - fmsystem locallog disk setting, 127
- uploadpass
 - fmsystem locallog disk setting, 127
- uploadport
 - fmsystem locallog disk setting, 127
- uploadsched
 - fmsystem locallog disk setting, 127
- upload-time
 - fmsystem locallog disk setting, 127
- uploadtype
 - fmsystem locallog disk setting, 127
- uploaduser
 - fmsystem locallog disk setting, 127
- uploadzip
 - fmsystem locallog disk setting, 127
- urlog
 - fmupdate av-ips push-override, 152
 - fmupdate web-spam fgd-log, 162
- user
 - execute fmupdate, 210
 - fmsystem backup, 113
- username
 - execute backup, 168
 - execute fgt-cli-access, 188
 - execute restore, 218
 - fmsystem log fortianalyzer, 135
 - fmupdate av-ips web-proxy, 154
 - fmupdate web-spam web-proxy, 165
- using the CLI, 23

V

- validation_type
 - fmclient, 92
- verify_serial_number
 - fmsystem admin setting, 108
- version
 - in get fmsystem status, 146

- virtual memory, 120
- vpn, 115
- vpn download
 - fcpolicy, 80
- VPN security policy, 81
- vpn security_policy
 - fcpolicy, 81

W

- webfilter option
 - fcpolicy, 82
- webfilter profile
 - fcpolicy, 83
- webfilter-default-action
 - fcpolicy webfilter option, 82
- webfilter-log-all-urls
 - fcpolicy webfilter option, 82
- webfilter-port
 - fcpolicy webfilter option, 82
- webfilter-server
 - fcpolicy webfilter option, 82
- webfilter-status
 - fcpolicy webfilter option, 82
- webfilter-using-override-server
 - fcpolicy webfilter option, 82
- web-spam fgd-log
 - fmupdate, 162
- web-spam poll-frequency
 - fmupdate, 164
- web-spam server-access-priorities
 - fmupdate, 165
- web-spam server-override
 - fmupdate, 165
- web-spam web-proxy
 - fmupdate, 165
- week_days
 - fmsystem backup, 113
- windows_group
 - fcdevice group, 41
- worm-scan
 - fcpolicy antivirus setting email, 54

Y

- year, setting, 174



www.fortinet.com



www.fortinet.com