

FortiManager - CLI Reference

VERSION 5.4.3

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

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

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



September 18, 2017

FortiManager 5.4.3 CLI Reference

02-543-310521-20170918

TABLE OF CONTENTS

| | |
|--|-----------|
| Change Log | 12 |
| Introduction | 13 |
| About the FortiManager system | 13 |
| FortiManager feature set | 13 |
| FortiAnalyzer feature set | 13 |
| FortiManager documentation | 13 |
| What's New in FortiManager 5.4 | 15 |
| FortiManager 5.4.3 | 15 |
| FortiManager 5.4.2 | 15 |
| FortiManager 5.4.1 | 17 |
| FortiManager 5.4.0 | 18 |
| Using the Command Line Interface | 22 |
| CLI command syntax | 22 |
| Connecting to the CLI | 23 |
| Connecting to the FortiManager console | 23 |
| Setting administrative access on an interface | 24 |
| Connecting to the FortiManager CLI using SSH | 24 |
| Connecting to the FortiManager CLI using the GUI | 25 |
| CLI objects | 25 |
| CLI command branches | 25 |
| config branch | 26 |
| get branch | 28 |
| show branch | 30 |
| execute branch | 30 |
| diagnose branch | 30 |
| Example command sequences | 31 |
| CLI basics | 32 |
| Command help | 32 |
| Command tree | 32 |
| Command completion | 32 |
| Recalling commands | 32 |
| Editing commands | 32 |
| Line continuation | 33 |
| Command abbreviation | 33 |

| | |
|--|-----------|
| Environment variables | 33 |
| Encrypted password support | 33 |
| Entering spaces in strings | 34 |
| Entering quotation marks in strings | 34 |
| Entering a question mark (?) in a string | 34 |
| International characters | 34 |
| Special characters | 35 |
| IPv4 address formats | 35 |
| Changing the baud rate | 35 |
| Debug log levels | 35 |
| Administrative Domains | 36 |
| ADOMs overview | 36 |
| Configuring ADOMs | 37 |
| Concurrent ADOM Access | 38 |
| system | 40 |
| admin | 40 |
| admin group | 40 |
| admin ldap | 41 |
| admin profile | 42 |
| admin radius | 48 |
| admin setting | 49 |
| admin tacacs | 52 |
| admin user | 54 |
| alert-console | 61 |
| alert-event | 62 |
| alertemail | 65 |
| auto-delete | 66 |
| backup all-settings | 67 |
| certificate | 68 |
| certificate ca | 68 |
| certificate crt | 69 |
| certificate local | 69 |
| certificate oftp | 70 |
| certificate ssh | 71 |
| dm | 71 |
| dns | 73 |
| fips | 74 |
| fortiview setting | 74 |
| fortiview autocache settings | 75 |
| global | 75 |
| Time zones | 80 |
| ha | 82 |

| | |
|---|------------|
| General FortiManager HA configuration steps | 84 |
| interface | 85 |
| locallog | 86 |
| locallog setting | 87 |
| locallog disk setting | 87 |
| locallog filter | 90 |
| locallog fortianalyzer (fortianalyzer2, fortianalyzer3) setting | 92 |
| locallog memory setting | 93 |
| locallog syslogd (syslogd2, syslogd3) setting | 93 |
| log | 95 |
| log alert | 95 |
| log breach-detect | 96 |
| log mail-domain | 96 |
| log settings | 96 |
| log-fetch | 99 |
| log-fetch client-profile | 100 |
| log-fetch server-setting | 102 |
| mail | 102 |
| metadata | 103 |
| ntp | 104 |
| password-policy | 104 |
| report | 105 |
| report auto-cache | 105 |
| report est-browse-time | 106 |
| report group | 106 |
| report setting | 107 |
| route | 108 |
| route6 | 108 |
| snmp | 109 |
| snmp community | 109 |
| snmp sysinfo | 112 |
| snmp user | 113 |
| sql | 115 |
| syslog | 118 |
| workflow approval-matrix | 119 |
| fmupdate | 120 |
| analyzer virusreport | 120 |
| av-ips | 120 |
| av-ips advanced-log | 121 |
| av-ips fct server-override | 121 |
| av-ips fgt server-override | 122 |
| av-ips push-override | 123 |

| | |
|--------------------------------------|------------|
| av-ips push-override-to-client | 124 |
| av-ips update-schedule | 124 |
| av-ips web-proxy | 125 |
| custom-url-list | 126 |
| disk-quota | 127 |
| fct-services | 127 |
| fds-setting | 128 |
| multilayer | 129 |
| publicnetwork | 129 |
| server-access-priorities | 130 |
| server-override-status | 131 |
| service | 132 |
| web-spam | 132 |
| web-spam fct server-override | 132 |
| web-spam fgd-log | 133 |
| web-spam fgd-setting | 134 |
| web-spam fgt server-override | 136 |
| web-spam fsa server-override | 137 |
| web-spam poll-frequency | 137 |
| web-spam web-proxy | 137 |
| execute | 139 |
| add-on-licence | 139 |
| add-vm-license | 140 |
| backup | 140 |
| bootimage | 142 |
| certificate | 142 |
| certificate ca | 142 |
| certificate local | 143 |
| chassis | 144 |
| console baudrate | 145 |
| date | 145 |
| device | 146 |
| dmserver | 146 |
| dmserver delrev | 146 |
| dmserver revlist | 147 |
| dmserver showconfig | 147 |
| dmserver showdev | 147 |
| dmserver showrev | 147 |
| erasedisk | 148 |
| factory-license | 148 |
| fgfm reclaim-dev-tunnel | 148 |
| fmpolicy | 148 |

| | |
|---------------------------------------|-----|
| fmppolicy check-upgrade-object | 149 |
| fmgppolicy clone-adom-object | 149 |
| fmppolicy copy-adom-object | 149 |
| fmppolicy install-config | 150 |
| fmppolicy print-adom-database | 150 |
| fmppolicy print-adom-object | 150 |
| fmppolicy print-adom-package | 151 |
| fmppolicy print-device-database | 151 |
| fmppolicy print-device-object | 152 |
| fmppolicy print-prov-templates | 152 |
| fmppolicy print-prov-database | 153 |
| fmppolicy promote-adom-object | 153 |
| fmppolicy upload print log | 153 |
| fmprofile | 154 |
| fmprofile copy-to-device | 154 |
| fmprofile delete-profile | 154 |
| fmprofile export-profile | 154 |
| fmprofile import-from-device | 155 |
| fmprofile import-profile | 155 |
| fmprofile list-profiles | 155 |
| fmscript | 156 |
| fmscript clean-sched | 156 |
| fmscript copy | 156 |
| fmscript delete | 156 |
| fmscript import | 157 |
| fmscript list | 157 |
| fmscript run | 158 |
| fmscript showlog | 158 |
| fmupdate | 159 |
| fmupdate cdrom | 160 |
| format | 160 |
| iotop | 161 |
| iotps | 161 |
| log | 162 |
| log device disk_quota | 162 |
| log device permissions | 163 |
| log device vdom | 163 |
| log dlp-files clear | 164 |
| log import | 164 |
| log ips-pkt clear | 164 |
| log quarantine-files clear | 165 |
| log-fetch | 165 |

| | |
|-------------------------------|------------|
| log-fetch client | 165 |
| log-fetch server | 166 |
| log-integrity | 166 |
| lvm | 166 |
| max-dev-licence | 167 |
| migrate | 168 |
| ping | 168 |
| ping6 | 168 |
| raid | 169 |
| reboot | 169 |
| remove | 169 |
| reset | 170 |
| reset-sqllog-transfer | 170 |
| restore | 171 |
| sdns | 172 |
| sensor | 173 |
| shutdown | 173 |
| sql-local | 173 |
| sql-local rebuild-adom | 174 |
| sql-local rebuild-db | 174 |
| sql-local rebuild-index | 174 |
| sql-local remove-db | 174 |
| sql-local remove-logs | 175 |
| sql-query-dataset | 175 |
| sql-query-generic | 175 |
| sql-report | 176 |
| ssh | 177 |
| ssh-known-hosts | 178 |
| tac | 178 |
| time | 178 |
| top | 179 |
| traceroute | 180 |
| traceroute6 | 180 |
| diagnose | 181 |
| auto-delete | 181 |
| cdb check | 182 |
| debug | 183 |
| debug application | 183 |
| debug cli | 186 |
| debug console | 186 |
| debug crashlog | 186 |
| debug disable | 187 |

| | |
|--------------------------------|-----|
| debug dpm | 187 |
| debug enable | 187 |
| debug info | 187 |
| debug reset | 188 |
| debug service | 188 |
| debug sysinfo | 188 |
| debug sysinfo-log | 188 |
| debug sysinfo-log-backup | 189 |
| debug sysinfo-log-list | 189 |
| debug timestamp | 189 |
| debug vminfo | 189 |
| dlp-archives | 190 |
| dvm | 190 |
| dvm adom | 190 |
| dvm capability | 191 |
| dvm chassis | 191 |
| dvm check-integrity | 191 |
| dvm debug | 191 |
| dvm device | 192 |
| dvm device-tree-update | 193 |
| dvm extender | 193 |
| dvm group | 194 |
| dvm lock | 194 |
| dvm proc | 194 |
| dvm supported-platforms | 194 |
| dvm task | 195 |
| dvm transaction-flag | 195 |
| dvm workflow | 195 |
| fgfm | 196 |
| fmnetwork | 196 |
| fmnetwork arp | 196 |
| fmnetwork interface | 196 |
| fmnetwork netstat | 197 |
| fmupdate | 197 |
| fortilogd | 200 |
| fwmanager | 201 |
| ha | 202 |
| hardware | 203 |
| log | 203 |
| log device | 203 |
| log device <DEVICE ID> | 203 |
| pm2 | 203 |

| | |
|---|------------|
| report | 204 |
| sniffer | 204 |
| sql | 208 |
| system | 210 |
| system admin-session | 210 |
| system disk | 210 |
| system export | 211 |
| system flash | 212 |
| system fsck | 212 |
| system geoip | 212 |
| system ntp | 213 |
| system print | 213 |
| system process | 214 |
| system raid | 214 |
| system route | 215 |
| system route6 | 215 |
| system server | 215 |
| test | 215 |
| test application | 216 |
| test connection | 218 |
| test deploymanager | 219 |
| test policy-check | 219 |
| test search | 219 |
| test sftp | 220 |
| upload | 220 |
| upload clear | 220 |
| upload force-retry | 220 |
| upload status | 220 |
| vpn | 221 |
| get | 222 |
| fmupdate analyzer | 223 |
| fmupdate av-ips | 223 |
| fmupdate custom-url-list | 223 |
| fmupdate device-version | 224 |
| fmupdate disk-quota | 224 |
| fmupdate fct-services | 224 |
| fmupdate fds-setting | 224 |
| fmupdate multilayer | 225 |
| fmupdate publicnetwork | 225 |
| fmupdate server-access-priorities | 225 |
| fmupdate server-override-status | 225 |
| fmupdate service | 226 |

| | |
|---|------------|
| fmupdate support-pre-fgt43 | 226 |
| fmupdate web-spam | 226 |
| system admin | 227 |
| system alert-console | 227 |
| system alertemail | 228 |
| system alert-event | 228 |
| system auto-delete | 228 |
| system backup | 229 |
| system certificate | 229 |
| system dm | 230 |
| system dns | 230 |
| system fips | 230 |
| system global | 231 |
| system ha | 231 |
| system interface | 232 |
| system locallog | 232 |
| system log | 233 |
| system log fetch | 233 |
| system loglimits | 234 |
| system mail | 234 |
| system metadata | 234 |
| system ntp | 235 |
| system password-policy | 235 |
| system performance | 235 |
| system report | 236 |
| system route | 236 |
| system route6 | 236 |
| system snmp | 236 |
| system sql | 237 |
| system status | 238 |
| system syslog | 239 |
| system workflow | 239 |
| show | 240 |
| Appendix A - CLI Error Codes | 241 |

Change Log

| Date | Change Description |
|------------|---|
| 2017-05-18 | Initial release. |
| 2017-09-18 | <code>config system global adom-select</code> and <code>policy-hit-count</code> descriptions updated. |
| | |
| | |

Introduction

FortiManager is designed for medium to large enterprises and managed security service providers. FortiManager system architecture emphasizes reliability, scalability, ease of use, and easy integration with third-party systems. FortiManager centralized management appliances deliver the essential tools needed to effectively manage your Fortinet-based security infrastructure.

About the FortiManager system

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

The FortiManager system manages communication between the managed devices and the FortiManager GUI.

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

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

FortiManager feature set

The FortiManager feature set includes the following modules:

- Device Manager
- Policy & Objects
- FortiGuard
- System Settings

FortiAnalyzer feature set

The FortiAnalyzer feature set can be enabled in FortiManager. The FortiAnalyzer feature set includes the following modules:

- FortiView
- Event Management
- Reports

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager Administration Guide*

This document describes how to set up the FortiManager system and use it to manage supported Fortinet units. It includes information on how to configure multiple Fortinet units, configuring and managing the

FortiGate VPN policies, monitoring the status of the managed devices, viewing and analyzing the FortiGate logs, updating the virus and attack signatures, providing web filtering and email filter service to the licensed FortiGate units as a local FDS, firmware revision control and updating the firmware images of the managed units.

- *FortiManager device QuickStart Guides*

These documents are included with your FortiManager system package. Use this document to install and begin working with the FortiManager system and FortiManager GUI.

- *FortiManager Online Help*

You can get online help from the FortiManager GUI. FortiManager online help contains detailed procedures for using the FortiManager GUI to configure and manage FortiGate units.

- *FortiManager CLI Reference*

This document describes how to use the FortiManager Command Line Interface (CLI) and contains references for all FortiManager CLI commands.

- *FortiManager Release Notes*

This document describes new features and enhancements in the FortiManager system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.

- *FortiManager VM Install Guide*

This document describes installing FortiManager VM in your virtual environment.

What's New in FortiManager 5.4

The following sections list commands that have been added, removed, or changed in the CLI.

FortiManager 5.4.3

The table below lists commands which have changed in version 5.4.3.

| Command | Change |
|--|--------------------------------------|
| <code>config system log settings</code> | Variable added: dns-resolve-dstip |
| <code>diagnose cdb check</code> | Variable added: preview |
| <code>execute add-on-license</code> | Command added |
| <code>execute fgfm reclaim-dev-tunnel</code> | Variable added: force |

FortiManager 5.4.2

The table below lists commands which have changed in version 5.4.2.

| Command | Change |
|---|--|
| <code>config fmupdate device-version</code> | Command removed. |
| <code>config fmupdate fds-setting</code> | Variables added: fds-ssl-protocol max-work system-support-faz system-support-fct system-support-fgt system-support-fml system-support-fsa system-support-fsw unreg-dev-option Variable removed: max-dlink-threads |
| <code>config fmupdate service</code> | Variable removed: use-cert |

| Command | Change |
|--|---|
| <code>config fmupdate support-pre-fgt43</code> | Command removed. |
| <code>config system admin profile</code> | Variables added: <code>config-revert</code> <code>intf-mapping</code> <code>import-policy-packages</code> <code>fgd-center-advanced</code> <code>fgd-center-fmw-mgmt</code> <code>fgd-center-licensing</code> |
| <code>config system auto-delete</code> <code>config dlp-files-auto-deletion</code> <code>config quarantine-files-auto-deletion</code> <code>config log-auto-deletion</code> <code>config report-auto-deletion</code> | Variables added: <code>retention</code> <code>runat</code> Variables removed: <code>when</code> |
| <code>config system dm</code> | Variable added: <code>skip-tunnel-fcp-req</code> |
| <code>config system global</code> | Variable added: <code>adom-rev-max-backup-revision</code> <code>fgfm-ssl-protocol</code> <code>max-log-forward</code> <code>oftp-ssl-protocol</code> <code>tunnel-mtu</code> Variable removed: <code>lcdpin</code> |
| <code>config system interface</code> | Variable added: <code>mtu</code> |
| <code>config system log settings</code> | Variable added: <code>FAC-custom-field1</code> <code>import-max-logfiles</code> |
| <code>config system report est-browse-time</code> | Variables removed: <code>compensate-read-time</code> <code>max-num-user</code> <code>min-read-time</code> <code>min-traffic-bytes</code> |
| <code>config system report setting</code> | Variable added: <code>ldap-cache-timeout</code> |
| <code>diagnose cdb check adom-revision</code> | Command added. |
| <code>diagnose debug application fdssvr</code> | Command added. |
| <code>diagnose dvm device monitor</code> | Command added. |

| Command | Change |
|---|---|
| <code>diagnose fwmanager</code> | Command added: delete-official-images Command removed: delete-offical-images |
| <code>diagnose report clean</code> | Command updated. |
| <code>diagnose sql config max-num-hcache</code> | Command removed. |
| <code>diagnose system export raidlog</code> | Command added. |
| <code>diagnose system raid alarms</code> | Command removed. |
| <code>execute fmpofile delete-profile</code> | Command added. |
| <code>execute max-dev-license</code> | Command added. |
| <code>execute reset adom-settings</code> | Command added. |
| <code>execute sdns</code> | Command added. |
| <code>execute sensor</code> | Command added. |
| <code>execute sql-report list-schedule</code> | Command updated. |

FortiManager 5.4.1

The table below lists commands which have changed in version 5.4.1.

| Command | Change |
|---|---|
| <code>config system admin settings</code> | Command added: gui-theme |
| <code>config system dm</code> | Commands added: concurrent-install-image-limit install-image-tunnel-timeout |
| <code>config system global</code> | Command added: detect-unregistered-log-device |
| <code>config system log</code> | Command added: breach-detect |

| Command | Change |
|---|---|
| <code>config system log-fetch</code> | Commands removed: client-adom server-adom sync-adom-config |
| <code>config system report est-browse-time</code> | Commands added: min-read-time min-traffic-bytes |
| <code>diagnose cdb-check</code> | Command added: policy-packages |
| <code>diagnose fmupdate</code> | Commands removed: fds-updatenow fgd-updatenow fct-updatenow add-device Command added: updatenow |
| <code>diagnose sql config</code> | Commands added: auto-cache-delay debug-filter hcache-agg-step set hcache-max-fv-row hcache-max-rpt-row max-num-hcache set report-engine top-dev set Commands removed: gui-rpt-shm sql-hcache-hk rebuild-report-hcache |
| <code>diagnose sql hcache</code> | Commands added: agg-status rebuild-both rebuild-report rebuild-status |
| <code>execute migrate all-settings</code> | Variables added: ftp scp sftp |
| <code>execute tree fmpolicy</code> | Variables added: clone-adom-object |

FortiManager 5.4.0

The table below lists commands which have changed in version 5.4.0.

| Command | Change |
|---|---|
| <code>config system admin profile</code> | Command removed: <code>workflow-approve</code> Commands added: <code>device-ap</code> <code>set device-forticlient</code> <code>set device-wan-link-load-balance</code> |
| <code>config system admin setting</code> | Command added: <code>shell-access</code> <code>shell-password</code> Commands removed: <code>show-adom-central-nat-policies</code> <code>show-adom-dos-policies</code> <code>show-adom-dynamic-objects</code> <code>show-adom-icap-policies</code> <code>show-adom-implicit-id-based-policy</code> <code>show-adom-implicit-policy</code> <code>show-adom-ipv6-settings</code> <code>show-adom-policy-consistency-button</code> <code>show-adom-rtmlog</code> <code>show-adom-sniffer-policies</code> <code>show-adom-taskmon-button</code> <code>show-adom-terminal-button</code> <code>show-adom-voip-policies</code> <code>show-adom-vpnman</code> <code>show-foc-settings</code> <code>show-fortimail-settingss</code> <code>show-fsw-settings</code> <code>show-global-object-settings</code> <code>show-global-policy-settings</code> |
| <code>config system admin user</code> | Command added: <code>adom-exclude</code> |
| <code>config system fortiview auto-cache</code> | Commands added: <code>aggressive-fortiview</code> <code>interval</code> <code>status</code> |
| <code>config system global</code> | Commands added: <code>adom-select</code> <code>partial-install-rev</code> <code>policy-hit-count</code> Command removed: <code>admin-maintainer</code> |

| Command | Change |
|--|--|
| <code>config system log settings</code> | Command added: FDD-custom-field1 |
| <code>config system log-fetch</code> | Command added. |
| <code>config system report auto-cache</code> | Commands removed: aggressive-drilldown drilldown-interval drilldown-status |
| <code>config system sql</code> | Commands removed: reset resend-device sql-database-quota-ratio |
| <code>diagnose debug application</code> | Commands added: fortimeter log-fetchd logfwd |
| <code>diagnose debug backup-oldformat-script-logs</code> | Command added. |
| <code>diagnose dvm supported-platforms</code> | Command added: mr-list |
| <code>diagnose fmupdate</code> | Command added: fct-updatenow fds-updateinfo fds-updatenow fgd-updatenow Command removed: updatenow |
| <code>diagnose fwmanager</code> | Command added: serverlist service-restart |
| <code>diagnose log device</code> | Variable added: DEVICE ID |
| <code>diagnose sql remove hcache</code> | Variable removed device-id Variable added: adom |
| <code>diagnose sql show log-stfile</code> | Variable added: vdom |
| <code>diagnose sql show policy-info</code> | Command added. |

| Command | Change |
|---|---|
| <code>diagnose sql status</code> | Command added: hcache |
| <code>diagnose test application</code> | Command removed: fazautormd Commands added: log-fetchd logfwd |
| <code>execute backup-logs</code> <code>execute backup-logs-only</code> <code>execute backup-logs-rescue</code> <code>execute backup-reports</code> <code>execute backup-reports-config</code> | Variable added: vdlist |
| <code>execute fmpolicy print-prov-database</code> | Command added. |
| <code>execute iotop</code> | Command added. |
| <code>execute iotps</code> | Command added. |
| <code>execute log device vdom</code> | Variable added: Index Variable removed: Id |
| <code>execute log-fetch</code> | Command added. |
| <code>execute remove</code> | Command removed: gui-logview-settings |
| <code>execute restore-logs</code> <code>execute restore-logs-only</code> <code>execute restore-reports</code> <code>execute restore-reports-config</code> | Command added: vdlist |
| <code>execute sql-local</code> | Command removed: remove-logtype |
| <code>execute sql-report</code> | Command added: hcache-build |
| <code>get system log-fetch</code> | Command added. |
| <code>get system loglimits</code> | Command added. |

Using the Command Line Interface

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

This chapter describes:

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

CLI command syntax

This guide uses the following conventions to describe command syntax.

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

For example:

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

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

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

For example:

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

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

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

For example:

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

You can enter any of the following:

```
set allowaccess ping
set allowaccess https ping
set allowaccess http https ping snmp ssh telnet webservice
```

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

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

Connecting to the CLI

You can use a direct console connection or SSH to connect to the FortiManager CLI.

Connecting to the FortiManager console

To connect to the FortiManager console, you need:

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



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

To connect to the CLI:

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

| | |
|-----------------|---------------|
| COM port | COM1 |
| Bits per second | 115200 |
| Data bits | 8 |
| Parity | None |
| Stop bits | 1 |
| Flow control | None |

7. Press `Enter` to connect to the FortiManager CLI.
The login prompt appears.
8. Enter a valid administrator name and press `Enter`.
9. Enter the password for this administrator and press `Enter`.
You have connected to the FortiManager CLI, and you can enter CLI commands.

Setting administrative access on an interface

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

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

To use the CLI to configure SSH access:

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

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

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

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

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



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

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

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

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

Connecting to the FortiManager CLI using SSH

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



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. Enter a valid administrator name and press `Enter`.
4. Enter the password for this administrator and press `Enter`.
The FortiManager model name followed by a # is displayed.

You have connected to the FortiManager CLI, and you can enter CLI commands.

Connecting to the FortiManager CLI using the GUI

The GUI also provides a CLI console window.

To connect to the CLI using the GUI:

1. Connect to the GUI and log in.
For information about how to do this, see the [FortiManager Administration Guide](#).
2. Go to *System Settings > Dashboard*
3. Click inside the CLI Console widget. If the widget is not available, select *Add Widget* to add the widget to the dashboard.

CLI objects

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

| | |
|-----------------|--|
| fmupdate | Configures settings related to FortiGuard service updates and the FortiManager unit's built-in FDS. See fmupdate on page 120 . |
| system | Configures options related to the overall operation of the FortiManager unit, such as interfaces, virtual domains, and administrators. See system on page 40 . |

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

CLI command branches

The FortiManager CLI consists of the following command branches:

| | |
|-------------------------------|---------------------------------|
| config branch | execute branch |
| get branch | diagnose branch |
| show branch | |

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

config branch

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

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

```
config system admin user
```

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

```
(user) #
```

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

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

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

```
edit admin_1
```

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

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

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

| | |
|---------------|---|
| abort | Exit an edit shell without saving the configuration. |
| config | In a few cases, there are subcommands that you access using a second config command while editing a table entry. An example of this is the command to add host definitions to an SNMP community. |
| end | Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell. |
| get | List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the keywords and their values. |
| next | Save the changes you have made in the current shell and continue working in the shell. For example if you want to add several new admin user accounts enter the <code>config system admin user shell</code> . Enter <code>edit User1</code> and press <code>Enter</code> . Use the <code>set</code> commands to configure the values for the new admin account. Enter <code>next</code> to save the configuration for User1 without leaving the <code>config system 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> then press <code>Enter</code> to save the last configuration and leave the shell. |
| set | Assign values. For example from the <code>edit admin</code> command shell, typing <code>set passwd newpass</code> changes the password of the admin administrator account to <code>newpass</code> . Note: When using a <code>set</code> command to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove. |
| show | Show changes to the default configuration in the form of configuration commands. |
| unset | Reset values to defaults. For example from the <code>edit admin</code> command shell, typing <code>unset passwd</code> resets the password of the admin administrator account to the default of no password. |

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

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

get branch

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

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

Example

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

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

```
get
```

The screen displays:

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

Example

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

```
edit admin
```

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

```
get
```

The screen displays:

```
userid : admin
password : *
trusthost1 : 0.0.0.0 0.0.0.0
trusthost2 : 0.0.0.0 0.0.0.0
trusthost3 : 0.0.0.0 0.0.0.0
trusthost4 : 0.0.0.0 0.0.0.0
trusthost5 : 0.0.0.0 0.0.0.0
trusthost6 : 0.0.0.0 0.0.0.0
trusthost7 : 0.0.0.0 0.0.0.0
trusthost8 : 0.0.0.0 0.0.0.0
trusthost9 : 0.0.0.0 0.0.0.0
trusthost10 : 127.0.0.1 255.255.255.255
ipv6_trusthost1 : ::/0
ipv6_trusthost2 : ::/0
ipv6_trusthost3 : ::/0
ipv6_trusthost4 : ::/0
ipv6_trusthost5 : ::/0
ipv6_trusthost6 : ::/0
ipv6_trusthost7 : ::/0
ipv6_trusthost8 : ::/0
ipv6_trusthost9 : ::/0
ipv6_trusthost10 : ::1/128
profileid : Super_User
adom:
```

```
    == [ all_adoms ]
    adom-name: all_adoms
policy-package:
    == [ all_policy_packages ]
    policy-package-name: all_policy_packages
restrict-access : disable
restrict-dev-vdom:
description : (null)
user_type : local
ssh-public-key1 :
ssh-public-key2 :
ssh-public-key3 :
meta-data:
last-name : (null)
first-name : (null)
email-address : (null)
phone-number : (null)
mobile-number : (null)
pager-number : (null)
hidden : 0
dashboard-tabs:
dashboard:
    == [ 6 ]
    moduleid: 6
    == [ 1 ]
    moduleid: 1
    == [ 2 ]
    moduleid: 2
    == [ 3 ]
    moduleid: 3
    == [ 4 ]
    moduleid: 4
    == [ 5 ]
    moduleid: 5
```

Example

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

At the # prompt, type:

```
get system interface port1
```

The screen displays:

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

show branch

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

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

Example

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

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

```
show
```

The screen displays:

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

Example

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

```
show system dns
```

The screen displays:

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

execute branch

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

Example

At the root prompt, type:

```
execute reboot
```

and press `Enter` to restart the FortiManager unit.

diagnose branch

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

documented in this CLI Reference.



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

Example command sequences



The command prompt changes for each shell.

To configure the primary and secondary DNS server addresses:

1. Starting at the root prompt, type:

```
config system dns
```

and press **Enter**. The prompt changes to `(dns) #`.

2. At the `(dns) #` prompt, type `?`

The following options are displayed.

```
set
unset
get
show
abort
end
```

3. Enter `set ?`

The following options are displayed:

```
primary
secondary
```

4. To set the primary DNS server address to `172.16.100.100`, type:

```
set primary 172.16.100.100
```

and press **Enter**.

5. To set the secondary DNS server address to `207.104.200.1`, type:

```
set secondary 207.104.200.1
```

and press **Enter**.

6. To restore the primary DNS server address to the default address, type `unset primary` and press **Enter**.

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

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

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

CLI basics

This section covers command line interface basic information.

Command help

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

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

Command tree

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

Command completion

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

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

Recalling commands

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

Editing commands

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

| Function | Key combination |
|-------------------|-----------------|
| Beginning of line | Control key + A |
| End of line | Control key + E |

| Function | Key combination |
|--|-----------------|
| Back one character | Control key + B |
| Forward one character | Control key + F |
| Delete current character | Control key + D |
| Previous command | Control key + P |
| Next command | Control key + N |
| Abort the command | Control key + C |
| If used at the root prompt, exit the CLI | Control key + C |

Line continuation

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

Command abbreviation

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

Environment variables

The FortiManager CLI supports several environment variables.

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

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

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

Encrypted password support

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

```
show system admin user user1
config system admin user
```

```
edit "user1"
  set password ENC
    UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMfc9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXc
    XdnQxskRcU3E9XqOit82PgScwzGzGuJ5a9f
  set profileid "Standard_User"
next
end
```

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

```
config system admin
then press Enter.
```

Enter:

```
edit user1
then press Enter.
```

Enter:

```
set password ENC
  UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMfc9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxs
  kRcU3E9XqOit82PgScwzGzGuJ5a9f
then press Enter.
```

Enter:

```
end
then press Enter.
```

Entering spaces in strings

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

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

Entering quotation marks in strings

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

Entering a question mark (?) in a string

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

International characters

The CLI supports international characters in strings.

Special characters

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

IPv4 address formats

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

```
set ip 192.168.1.1 255.255.255.0
```

or

```
set ip 192.168.1.1/24
```

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

Changing the baud rate

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



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

Debug log levels

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

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

Administrative Domains

This chapter provides information about the ADOM functionality in FortiManager .

ADOMs overview

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

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

Administrative domains are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator. For more information, see [Configuring ADOMs on page 37](#).

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

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

| FortiManager Model | Administrative Domain / Network Devices |
|--------------------|---|
| FMG-VM-100-UG | +100 / +100 |
| FMG-VM-1000-UG | +1000 / +1000 |
| FMG-VM-5000-UG | +5000 / +5000 |
| FMG-VM-U-UG | +10000 / +10000 |

Configuring ADOMs

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



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



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



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

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

To Enable/disable ADOMs:

Enter the following CLI command:

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

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



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

To change ADOM device modes:

Enter the following CLI command:

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

To assign an administrator to an ADOM:

Enter the following CLI command:

```
config system admin user
    edit <name>
        set adom <adom_name>
    next
end
```

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

Concurrent ADOM Access

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

Concurrent ADOM access can be enabled or disabled using the CLI.



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

To enable ADOM locking and disable concurrent ADOM access:

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

To disable ADOM locking and enable concurrent ADOM access:

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

To enable workspace workflow mode:

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



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

system

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



FortiManager CLI commands and variables are case sensitive.

| | | | |
|---------------------|-------------------|-----------------|--------------------------|
| admin | dm | locallog | report |
| alert-console | dns | log | route |
| alertemail | fips | log-fetch | route6 |
| alert-event | fortiview setting | mail | snmp |
| auto-delete | global | metadata | sql |
| backup all-settings | ha | ntp | syslog |
| certificate | interface | password-policy | workflow approval-matrix |

admin

Use the following commands to configure admin related settings.

admin group

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

Syntax

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

| Variable | Description |
|----------|---|
| <name> | Enter the name of the group you are editing or enter a new name to create an entry. Character limit: 63 |
| <member> | Add group members. |

admin ldap

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

Syntax

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

| Variable | Description |
|-------------------------------------|---|
| <name> | Enter the name of the LDAP server or enter a new name to create an entry. Character limit: 63 |
| server <string> | Enter the LDAP server domain name or IPv4 address. Enter a new name to create a new entry. |
| secondary-server <string> | Enter the secondary LDAP server domain name or IPv4 address. Enter a new name to create a new entry. |
| tertiary-server <string> | Enter the tertiary LDAP server domain name or IPv4 address. Enter a new name to create a new entry. |
| cnid <string> | Enter the common name identifier. Default: <code>cn</code> . Character limit: 20 |
| dn <string> | Enter the distinguished name. |
| port <integer> | Enter the port number for LDAP server communication. Default: 389. Range: 1 to 65535 |
| type {anonymous regular simple} | Set a binding type. The following options are available: <ul style="list-style-type: none"> <code>anonymous</code>: Bind using anonymous user search <code>regular</code>: Bind using username/password and then search <code>simple</code>: Simple password authentication without search (default) |
| username <string> | Enter a username. This variable appears only when <code>type</code> is set to <code>regular</code> . |

| Variable | Description |
|-------------------------------------|---|
| password <passwd> | Enter a password for the username above. This variable appears only when type is set to regular. |
| group <string> | Enter an authorization group. The authentication user must be a member of this group (full DN) on the server. |
| filter <string> | Enter content for group searching. For example: <ul style="list-style-type: none"> • (&(objectcategory=group) (member=*)) • (&(objectclass=groupofnames) (member=*)) • (&(objectclass=groupofuniquenames) (uniquemember=*)) • (&(objectclass=posixgroup) (memberuid=*)) |
| attributes <filter> | Attributes used for group searching (for multi-attributes, a use comma as a separator). For example: <ul style="list-style-type: none"> • member • uniquemember • member,uniquemember |
| secure {disable ldaps starttls} | Set the SSL connection type. The following options are available: <ul style="list-style-type: none"> • disable: no SSL • ldaps: use LDAPS • starttls: use STARTTLS |
| ca-cert <string> | CA certificate name. This variable appears only when secure is set to ldaps or starttls. |
| connect-timeout <integer> | Set the LDAP connection timeout (msec). |
| adom <adom-name> | Set the ADOM name to link to the LDAP configuration. |

Example

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

```
config system admin ldap
edit user1
set server 206.205.204.203
set dn techdoc
set type regular
set username auth1
set password auth1_pwd
set group techdoc
end
```

admin profile

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

Syntax

```

config system admin profile
edit <profile>
    set adom-policy-packages {none | read | read-write}
    set adom-switch {none | read | read-write}
    set app-filter {enable | disable}
    set assignment {none | read | read-write}
    set change-password {enable | disable}
    set config-retrieve {none | read | read-write}
    set config-revert {none | read | read-write}
    set consistency-check {none | read | read-write}
    set deploy-management {none | read | read-write}
    set description <string>
    set device-ap {none | read | read-write}
    set device-config {none | read | read-write}
    set device-forticlient {none | read | read-write}
    set device-manager {none | read | read-write}
    set device-op {none | read | read-write}
    set device-profile {none | read | read-write}
    set device-wan-link-load-balance {none | read | read-write}
    set event-management {none | read | read-write}
    set fgd_center {none | read | read-write}
    set fgd-center-advanced {none | read | read-write}
    set fgd-center-fmw-mgmt {none | read | read-write}
    set fgd-center-licensing {none | read | read-write}
    set global-policy-packages {none | read | read-write}
    set import-policy-packages {none | read | read-write}
    set intf-mapping {none | read | read-write}
    set ips-filter {enable | disable}
    set log-viewer {none | read | read-write}
    set policy-objects {none | read | read-write}
    set read-passwd {none | read | read-write}
    set realtime-monitor {none | read | read-write}
    set report-viewer {none | read | read-write}
    set scope (Not Applicable)
    set system-setting {none | read | read-write}
    set term-access {none | read | read-write}
    set type {restricted | system}
    set vpn-manager {none | read | read-write}
    set web-filter {enable | disable}
end

```

| Variable | Description |
|-----------|---|
| <profile> | Edit the access profile. Enter a new name to create a new profile. The pre-defined access profiles are <i>Super_User</i> , <i>Standard_User</i> , <i>Restricted_User</i> , and <i>Package_User</i> . Character limit: 35 |

| Variable | Description |
|---|---|
| adom-policy-packages {none read read-write} | <p>Enter the level of access to ADOM policy packages for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. The following options are available:</p> <ul style="list-style-type: none"> <code>none</code>: No permission. <code>read</code>: Read permission. <code>read-write</code>: Read-write permission. <p>This command corresponds to the Policy Packages & Objects option on the administrator profile settings page in the GUI. It is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: All the operations in ADOMs</p> <p>Dependencies: Install and re-install depends on Install to Devices in DVM settings, <code>type</code> must be <code>system</code>.</p> |
| adom-switch {none read read-write} | <p>Configure administrative domain (ADOM) permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Administrative Domain option in the GUI.</p> <p>Controlled functions: ADOM settings in DVM, ADOM settings in All ADOMs page (under System Settings tab)</p> <p>Dependencies: If <code>system-setting</code> is <code>none</code>, the All ADOMs page is not accessible, <code>type</code> must be <code>system</code>.</p> |
| app-filter {enable disable} | <p>Enable/disable IPS Sensor permission for the restricted admin profile.</p> <p>Dependencies: <code>type</code> must be <code>restricted</code>.</p> |
| assignment {none read read-write} | <p>Configure assignment permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Assignment option in the GUI. It is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: Global assignment in Global ADOM.</p> <p>Dependencies: <code>type</code> must be <code>system</code>.</p> |
| change-password {enable disable} | <p>Enable/disable allowing restricted users to change their password</p> |
| config-retrieve {none read read-write} | <p>Set the configuration retrieve settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Retrieve Configuration from Devices option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Retrieve configuration from devices</p> <p>Dependencies: <code>type</code> must be <code>system</code>.</p> |
| config-revert {none read read-write} | <p>Set the configuration revert settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Revert Configuration from Revision History option in the GUI. It is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Revert configuration from revision history.</p> <p>Dependencies: <code>type</code> must be <code>system</code>.</p> |

| Variable | Description |
|--|---|
| consistency-check {none read read-write} | Configure Policy Check permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Policy Check option in the GUI. It is a sub-setting of <code>policy-objects</code> . Controlled functions: Policy check. Dependencies: <code>type</code> must be <code>system</code> . |
| deploy-management {none read read-write} | Enter the level of access to the deployment management configuration settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Install to Devices option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Install to devices. Dependencies: <code>type</code> must be <code>system</code> . |
| description <string> | Enter a description for this access profile. Enclose the description in quotes if it contains spaces. Character limit: 1023 |
| device-ap | Enter the level of access to device AP settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the AP Manager option in the GUI. Controlled functions: AP Manager pane. Dependencies: <code>type</code> must be <code>system</code> . |
| device-config {none read read-write} | Enter the level of access to device configuration settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Manage Device Configuration option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Edit devices, All settings under Menu in Dashboard. Dependencies: <code>type</code> must be <code>system</code> . |
| device-forticlient | Enter the level of access to FortiClient settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the FortiClient Manager option in the GUI. Controlled functions: FortiClient Manager pane. Dependencies: <code>type</code> must be <code>system</code> . |
| device-manager {none read read-write} | Enter the level of access to Device Manager settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Device Manager option in the GUI. Controlled functions: Device Manager pane. Dependencies: <code>type</code> must be <code>system</code> . |
| device-op {none read read-write} | Add the capability to add, delete, and edit devices to this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Add/Delete Devices/Groups option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Add or delete devices or groups. Dependencies: <code>type</code> must be <code>system</code> . |

| Variable | Description |
|---|--|
| device-profile {none read read-write} | Configure device profile permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Provisioning Templates option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Provisioning Templates. Dependencies: <code>type</code> must be <code>system</code> . |
| device-wan-link-load-balance | Enter the level of access to <code>wan-link-load-balance</code> settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to WAN Link Load Balance option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Wan LLB. Dependencies: <code>type</code> must be <code>system</code> . |
| event-management {none read read-write} | Set the Event Management permission. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Event Management option in the GUI. Controlled functions: Event Management pane and all its operations. Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code> , <code>type</code> must be <code>system</code> . |
| fgd_center {none read read-write} | Set the FortiGuard Center permission. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the FortiGuard Center option in the GUI. Controlled functions: FortiGuard pane, All the settings under FortiGuard. Dependencies: <code>type</code> must be <code>system</code> . |
| fgd-center-advanced {none read read-write} | Set the FortiGuard Center permission. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Advanced option in the GUI. It is a sub-setting of <code>fgd-center</code> . Controlled functions: FortiGuard pane Advanced Settings options. Dependencies: <code>type</code> must be <code>system</code> . |
| fgd-center-fmw-mgmt {none read read-write} | Set the FortiGuard Center permission. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Firmware Management option in the GUI. It is a sub-setting of <code>fgd-center</code> . Controlled functions: FortiGuard pane Firmware Images options. Dependencies: <code>type</code> must be <code>system</code> . |
| fgd-center-licensing {none read read-write} | Set the FortiGuard Center permission. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the License Management option in the GUI. It is a sub-setting of <code>fgd-center</code> . Controlled functions: FortiGuard pane Licensing Status options. Dependencies: <code>type</code> must be <code>system</code> . |

| Variable | Description |
|---|--|
| global-policy-packages {none read read-write} | Configure global policy package permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Global Policy Packages & Objects option in the GUI. It is a sub-setting of <code>policy-objects</code> . Controlled functions: All operations in Global ADOM. Dependencies: <code>type</code> must be <code>system</code> . |
| import-policy-packages {none read read-write} | Configure importing policy package permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Import Policy Package option in the GUI. Controlled functions: Importing policy packages. Dependencies: <code>type</code> must be <code>system</code> . |
| intf-mapping {none read read-write} | Configure interface mapping permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Interface Mapping option in the GUI. Controlled functions: Mapping interfaces. Dependencies: <code>type</code> must be <code>system</code> . |
| ips-filter {enable disable} | Enable/disable Application Sensor permission for the restricted admin profile. Dependencies: <code>type</code> must be <code>restricted</code> . |
| log-viewer {none read read-write} | Set the Log View permission. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Log View option in the GUI. Controlled functions: Log View and all its operations. Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code> , <code>type</code> must be <code>system</code> . |
| policy-objects {none read read-write} | Set the Policy & Objects permission. Select <code>none</code> to hide this option from the administrator in the GUI. Controlled functions: Policy & Objects pane. Dependencies: <code>type</code> must be <code>system</code> . |
| read-passwd {none read read-write} | Add the capability to view the authentication password in clear text to this profile. Dependencies: <code>type</code> must be <code>system</code> . |
| realtime-monitor {none read read-write} | Enter the level of access to the Drill Down configuration settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code> , <code>type</code> must be <code>system</code> . |
| report-viewer {none read read-write} | Set the Reports permission. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Reports option in the GUI. Controlled functions: Reports pane and all its operations. Dependencies: <code>faz-status</code> must be set to <code>enable</code> in <code>system global</code> , <code>type</code> must be <code>system</code> . |

| Variable | Description |
|---|--|
| scope (Not Applicable) | CLI command is not in use. |
| system-setting {none read read-write} | Configure System Settings permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the System Settings option in the GUI. Controlled functions: System Settings pane, all the settings under system setting. Dependencies: <code>type</code> must be <code>System Admin</code> . |
| term-access {none read read-write} | Set the terminal access permissions for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Terminal Access option in the GUI. It is a sub-setting of <code>device-manager</code> . Controlled functions: Connect to the CLI via Telnet or SSH. Dependencies: Depends on <code>device-config</code> option, <code>type</code> must be <code>System Admin</code> . |
| type {restricted system} | Enter the admin profile type: <ul style="list-style-type: none"> <code>restricted</code>: Restricted admin profile <code>system</code>: System admin profile |
| vpn-manager {none read read-write} | Enter the level of access to VPN console configuration settings for this profile. Select <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the VPN Manager option in the GUI. It is a sub-setting of <code>policy-objects</code> . Controlled functions: VPN Console. Dependencies: <code>type</code> must be <code>System Admin</code> . |
| web-filter {enable disable} | Enable/disable Web Filter Profile permission for the restricted admin profile. Dependencies: <code>type</code> must be <code>Restricted Admin</code> . |

admin radius

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

Syntax

```

config system admin radius
  edit <server>
    set auth-type {any | chap | mschap2 | pap}
    set nas-ip <ipv4_address>
    set port <integer>
    set secondary-secret <passwd>
    set secondary-server <string>
    set secret <passwd>
    set server <string>
  end

```

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

Example

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

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

admin setting

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

Syntax

```
config system admin setting
  set access-banner {enable | disable}
  set admin-https-redirect {enable | disable}
  set admin-login-max <integer>
  set admin_server_cert <admin_server_cert>
  set allow_register {enable | disable}
  set auto-update {enable | disable}
  set banner-message <string>
  set chassis-mgmt {enable | disable}
  set chassis-update-interval <integer>
```

```

set device_sync_status {enable | disable}
set gui-theme
set http_port <integer>
set https_port <integer>
set idle_timeout <integer>
set install-ifpolicy-only {enable | disable}
set mgmt-addr <string>
set mgmt-fqdn <string>
set offline_mode {enable | disable}
set register_passwd <passwd>
set shell-access {enable | disable}
set shell-password <passwd>
set show-add-multiple {enable | disable}
set show-adom-devman {enable | disable}
set show-device-import-export {enable | disable}
set show_automatic_script {enable | disable}
set show-checkbox-in-table {enable | disable}
set show_grouping_script {enable | disable}
set show_schedule_script {enable | disable}
set show_tcl_script {enable | disable}
set unreg_dev_opt {add_allow_service | add_no_service | ignore}
set webadmin_language {auto_detect | english | japanese | korean | simplified_
chinese | traditional_chinese}
end

```

| Variable | Description |
|---|---|
| access-banner {enable disable} | Enable/disable the access banner. Default: disable |
| admin-https-redirect {enable disable} | Enable/disable redirection of HTTP admin traffic to HTTPS. |
| admin-login-max <integer> | Set the maximum number of admin users that be logged in at one time. Range: 1 to 256 (users) |
| admin_server_cert <admin_server_cert> | Enter the name of an https server certificate to use for secure connections. Default: server.crt |
| allow_register {enable disable} | Enable/disable the ability an unregistered device to be registered. Default: disable |
| auto-update {enable disable} | Enable/disable device config automatic update. |
| banner-message <string> | Set the banner messages. Default: none Character limit: 255 |
| chassis-mgmt {enable disable} | Enable/disable chassis management. Default: disable |
| chassis-update-interval <integer> | Set the chassis background update interval. Range: 4 to 1440 minutes. Default: 15 |

| Variable | Description |
|--|--|
| device_sync_status {enable disable} | Enable/disable device synchronization status indication. Default: enable |
| gui-theme | Configure the GUI theme. |
| http_port <integer> | Enter the HTTP port number for web administration. Default: 80. Range: 1 to 65535 |
| https_port <integer> | Enter the HTTPS port number for web administration. Default: 443. Range: 1 to 65535 |
| idle_timeout <integer> | Enter the idle timeout value. Range: 1 to 480 (minutes). Default: 5 |
| install-ifpolicy-only {enable disable} | Enable to allow only the interface policy to be installed. The following options are available: <ul style="list-style-type: none"> disable: Disable setting. enable: Enable setting. Default: disable |
| mgmt-addr <string> | FQDN/IPv4 of FortiManager used by FGFM. |
| mgmt-fqdn <string> | FQDN of FortiManager used by FGFM. |
| offline_mode {enable disable} | Enable offline mode to shut down the protocol used to communicate with managed devices. The following options are available: <ul style="list-style-type: none"> disable: Disable offline mode. enable: Enable offline mode. Default: disable |
| register_passwd <passwd> | Enter the password to use when registering a device. Character limit: 19 |
| shell-access {enable disable} | Enable shell access. The following options are available: <ul style="list-style-type: none"> disable: Disable shell-access enable: Enable shell-access. |
| shell-password <passwd> | Enter the password to use for shell access. |
| show-add-multiple {enable disable} | Show the add multiple button. The following options are available: <ul style="list-style-type: none"> disable: Disable setting. enable: Enable setting. |
| show-adom-devman {enable disable} | Show device manager tools on the GUI. The following options are available: <ul style="list-style-type: none"> disable: Hide device manager tools on GUI. enable: Show device manager tools on GUI. Default: disable |

| Variable | Description |
|--|---|
| show-checkbox-in-table {enable disable} | Show checkboxes in tables in the GUI. |
| show-device-import-export {enable disable} | Enable import/export of ADOM, device, and group lists. The following options are available: <ul style="list-style-type: none"> disable: Disable setting. enable: Enable setting. |
| show_automatic_script {enable disable} | Enable/disable automatic script. The following options are available: <ul style="list-style-type: none"> disable: Disable script option. enable: Enable script option. |
| show_grouping_script {enable disable} | Enable/disable grouping script. The following options are available: <ul style="list-style-type: none"> disable: Disable script option. enable: Enable script option. |
| show_schedule_script {enable disable} | Enable/disable schedule script. The following options are available: <ul style="list-style-type: none"> disable: Disable script option. enable: Enable script option. |
| show_tcl_script {enable disable} | Enable/disable TCL script. The following options are available: <ul style="list-style-type: none"> disable: Disable script option. enable: Enable script option. |
| unreg_dev_opt {add_allow_service add_no_service ignore} | Select action to take when an unregistered device connects to FortiManager. The following options are available: <ul style="list-style-type: none"> add_allow_service: Add unregistered devices and allow service requests (default value). add_no_service: Add unregistered devices and deny service requests. ignore: Ignore unregistered devices. |
| webadmin_language {auto_detect english japanese korean simplified_chinese traditional_chinese} | Select the language to be used for web administration. The following options are available: <ul style="list-style-type: none"> auto_detect: Automatically detect language. english: English. japanese: Japanese. korean: Korean. simplified_chinese: Simplified Chinese. traditional_chinese: Traditional Chinese. Default: auto_detect |

admin tacacs

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

Syntax

```

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

```

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

Example

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

```

config system admin tacacs
  edit TAC1

```

```

set server 206.205.204.203
set key R1a2D3i4U5s
end

```

admin user

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

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



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

Syntax

```

config system admin user
edit <name_str>
    set password <passwd>
    set change-password {enable | disable}
    set trusthost1 <ipv4_mask>
    set trusthost2 <ipv4_mask>
    set trusthost3 <ipv4_mask>
    ...
    set trusthost10 <ipv4_mask>
    set ipv6_trusthost1 <ipv6_mask>
    set ipv6_trusthost2 <ipv6_mask>
    set ipv6_trusthost3 <ipv6_mask>
    ...
    set ipv6_trusthost10 <ipv6_mask>
    set profileid <profile-name>
    set adom <adom_name(s)>
    set adom-exclude <adom_name(s)>
    set web-filter <Web Filter profile name>
    set ips-filter <IPS Sensor name>
    set app-filter <Application Sensor name>
    set policy-package {<adom name>: <policy package id> <adom policy folder name>/
        <package name> | all_policy_packages}
    set restrict-access {enable | disable}
    set rpc-permit {none | read-only | read-write}
    set description <string>
    set user_type {group | ldap | local | pki-auth | radius | tacacs-plus}
    set group <string>
    set ldap-server <string>
    set radius_server <string>
    set tacacs-plus-server <string>
    set ssh-public-key1 <key-type> <key-value>
    set ssh-public-key2 <key-type>, <key-value>
    set ssh-public-key3 <key-type> <key-value>
    set wildcard {enable | disable}

```

```
    set radius-accprofile-override <enable | disable>
    set radius-adom-override <enable | disable>
    set radius-group-match <string>
    set password-expire <yyyy-mm-dd>
    set force-password-change {enable | disable}
    set subject <string>
    set ca <string>
    set two-factor-auth {enable | disable}
    set last-name <string>
    set first-name <string>
    set email-address <string>
    set phone-number <string>
    set mobile-number <string>
    set pager-number <string>
end
config meta-data
    edit <fieldname>
        set fieldlength
        set fieldvalue <string>
        set importance
        set status
    end
end
config dashboard-tabs
    edit tabid <integer>
        set name <string>
    end
end
config dashboard
    edit moduleid
        set name <string>
        set column <column_pos>
        set refresh-interval <integer>
        set status {close | open}
        set tabid <integer>
        set widget-type <string>
        set log-rate-type {device | log}
        set log-rate-topn {1 | 2 | 3 | 4 | 5}
        set log-rate-period {1hour | 2min | 6hours}
        set res-view-type {history | real-time}
        set res-period {10min | day | hour}
        set res-cpu-display {average | each}
        set num-entries <integer>
        set time-period {1hour | 24hour | 8hour}
        set diskio-content-type
        set diskio-period {1hour | 24hour | 8hour}
    end
end
config restrict-dev-vdom
    edit dev-vdom <string>
end
end
```

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

| Variable | Description |
|--|--|
| policy-package {<adom name>: <policy package id> <adom policy folder name>/ <package name> all_policy_packages} | Policy package access |
| restrict-access {enable disable} | Enable/disable restricted access to the development VDOM (dev-vdom) . Default: <code>disable</code> |
| rpc-permit {none read-only read-write} | Set the permission level for login via Remote Procedure Call (RPC). The following options are available: <ul style="list-style-type: none"> <code>none</code>: No permission. <code>read-only</code>: Read-only permission. <code>read-write</code>: Read-write permission (default). |
| description <string> | Enter a description for this administrator account. When using spaces, enclose description in quotes. Character limit: 127 |
| user_type {group ldap local pki-auth radius tacacs-plus} | Enter <code>local</code> if the FortiManager system verifies the administrator's password. Enter <code>radius</code> if a RADIUS server verifies the administrator's password. Enter one of the following: <ul style="list-style-type: none"> <code>group</code>: Group user. <code>ldap</code>: LDAP user. <code>local</code>: Local user. <code>pki-auth</code>: PKI user. <code>radius</code>: RADIUS user. <code>tacacs-plus</code>: TACACS+ user. Default: <code>local</code> |
| group <string> | Enter the group name. |
| ldap-server <string> | Enter the LDAP server name if the user type is set to LDAP. |
| radius_server <string> | Enter the RADIUS server name if the user type is set to RADIUS. |
| tacacs-plus-server <string> | Enter the TACACS+ server name if the user type is set to TACACS+. |
| 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 <code>ssh-dss</code> for a DSA key, <code>ssh-rsa</code> for an RSA key. <key-value> is the public key string of the SSH client. |
| ssh-public-key2 <key-type>, <key-value> | |
| ssh-public-key3 <key-type> <key-value> | |

| Variable | Description |
|---|---|
| wildcard <enable disable> | <p>Enable/disable wildcard remote authentication. The following options are available:</p> <ul style="list-style-type: none"> <code>disable</code>: Disable username wildcard. <code>enable</code>: Enable username wildcard. |
| radius-accprofile-override <enable disable> | <p>Allow access profile to be overridden from RADIUS. The following options are available:</p> <ul style="list-style-type: none"> <code>disable</code>: Disable access profile override. <code>enable</code>: Enable access profile override. |
| radius-adom-override <enable disable> | <p>Enable/disable the ADOM to be overridden from RADIUS. The following options are available:</p> <ul style="list-style-type: none"> <code>disable</code>: Disable ADOM override. <code>enable</code>: Enable ADOM override. <p>In order to support vendor specific attributes (VSA), the RADIUS server requires a dictionary to define which VSAs to support. The Fortinet RADIUS vendor ID is 12365. The <code>Fortinet-Vdom-Name</code> attribute is used by this command.</p> |
| radius-group-match <string> | Only admin that belong to this group are allowed to login. |
| password-expire <yyyy-mm-dd> | When enforcing the password policy, enter the date that the current password will expire. |
| force-password-change {enable disable} | Enable/disable force password change on next login. |
| subject <string> | PKI user certificate name constraints. This command is available when a PKI administrator account is configured. |
| ca <string> | PKI user certificate CA (CA name in local). This command is available when a PKI administrator account is configured. |
| two-factor-auth {enable disable} | <p>Enable/disable two-factor authentication (certificate + password). The following options are available:</p> <ul style="list-style-type: none"> <code>disable</code>: Disable 2-factor authentication. <code>enable</code>: Enable 2-factor authentication. <p>This command is available when a PKI administrator account is configured.</p> |
| last-name <string> | Administrators last name. Character limit: 63 |
| first-name <string> | Administrators first name. Character limit: 63 |
| email-address <string> | Administrators email address. |
| phone-number <string> | Administrators phone number. |
| mobile-number <string> | Administrators mobile phone number. |

| Variable | Description |
|--|--|
| pager-number <string> | Administrators pager number. |
| Variables for <code>config meta-data</code> subcommand: This subcommand can only change the value of an existing field. To create a new metadata field, use the <code>config system metadata</code> command. | |
| fieldname | The label/name of the field. Read-only. Default: 50 |
| fieldlength | The maximum number of characters allowed for this field. Read-only. |
| fieldvalue <string> | Enter a pre-determined value for the field. This is the only value that can be changed with the <code>config meta-data</code> subcommand. Character limit: 255 |
| importance | Indicates whether the field is compulsory (<code>required</code>) or optional (<code>optional</code>). Read-only. Default: <code>optional</code> |
| status | For display only. Value cannot be changed. Default: <code>enable</code> |
| Variables for <code>config dashboard-tabs</code> subcommand: | |
| tabid <integer> | Tab ID. |
| name <string> | Tab name. |
| Variables for <code>config dashboard</code> subcommand: | |
| moduleid | Widget ID. <ul style="list-style-type: none"> 1: System Information 2: System Resources 3: License Information 4: Unit Operation 5: Log Receive Monitor 6: Logs/Data Received 7: Statistics 8: Insert Rate vs Receive Rate 9: Log Insert Lag Time 10: Alert Message Console 11: CLI Console 12: Disk I/O |
| name <string> | Widget name. Character limit: 63 |
| column <column_pos> | Widget's column ID. |
| refresh-interval <integer> | Widget's refresh interval. Default: 300 |

| Variable | Description |
|---|--|
| status {close open} | Widget's opened/closed status. Default: open |
| tabid <integer> | ID of the tab where the widget is displayed. Default: 0 |
| widget-type <string> | Widget type. The following options are available: <ul style="list-style-type: none"> • alert: Alert Message Console. • devsummary: Device Summary. • jsconsole: CLI Console. • licinfo: License Information. • logdb-lag: Log Database Lag Time. • logdb-perf: Log Database Performance Monitor. • logrecv: Logs/Data Received. • raid: Disk Monitor. • rpteng: Report Engine. • statistics: Statistics. • sysinfo: System Information. • sysop: Unit Operation. • sysres: System resources. • top-lograte: Log Receive Monitor. |
| log-rate-type {device log} | Log receive monitor widget's statistics breakdown options. |
| log-rate-topn {1 2 3 4 5} | Log receive monitor widgets's number of top items to display. |
| log-rate-period {1hour 2min 6hours} | Log receive monitor widget's data period. |
| res-view-type {history real-time} | Widget's data view type. The following options are available: <ul style="list-style-type: none"> • history: History view. • real-time: Real-time view. |
| res-period {10min day hour} | Widget's data period. The following options are available: <ul style="list-style-type: none"> • 10min: Last 10 minutes. • day: Last day. • hour: Last hour. |
| res-cpu-display {average each} | Widget's CPU display type. The following options are available: <ul style="list-style-type: none"> • average: Average usage of CPU. • each: Each usage of CPU. |
| num-entries <integer> | Number of entries. |
| time-period {1hour 24hour 8hour} | Set the Log Database Monitor widget's data period. One of 1 hour, 8 hours, or 24 hours. |

| Variable | Description |
|---|--|
| diskio-content-type {blks iops util} | Set the Disk I/O Monitor widget's chart type. <ul style="list-style-type: none"> blks: the amount of data of I/O requests. iops: the number of I/O requests. util: bandwidth utilization. |
| diskio-period {1hour 24hour 8hour} | Set the Disk I/O Monitor widget's data period. |
| Variable for <code>config restrict-dev-vdom</code> subcommand: | |
| dev-vdom <string> | Enter device or VDOM to edit. |

Using trusted hosts

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

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

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

Example

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

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

alert-console

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

Syntax

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

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

Example

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

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

alert-event

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

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



`alert-event` was removed from the GUI in FortiManager version 5.0.3. This command has been kept in the CLI for customers who previously configured this function.

Syntax

```
config system alert-event
    edit <name_string>
        config alert-destination
            edit destination_id <integer>
                set type {mail | snmp | syslog}
                set from <email_address>
                set to <email_address>
                set smtp-name <server_name>
                set snmp-name <server_name>
                set syslog-name <server_name>
            end
        end
    end
end
```

```

end
set enable-generic-text {enable | disable}
set enable-severity-filter {enable | disable}
set event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}
set generic-text <string>
set num-events {1 | 5 | 10 | 50 | 100}
set severity-filter {high | low | medium | medium-high | medium-low}
set severity-level-comp {>= | = | <=}
set severity-level-logs {no-check | information | notify | warning | error |
    critical | alert | emergency}
end

```

| Variable | Description |
|---|--|
| <name_string> | Enter a name for the alert event. Character limit: 63 |
| destination_id <integer> | Enter the table sequence number, beginning at 1. |
| type {mail snmp syslog} | Select the alert event message method of delivery. The following options are available: <ul style="list-style-type: none"> mail: Send email alert (default). snmp: Send SNMP trap. syslog: Send syslog message. |
| from <email_address> | Enter the email address of the sender of the message. This is available when the type is set to mail. |
| to <email_address> | Enter the recipient of the alert message. This is available when the type is set to mail. |
| smtp-name <server_name> | Enter the name of the mail server. This is available when the type is set to mail. |
| snmp-name <server_name> | Enter the snmp server name. This is available when the type is set to snmp. |
| syslog-name <server_name> | Enter the syslog server name or IPv4 address. This is available when the type is set to syslog. |
| enable-generic-text {enable disable} | Enable the text alert option. Default: disable |
| enable-severity-filter {enable disable} | Enable the severity filter option. Default: disable |

| Variable | Description |
|--|--|
| event-time-period {0.5 1 3 6 12 24 72 168} | The period of time in hours during which if the threshold number is exceeded, the event will be reported. The following options are available: <ul style="list-style-type: none"> 0.5: 30 minutes. 1: 1 hour. 3: 3 hours. 6: 6 hours. 12: 12 hours. 24: 1 day. 72: 3 days. 168: 1 week. |
| generic-text <string> | Enter the text the alert looks for in the log messages. Character limit: 255 |
| num-events {1 5 10 50 100} | Set the number of events that must occur in the given interval before it is reported. |
| severity-filter {high low medium medium-high medium-low} | Set the alert severity indicator for the alert message the FortiManager unit sends to the recipient. The following options are available: <ul style="list-style-type: none"> high: High level alert. low: Low level alert. medium: Medium level alert. medium-high: Medium-high level alert. medium-low: Medium-low level alert. |
| severity-level-comp {>= = <=} | Set the severity level in relation to the log level. Log messages are monitored based on the log level. For example, alerts may be monitored if the messages are greater than, and equal to (>=) the Warning log level. The following options are available: <ul style="list-style-type: none"> >=: Greater than or equal to. =: Equal to. <=: Less than or equal to. |
| severity-level-logs {no-check information notify warning error critical alert emergency} | Set the log level the FortiManager looks for when monitoring for alert messages. The following options are available: <ul style="list-style-type: none"> no-check: Do not check severity level for this log type. 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. |

Example

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

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

alertemail

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

All variables are required if `authentication` is enabled.

Syntax

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

| Variable | Description |
|------------------------------------|--|
| authentication {enable disable} | Enable/disable alert email authentication. Default: <code>enable</code> |
| fromaddress <email-address_string> | The email address the alertmessage is from. This is a required variable. |
| fromname <string> | The SMTP name associated with the email address. To enter a name that includes spaces, enclose the whole name in quotes. |
| smtppassword <passwd> | Set the SMTP server password. Character limit: 39 |
| smtpport <integer> | The SMTP server port. Default: 25. Range: 1 to 65535 |

| Variable | Description |
|---|--|
| smtpserver {<ipv4_address> <fqdn_string>} | The SMTP server address. Enter either a DNS resolvable host name or an IPv4 address. |
| smtpuser <username> | Set the SMTP server username. Character limit: 63 |

Example

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

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

auto-delete

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

Syntax

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

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

backup all-settings

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

Syntax

```

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

```

| Variable | Description |
|------------------------------------|--|
| status {enable disable} | Enable/disable scheduled backups. Default: <code>disable</code> |
| server {<ipv4_address> <fqdn_str>} | Enter the IPv4 address or DNS resolvable host name of the backup server. |
| user <username> | Enter the user account name for the backup server. Character limit: 63 |
| directory <string> | Enter the name of the directory on the backup server in which to save the backup file. |

| Variable | Description |
|---|--|
| <code>week_days {monday tuesday wednesday thursday friday saturday sunday}</code> | Enter the days of the week on which to perform backups. You may enter multiple days. |
| <code>time <hh:mm:ss></code> | Enter the time of day to perform the backup. Time is required in the form <hh:mm:ss>. |
| <code>protocol {ftp scp sftp}</code> | Enter the transfer protocol: <code>ftp</code> , <code>scp</code> , or <code>sftp</code> (default). |
| <code>passwd <passwd></code> | Enter the password for the backup server. Character limit: 63 |
| <code>cert <string></code> | SSH certificate for authentication. Only available if the protocol is set to <code>scp</code> . |
| <code>crptpasswd <passwd></code> | Optional password to protect backup content. Character limit: 63 |

Example

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

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

certificate

Use the following commands to configure certificate related settings.

certificate ca

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

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

The process for obtaining and installing certificates is as follows:

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

Syntax

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

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

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

| Variable | Description |
|------------------|---|
| <ca_name> | Enter a name for the CA certificate. Character limit: 35 |
| ca <certificate> | Enter or retrieve the CA certificate in PEM format. |
| comment <string> | Optionally, enter a descriptive comment. Character limit: 127 |

certificate crl

Use this command to configure CRLs.

Syntax

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

| Variable | Description |
|------------------|--|
| <name> | Enter a name for the CRL. Character limit: 35 |
| crl <crl> | Enter or retrieve the CRL in PEM format. |
| comment <string> | Optionally, enter a descriptive comment for this CRL. Character limit: 127 |

certificate local

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

The process for obtaining and installing certificates is as follows:

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

Syntax

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

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

```
get system certificate local [cert_name]
```

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

certificate oftp

Use this command to install OFTP certificates and keys.

Syntax

```
config system certificate oftp
  set certificate <certificate>
  set comment <string>
  set custom {enable | disable}
  set password
  set private-key <key>
end
```

| Variable | Description |
|-----------------------------|--|
| certificate <certificate> | PEM format certificate. |
| comment <string> | OFTP certificate comment. Character limit: 127 |
| custom {enable disable} | Enable/disable custom certificates. |
| password {enable disable} | Enable/disable passwords. |
| private-key <key> | PEM format private key. |

certificate ssh

Use this command to install SSH certificates and keys.

The process for obtaining and installing certificates is as follows:

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

Syntax

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

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

```
get system certificate ssh [cert_name]
```

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

dm

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

Syntax

```
config system dm
  set concurrent-install-image-limit <integer>
  set concurrent-install-limit <integer>
  set concurrent-install-script-limit <integer>
  set discover-timeout <integer>
  set dpm-logsize <integer>
  set fgfm-sock-timeout <integer>
  set fgfm-keepalive_itvl <integer>
  set force-remote-diff {enable | disable}
```

```

set fortiap-refresh-itvl <integer>
set install-image-tunnel-timeout <integer>
set install-tunnel-retry-itvl <integer>
set max-revs <integer>
set nr-retry <integer>
set retry {enable | disable}
set retry-intvl <integer>
set rollback-allow-reboot {enable | disable}
set script-logsize <integer>

set verify-install {enable | disable | optimal}
end

```

| Variable | Description |
|---|---|
| concurrent-install-image-limit <integer> | The maximum number of concurrent installs. Range: 5 to 1000. Default: 480 |
| concurrent-install-limit <integer> | The maximum number of concurrent installs. Range: 5 to 1000. Default: 480 |
| concurrent-install-script-limit <integer> | The maximum number of concurrent install scripts. Range: 5 to 1000. Default: 480 |
| discover-timeout <integer> | Check connection timeout when discovering a device. Range: 3 to 15. |
| dpm-logsize <integer> | The maximum DPM log size per device. Range: 1 to 10000 (kB). Default: 10000 |
| fgfm-sock-timeout <integer> | The maximum FortiManager /FortiGate communication socket idle time. Range: 90 to 1800 (seconds). Default: 360 |
| fgfm_heartbeat_itvl <integer> | The interval at which the FortiManager will send a heartbeat signal to a FortiGate unit to keep the FortiManager /FortiGate communication protocol active. Range: 30 to 600 (seconds). Default: 120 |
| force-remote-diff {enable disable} | Enable to always use <code>remote diff</code> when installing. Default: disable |
| fortiap-refresh-itvl <integer> | Auto refresh FortiAP status interval. Range: 1 to 1440 (minutes) |
| install-image-tunnel-timeout <integer> | Time to timeout tunnel (10-60 sec). |
| install-tunnel-retry-itvl <integer> | Time to re-establish tunnel during install (10-60 sec). |
| max-revs <integer> | The maximum number of revisions saved. Range: 1 to 250. Default: 100 |
| nr-retry <integer> | The number of times the FortiManager unit will retry. Default: 1 |
| retry {enable disable} | Enable/disable configuration installation retries. Default: enable |

| Variable | Description |
|---|--|
| retry-intvl <integer> | The interval between attempting another configuration installation following a failed attempt. Default: 15 |
| rollback-allow-reboot {enable disable} | Enable/disable allowing a FortiGate unit to reboot when installing a script or configuration. Default: <code>disable</code> |
| script-logsize <integer> | Enter the maximum script log size per device. Range: 1 to 10000 (kB). |
| skip-tunnel-fcp-req {enable disable} | Enable/disable skipping the FCP request sent from an FGFM tunnel |
| verify-install {enable disable optimal} | Enable/disable verify install against remote configuration. The following options are available: <ul style="list-style-type: none"> <code>disable</code>: Disable. <code>enable</code>: Always verify installation (default). <code>optimal</code>: Verify installation for command errors. |

Example

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

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

dns

Use these commands to set the DNS server addresses. Several FortiManager functions, including sending alert email, use DNS. In FortiManager v5.2.1 or later, you can configure both IPv4 and IPv6 DNS server addresses.

Syntax

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

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

Example

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

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

fips

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

Syntax

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

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

fortiview setting

Use this command to configure FortiView settings.

Syntax

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

| Variable | Description |
|--------------------------------------|--|
| not-scanned apps {exclude include} | Include/exclude 'Not.Scanned' applications in FortiView. |
| resolve-ip {enable disable} | Enable or disable resolving the IP address to the hostname in FortiView. |

fortiview autocache settings

Use this command to configure FortiView autocache settings.

Syntax

```
config system fortiview auto-cache
    set aggressive-fortiview
    set interval
    set status
end
```

| Variable | Description |
|----------------------|---|
| aggressive-fortiview | Configure FortiView drilldown settings. |
| interval | Configure FortiView interval settings. |
| status | Configure FortiView status settings. |

global

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

Syntax

```
config system global
    set admin-https-pki-required {disable | enable}
    set admin-lockout-duration <integer>
    set admin-lockout-threshold <integer>
    set adom-mode {advanced | normal}sh
    set adom-rev-auto-delete {by-days | by-revisions | disable}
    set adom-rev-max-backup-revisions <integer>
    set adom-rev-max-days <integer>
    set adom-rev-max-revisions <integer>
    set adom-select {enable | disable}
    set adom-status {enable | disable}
    set auto-register-device {enable | disable}
    set clt-cert-req {disable | enable}
    set console-output {more | standard}
    set create-revision {disable | enable}
    set daylightsavetime {enable | disable}
    set default-disk-quota <integer>
    set detect-unregistred-log-device {enable | disable}
```

```

set faz-status {enable | disable}
set fgfm-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
set enc-algorithm {default | high | low}
set hostname <string>
set language {english | japanese | simch | trach}
set ldapconntimeout <integer>
set lock-preempt {enable | disable}
set log-checksum {md5 | md5-auth | none}
set max-log-forward <integer>
set max-running-reports <integer>
set oftp-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
set partial-install {enable | disable}
set partial-install-rev {enable | disable}
set policy-hit-count {enable | disable}
set pre-login-banner {disable | enable}
set pre-login-banner-message <string>
set remoteauthtimeout <integer>
set search-all-adoms {enable | disable}
set ssl-low-encryption {enable | disable}
set ssl-protocol {tlsv1 | sslsv3}
set swapmem {enable | disable}
set task-list-size <integer>
set timezone <integer>
set tunnel-mtu <integer>
set vdom-mirror {enable | disable}
set webservice-proto {tlsv1 | sslsv3 | sslsv2}
set workflow-max-sessions <integer>
set workspace-mode {disabled | normal | workflow}
end

```

| Variable | Description |
|--|---|
| admin-https-pki-required {disable enable} | <p>Enable/disable HTTPS login page when PKI is enabled. The following options are available:</p> <ul style="list-style-type: none"> • disable: Admin users can login by providing a valid certificate or password. • enable: Admin users have to provide a valid certificate when PKI is enabled for HTTPS admin access. <p>When both <code>set clt-cert-req</code> and <code>set admin-https-pki-required</code> are enabled, only PKI administrators can connect to the FortiManager GUI.</p> |
| admin-lockout-duration <integer> | <p>Set the lockout duration (seconds) for FortiManager administration. Default: 60</p> |
| admin-lockout-threshold <integer> | <p>Set the lockout threshold for FortiManager administration. Range: 1 to 10. Default: 3</p> |
| adom-mode {advanced normal} | <p>Set the ADOM mode: <code>advanced</code> or <code>normal</code>.</p> |

| Variable | Description |
|---|--|
| adom-rev-auto-delete {by-days by-revisions disable} | Auto delete features for old ADOM revisions: <ul style="list-style-type: none"> <code>by-days</code>: Auto delete ADOM revisions by maximum days. <code>by-revisions</code>: Auto delete ADOM revisions by maximum number of revisions. <code>disable</code>: Disable auto delete function for ADOM revision. |
| adom-rev-max-backup-revisions <integer> | The maximum number of ADOM revisions to backup. |
| adom-rev-max-days <integer> | The maximum number of days to keep old ADOM revisions. |
| adom-rev-max-revisions <integer> | The maximum number of ADOM revisions to keep. |
| adom-status {enable disable} | Enable/disable administrative domains (ADOMs). Default: <code>disable</code> |
| adom-select {enable disable} | Enable/disable a pop-up window that allows administrators to select an ADOM after logging in. Default: <code>enable</code> |
| auto-register-device {enable disable} | Enable or disable device auto registration by log message. |
| clt-cert-req {disable enable} | Enable/disable requiring a client certificate for GUI login. The following options are available: <ul style="list-style-type: none"> <code>disable</code>: Disable setting. <code>enable</code>: Require client certificate for GUI login. When both <code>set clt-cert-req</code> and <code>set admin-https-pki-required</code> are enabled, only PKI administrators can connect to the FortiManager GUI. |
| console-output {more standard} | Select how the output is displayed on the console. Select <code>more</code> to pause the output at each full screen until keypress. Select <code>standard</code> for continuous output without pauses. The following options are available: <ul style="list-style-type: none"> <code>more</code>: More page output. <code>standard</code>: Standard output (default) |
| create-revision {disable enable} | Enable/disable create revision by default. The following options are available: <ul style="list-style-type: none"> <code>disable</code>: Disable create revision by default. <code>enable</code>: Enable create revision by default. |
| daylightsavetime {enable disable} | Enable/disable daylight saving time. If you enable daylight saving time, the FortiManager unit automatically adjusts the system time when daylight saving time begins or ends. Default: <code>enable</code> |
| default-disk-quota <integer> | Default disk quota (MB) for registered device. Range: 100 to 100 000 (MB). |
| detect-unregistered-log-device | Enable/disable unregistered log device detection. |

| Variable | Description |
|--|---|
| faz-status {enable disable} | Enable/disable FortiAnalyzer features in FortiManager. This command is not available on the FMG-100C. |
| fgfm-ssl-protocol {ssl3 tlsv1.0 tlsv1.1 tlsv1.2} | Set the lowest SSL protocols for fgfmsd. Default: <code>tlsv1.0</code> . |
| enc-algorithm {default high low} | Set SSL communication encryption algorithms. The following options are available: <ul style="list-style-type: none"> <code>high</code>: SSL communication using high encryption algorithms. <code>low</code>: SSL communication using all available encryption algorithms. <code>medium</code>: SSL communication using high and medium encryption algorithms. Default: <code>default</code> |
| hostname <string> | FortiManager host name. |
| language {english japanese simch trach} | GUI language. The following options are available: <ul style="list-style-type: none"> <code>english</code>: English <code>japanese</code>: Japanese <code>simch</code>: Simplified Chinese <code>trach</code>: Traditional Chinese Default: <code>English</code> |
| ldapconntimeout <integer> | LDAP connection timeout (in milliseconds). Default: <code>60000</code> |
| lock-preempt {enable disable} | Enable/disable the ADOM lock override. |
| log-checksum {md5 md5-auth none} | Record log file hash value, timestamp, and authentication code at transmission or rolling. The following options are available: <ul style="list-style-type: none"> <code>md5</code>: Record log file's MD5 hash value only <code>md5-auth</code>: Record log file's MD5 hash value and authentication code <code>none</code>: Do not record the log file checksum |
| max-log-forward <integer> | Set the maximum log forwarding and aggregation number, from 5 to 20. |
| max-running-reports <integer> | Maximum running reports number. Range: 1 to 10 |
| oftp-ssl-protocol {ssl3 tlsv1.0 tlsv1.1 tlsv1.2} | Set the lowest SSL protocols for oftpd. Default: <code>tlsv1.0</code> . |
| partial-install {enable disable} | Enable/disable partial install (install only some objects). Use this command to enable pushing individual objects of the policy package down to all FortiGates in the Policy Package. Once enabled, in the GUI you can right-click an object and choose to install it. |

| Variable | Description |
|---|--|
| partial-install-rev {enable disable} | Enable/disable partial install revision. |
| policy-hit-count {enable disable} | Enable/disable show policy hit count. Default: <code>disable</code> The policy hit count is the number of sessions that match to a firewall policy on a FortiGate. When <code>policy-hit-count</code> is enabled, it collects all hits from all managed FortiGate devices. FortiManager sums up all hit counts for each policy package from the assigned FortiGate devices, and displays the hit count for each of the firewall rules. |
| pre-login-banner {disable enable} | Enable/disable pre-login banner. |
| pre-login-banner-message <string> | Set the pre-login banner message. |
| remoteauthtimeout <integer> | Remote authentication (RADIUS/LDAP) timeout (in seconds). Default: 10 |
| search-all-adoms {enable disable} | Enable/disable search all ADOMs for where-used queries. |
| ssl-low-encryption {enable disable} | Enable/disable SSL low-grade (40-bit) encryption. Default: <code>enable</code> |
| ssl-protocol {tls1 sslv3} | Set the SSL protocols: <code>tls1</code> or <code>sslv3</code> . |
| swapmem {enable disable} | Enable/disable virtual memory. |
| task-list-size <integer> | Set the maximum number of completed tasks to keep. Default: 2000 |
| timezone <integer> | The time zone for the FortiManager unit. Default: (GMT-8) Pacific Time (US & Canada) |
| tunnel-mtu <integer> | Set the maximum transportation unit, from 68 to 9000. Default: 1500. |
| vdom-mirror {enable disable} | Enable/disable VDOM mirror. Once enabled in the CLI, you can select to enable VDOM Mirror when editing a virtual domain in the System > Virtual Domain device tab in Device Manager. You can then add devices and VDOMs to the list so they may be mirrored. A icon is displayed in the Mirror column of this page to indicate that the VDOM is being mirrored to another device/VDOM. When changes are made to the master device's VDOM database, a copy is applied to the mirror device's VDOM database. A revision is created and then installed to the devices. Default: <code>disable</code> VDOM mirror is intended to be used by MSSP or enterprise companies who need to provide a backup VDOM for their customers. |
| webservice-proto {tls1 sslv3 sslv2} | Web Service connection: <code>tls1</code> , <code>sslv3</code> , or <code>sslv2</code> . |

| Variable | Description |
|--|--|
| workflow-max-sessions <integer> | Maximum number of workflow sessions per ADOM. Range: 100 to 1000. Default: 500 |
| workspace-mode {disabled normal workflow} | Enable/disable Workspace and Workflow (ADOM locking). The following options are available: <ul style="list-style-type: none"> disabled: Workspace is disabled. normal: Workspace lock mode enabled. workspace: Workspace workflow mode enabled. |

Example

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

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

Time zones

| Integer | Time zone | Integer | Time zone |
|-----------|--|---------|---|
| 00 | (GMT-12:00) Eniwetak, Kwajalein | 40 | (GMT+3:00) Nairobi |
| 01 | (GMT-11:00) Midway Island, Samoa | 41 | (GMT+3:30) Tehran |
| 02 | (GMT-10:00) Hawaii | 42 | (GMT+4:00) Abu Dhabi, Muscat |
| 03 | (GMT-9:00) Alaska | 43 | (GMT+4:00) Baku |
| 04 | (GMT-8:00) Pacific Time (US & Canada) | 44 | (GMT+4:30) Kabul |
| 05 | (GMT-7:00) Arizona | 45 | (GMT+5:00) Ekaterinburg |
| 06 | (GMT-7:00) Mountain Time (US & Canada) | 46 | (GMT+5:00) Islamabad, Karachi, Tashkent |
| 07 | (GMT-6:00) Central America | 47 | (GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi |
| 08 | (GMT-6:00) Central Time (US & Canada) | 48 | (GMT+5:45) Kathmandu |
| 09 | (GMT-6:00) Mexico City | 49 | (GMT+6:00) Almaty, Novosibirsk |
| 10 | (GMT-6:00) Saskatchewan | 50 | (GMT+6:00) Astana, Dhaka |
| 11 | (GMT-5:00) Bogota, Lima, Quito | 51 | (GMT+6:00) Sri Jayawardenapura |
| 12 | (GMT-5:00) Eastern Time (US & Canada) | 52 | (GMT+6:30) Rangoon |

| Integer | Time zone | Integer | Time zone |
|---------|--|---------|---|
| 13 | (GMT-5:00) Indiana (East) | 53 | (GMT+7:00) Bangkok, Hanoi, Jakarta |
| 14 | (GMT-4:00) Atlantic Time (Canada) | 54 | (GMT+7:00) Krasnoyarsk |
| 15 | (GMT-4:00) La Paz | 55 | (GMT+8:00) Beijing, ChongQing, HongKong, Urumqi |
| 16 | (GMT-4:00) Santiago | 56 | (GMT+8:00) Irkutsk, Ulaanbaatar |
| 17 | (GMT-3:30) Newfoundland | 57 | (GMT+8:00) Kuala Lumpur, Singapore |
| 18 | (GMT-3:00) Brasilia | 58 | (GMT+8:00) Perth |
| 19 | (GMT-3:00) Buenos Aires, Georgetown | 59 | (GMT+8:00) Taipei |
| 20 | (GMT-3:00) Nuuk (Greenland) | 60 | (GMT+9:00) Osaka, Sapporo, Tokyo, Seoul |
| 21 | (GMT-2:00) Mid-Atlantic | 61 | (GMT+9:00) Yakutsk |
| 22 | (GMT-1:00) Azores | 62 | (GMT+9:30) Adelaide |
| 23 | (GMT-1:00) Cape Verde Is | 63 | (GMT+9:30) Darwin |
| 24 | (GMT) Casablanca, Monrovia | 64 | (GMT+10:00) Brisbane |
| 25 | (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London | 65 | (GMT+10:00) Canberra, Melbourne, Sydney |
| 26 | (GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna | 66 | (GMT+10:00) Guam, Port Moresby |
| 27 | (GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague | 67 | (GMT+10:00) Hobart |
| 28 | (GMT+1:00) Brussels, Copenhagen, Madrid, Paris | 68 | (GMT+10:00) Vladivostok |
| 29 | (GMT+1:00) Sarajevo, Skopje, Sofia, Vilnius, Warsaw, Zagreb | 69 | (GMT+11:00) Magadan |
| 30 | (GMT+1:00) West Central Africa | 70 | (GMT+11:00) Solomon Is., New Caledonia |
| 31 | (GMT+2:00) Athens, Istanbul, Minsk | 71 | (GMT+12:00) Auckland, Wellington |
| 32 | (GMT+2:00) Bucharest | 72 | (GMT+12:00) Fiji, Kamchatka, Marshall Is |
| 33 | (GMT+2:00) Cairo | 73 | (GMT+13:00) Nuku'alofa |
| 34 | (GMT+2:00) Harare, Pretoria | 74 | (GMT-4:30) Caracas |
| 35 | (GMT+2:00) Helsinki, Riga, Tallinn | 75 | (GMT+1:00) Namibia |

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

ha

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

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

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

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

Syntax

```
config system ha
    set clusterid <clusert_ID_int>
    set file-quota <integer>
    set hb-interval <integer>
    set hb-lost-threshold <integer>
    set mode {master | slave | standalone}
    set password <passwd>
    config peer
        edit <peer_id_int>
            set ip <peer_ipv4_address>
            set ip6 <peer_ipv6_address>
            set serial-number <string>
            set status <peer_status>
        end
    end
end
```

| Variable | Description |
|---|---|
| clusterid <cluser_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. |
| file-quota <integer> | Set the HA file quota, in MB (2048 - 20480). |
| hb-interval <integer> | 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. Range: 1 to 255 (seconds) Default: 5 (seconds) |
| hb-lost-threshold <integer> | 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. Range: 1 to 255 Default: 3 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. 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. 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. |
| mode {master slave standalone} | Select <code>master</code> to configure the FortiManager unit to be the primary unit in a cluster. Select <code>slave</code> to configure the FortiManager unit to be a backup unit in a cluster. Select <code>standalone</code> to stop operating in HA mode. |
| password <passwd> | A group password for the HA cluster. All members of the HA cluster must have the same group password. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password. Character limit: 19 |
| peer | 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 four). For each backup unit you add the primary unit. |
| Variables for <code>config peer</code> subcommand: | |

| Variable | Description |
|-------------------------|---|
| <peer_id_int> | Add a peer and add the peer's IPv4 or IPv6 address and serial number. |
| ip <peer_ipv4_address> | Enter the IPv4 address of the peer FortiManager unit. |
| ip6 <peer_ipv6_address> | Enter the IPv6 address of the peer FortiManager unit. |
| serial-number <string> | Enter the serial number of the peer FortiManager unit. |
| status <peer_status> | Enter the status of the peer FortiManager unit. |

General FortiManager HA configuration steps

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

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

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

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

3. Repeat step 2 to configure each backup unit.

interface

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

Syntax

```
config system interface
  edit <port>
    set status {up | down}
    set ip <ipv4_mask>
    set allowaccess {http https ping snmp ssh telnet webservice}
    set serviceaccess {fclupdates fgtupdates webfilter-antispam}
    set speed {1000full 100full 100half 10full 10half auto}
    set description <string>
    set alias <string>
    set mtu <integer>
    config <ipv6>
      set ip6-address <ipv6 prefix>
      set ip6-allowaccess {http https ping snmp ssh telnet webservice}
    end
  end
end
```

| Variable | Description |
|--|---|
| <port> | <port> can be set to a port number such as port1, port2, port3, or port4. Different FortiManager models have different numbers of ports. |
| status {up down} | Start or stop the interface. If the interface is stopped it does not accept or send packets. If you stop a physical interface, VLAN interfaces associated with it also stop. Default: up |
| ip <ipv4_mask> | Enter the interface IPv4 address and netmask. The IPv4 address cannot be on the same subnet as any other interface. |
| 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. Options include: http, https, ping, snmp, ssh, telnet, and webservice. |

| Variable | Description |
|---|---|
| serviceaccess {fclupdates fgtupdates webfilter-antispam} | Enter the types of service access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required. The following options are available: <ul style="list-style-type: none"> fclupdates: FortiClient updates access. fgtupdates: FortiGate updates access. webfilter-antispam: Web filtering and antispam access. |
| speed {1000full 100full 100half 10full 10half auto} | Enter the speed and duplexing the network port uses. Enter <code>auto</code> to automatically negotiate the fastest common speed. The following options are available: <ul style="list-style-type: none"> 100full: 100M full-duplex. 100half: 100M half-duplex. 10full: 10M full-duplex. 10half: 10M half-duplex. auto: Auto adjust speed default). |
| description <string> | Enter a description of the interface. Character limit: 63 |
| alias <string> | Enter an alias for the interface. |
| mtu <integer> | Set the maximum transportation unit, from 68 to 9000. Default: 1500. |
| Variables for <code>config ipv6</code> subcommand: | |
| ip6-address <ipv6 prefix> | IPv6 address/prefix of interface. |
| ip6-allowaccess {http https ping snmp ssh telnet web-service} | Allow management access to the interface. Options include: <code>http</code> , <code>https</code> , <code>ping</code> , <code>snmp</code> , <code>ssh</code> , <code>telnet</code> , and <code>web-service</code> . |

Example

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

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

locallog

Use the following commands to configure local log settings.

locallog setting

Use this command to configure locallog logging settings.

Syntax

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

| Variable | Description |
|---------------------------------------|---|
| log-interval-dev-no-logging <integer> | Interval in minute for logging the event of no logs received from a device. Default: 5. |
| log-interval-disk-full <integer> | Interval in minute for logging the event of disk full. Default: 5. |
| log-interval-gbday-exceeded <integer> | Interval in minute for logging the event of the GB/Day license exceeded. Default: 1440. |

locallog disk setting

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

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

Syntax

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

end

| Variable | Description |
|--|---|
| status {enable disable} | Enable or disable logging to the local disk. Default: <code>disable</code> |
| severity {alert critical debug emergency error information notification warning} | <p>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.</p> <p>The logging levels in descending order are:</p> <ul style="list-style-type: none"> • <code>emergency</code>: The unit is unusable. • <code>alert</code>: Immediate action is required (default). • <code>critical</code>: Functionality is affected. • <code>error</code>: Functionality is probably affected. • <code>warning</code>: Functionality might be affected. • <code>notification</code>: Information about normal events. • <code>information</code>: General information about unit operations. • <code>debug</code>: Information used for diagnosis or debugging. |
| max-log-file-size <integer> | <p>Enter the size at which the log is rolled.</p> <p>Range: 1 to 1024 (MB)</p> <p>Default: 100</p> |
| roll-schedule {none daily weekly} | <p>Enter the period for the scheduled rolling of a log file. If <code>roll-schedule</code> is <code>none</code>, the log rolls when <code>max-log-file-size</code> is reached. The following options are available:</p> <ul style="list-style-type: none"> • <code>none</code>: Not scheduled (default). • <code>daily</code>: Every day. • <code>weekly</code>: Every week. |
| roll-day <string> | Enter the day for the scheduled rolling of a log file. |
| roll-time <hh:mm> | Enter the time for the scheduled rolling of a log file. |
| diskfull {nolog overwrite} | <p>Enter action to take when the disk is full:</p> <ul style="list-style-type: none"> • <code>nolog</code>: stop logging • <code>overwrite</code>: overwrites oldest log entries (default) |
| log-disk-full-percentage <integer> | Enter the percentage at which the log disk will be considered full (50-90%). |
| upload {disable enable} | Enable or disable uploading of logs when rolling log files. Default: <code>disable</code> |
| uploadip <ipv4_address> | Enter IPv4 address of the destination server. Default: 0.0.0.0 |

| Variable | Description |
|--|---|
| server-type {FAZ FTP SCP SFTP} | Enter the server type to use to store the logs: <ul style="list-style-type: none"> FAZ: Upload to FortiAnalyzer. FTP: Upload via FTP. SCP: Upload via SCP. SFTP: Upload via SFTP. |
| uploadport <integer> | Enter the port to use when communicating with the destination server. Default: 21. Range: 1 to 65535 |
| uploaduser <string> | Enter the user account on the destination server. |
| uploadpass <passwd> | Enter the password of the user account on the destination server. Character limit: 127 |
| uploaddir <string> | Enter the destination directory on the remote server. |
| uploadtype <event> | Enter to upload the event log files. Default: event |
| uploadzip {disable enable} | Enable to compress uploaded log files. Default: disable |
| uploadsched {disable enable} | Enable to schedule log uploads. The following options are available: <ul style="list-style-type: none"> disable: Upload when rolling. enable: Scheduled upload. |
| upload-time <hh:mm> | Enter to configure when to schedule an upload. |
| upload-delete-files {disable enable} | Enable or disable deleting log files after uploading. Default: enable |

Example

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

```
config system locallog disk setting
    set status enable
    set severity information
    set max-log-file-size 1000MB
    set roll-schedule daily
    set upload enable
    set uploadip 10.10.10.1
    set uploadport port 443
    set uploaduser myname2
    set uploadpass 12345
    set uploadtype event
    set uploadzip enable
    set uploadsched enable
    set upload-time 06:45
    set upload-delete-file disable
end
```

locallog filter

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

Syntax

```
config system locallog [memory | disk | fortianalyzer | fortianalyzer2 |
    fortianalyzer3 | syslogd | syslogd2 | syslogd3] filter
    set devcfg {disable | enable}
    set devops {disable | enable}
    set dm {disable | enable}
    set dvm {disable | enable}
    set epmgr {disable | enable}
    set event {disable | enable}
    set faz {enable | disable}
    set fgd {disable | enable}
    set fgfm {disable | enable}
    set fips {disable | enable}
    set fmgws {disable | enable}
    set fmlmgr {disable | enable}
    set fmwmgr {disable | enable}
    set glbcfg {disable | enable}
    set ha {disable | enable}
    set iolog {disable | enable}
    set logd {disable | enable}
    set lrmgr {disable | enable}
    set objcfg {disable | enable}
    set rev {disable | enable}
    set rtmon {disable | enable}
    set scfw {disable | enable}
    set scply {disable | enable}
    set scrmgr {disable | enable}
    set scvpn {disable | enable}
    set system {disable | enable}
    set webport {disable | enable}
end
```

| Variable | Description |
|---------------------------|--|
| devcfg {disable enable} | Enable to log device configuration messages. |
| devops {disable enable} | Enable managed devices operations messages. |
| dm {disable enable} | Enable to log deployment manager messages. Default: <code>disable</code> |
| dvm {disable enable} | Enable to log device manager messages. Default: <code>disable</code> |
| epmgr {disable enable} | Enable to log endpoint manager messages. Default: <code>disable</code> |
| event {disable enable} | Enable to configure log filter messages. Default: <code>disable</code> |
| faz {enable disable} | Enable to log FortiAnalyzer messages. Default: <code>disable</code> |

| Variable | Description |
|----------------------------|--|
| fgd {disable enable} | Enable to log FortiGuard service messages. Default: disable |
| fgfm {disable enable} | Enable to log FortiGate/FortiManager communication protocol messages. Default: disable |
| fips {disable enable} | Enable to log FIPS messages. Default: disable |
| fmgws {disable enable} | Enable to log web service messages. Default: disable |
| fmlmgr {disable enable} | Enable to log FortiMail manager messages. Default: disable |
| fmwmgr {disable enable} | Enable to log firmware manager messages. Default: disable |
| glbcfg {disable enable} | Enable to log global database messages. Default: disable |
| ha {disable enable} | Enable to log high availability activity messages. Default: disable |
| iolog {disable enable} | Enable input/output log activity messages. Default: disable |
| logd {disable enable} | Enable logd messages. Default: disable |
| lrngr {disable enable} | Enable to log log and report manager messages. Default: disable |
| objcfg {disable enable} | Enable to log object configuration. Default: disable |
| rev {disable enable} | Enable to log revision history messages. Default: disable |
| rtmon {disable enable} | Enable to log real-time monitor messages. Default: disable |
| scfw {disable enable} | Enable to log firewall objects messages. Default: disable |
| scply {disable enable} | Enable to log policy console messages. Default: disable |
| scrmgr {disable enable} | Enable to log script manager messages. Default: disable |
| scvpn {disable enable} | Enable to log VPN console messages. Default: disable |
| system {disable enable} | Enable to log system manager messages. Default: disable |
| webport {disable enable} | Enable to log web portal messages. Default: disable |

Example

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

```
config system locallog filter
  set event enable
  set lrngr enable
  set system enable
```

```
end
```

locallog fortianalyzer (fortianalyzer2, fortianalyzer3) setting

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

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

Syntax

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

| Variable | Description |
|--|--|
| 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 unit. The following options are available: <ul style="list-style-type: none"> emergency: The unit is unusable. alert: Immediate action is required (default). 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. |
| server-ip <ip> | Set the remote FortiAnalyzer server IP address. |
| secure-connection {enable disable} | Enable/disable connection secured by TLS/SSL. |
| status {disable realtime upload} | Set the log to FortiAnalyzer status. The following options are available: <ul style="list-style-type: none"> disable: Do not log to FortiAnalyzer. realtime: Log to FortiAnalyzer in realtime. upload: Log to FortiAnalyzer at a scheduled time. Default: disable |
| upload-time <hh:mm> | Set the time to upload local log files. |

Example

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

```
config system locallog fortianalyzer setting
```

```
    set status enable
    set severity information
end
```

locallog memory setting

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

Syntax

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

| Variable | Description |
|--|--|
| diskfull {nolog overwrite} | Enter the action to take when the disk is full: <ul style="list-style-type: none">• nolog: Stop logging when disk full• overwrite: Overwrites oldest log entries |
| severity {emergency alert critical error warning notification information debug} | Enter the log severity level to log files. The following options are available: <ul style="list-style-type: none">• emergency: The unit is unusable.• alert: Immediate action is required (default).• 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 <disable enable> | Enable or disable logging to the memory buffer. Default: disable |

Example

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

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

locallog syslogd (syslogd2, syslogd3) setting

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

Syntax

```
config system locallog {syslogd | syslogd2 | syslogd3} setting
```

```

set 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 severity {emergency | alert | critical | error | warning | notification |
information | debug}
set status {enable | disable}
set syslog-name <string>
end

```

| Variable | Description |
|--|---|
| 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. Default: 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} | <p>Enter the facility type. <code>facility</code> identifies the source of the log message to syslog. Change <code>facility</code> to distinguish log messages from different FortiManager units so you can determine the source of the log messages. Available facility types are:</p> <ul style="list-style-type: none"> • <code>alert</code>: Log alert. • <code>audit</code>: Log audit. • <code>auth</code>: Security/authorization messages. • <code>authpriv</code>: Security/authorization messages (private). • <code>clock</code>: Clock daemon • <code>cron</code>: Clock daemon. • <code>daemon</code>: System daemons. • <code>ftp</code>: File Transfer Protocol (FTP) daemon • <code>kernel</code>: Kernel messages. • <code>local0 to local7</code>: reserved for local use (default) • <code>lpr</code>: Line printer subsystem. • <code>mail</code>: Mail system. • <code>news</code>: Network news subsystem. • <code>ntp</code>: Network Time Protocol (NTP) daemon • <code>syslog</code>: Messages generated internally by the syslog daemon. • <code>user</code>: Random user-level messages. • <code>uucp</code>: Network news subsystem. |

| Variable | Description |
|--|---|
| severity {emergency alert critical error warning notification information debug} | <p>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.</p> <p>The logging levels in descending order are:</p> <ul style="list-style-type: none"> <code>emergency</code>: The unit is unusable. <code>alert</code>: Immediate action is required. <code>critical</code>: Functionality is affected. <code>error</code>: Functionality is probably affected. <code>warning</code>: Functionality might be affected. <code>notification</code>: Information about normal events. <code>information</code>: General information about unit operations. <code>debug</code>: Information used for diagnosis or debugging. |
| status {enable disable} | Enable or disable logging to the remote syslog server. |
| syslog-name <string> | Enter the remote syslog server name. |

Example

In this example, the logs are uploaded to a syslog server at IPv4 address `10.10.10.8`. The FortiManager unit is identified as facility `local0`.

```
config system locallog syslogd setting
    set facility local0
    set status enable
    set severity information
end
```

log

Use the following commands to configure log settings.

log alert

Use this command to configure log based alert settings.

Syntax

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

| Variable | Description |
|---------------------------|--|
| max-alert-count <integer> | Maximum number of alerts supported. Range: 100 to 1000 |

log breach-detect

Use this command to configure log based breach-detect settings.

Syntax

```
config system log breach-detect
    set max-endpoints-per-adom
    set status
end
```

| Variable | Description |
|-------------------------------------|---|
| max-endpoints-per-adom <integer> | Maximum number of endpoints per adom. |
| status | Set the status of the breach detect settings. |

log mail-domain

Use this command to configure FortiMail domain settings.

Syntax

```
config system log mail-domain
    edit <id>
        set devices <string>
        set domain <string>
        set vdom <string>
    end
```

| Variable | Description |
|------------------|--|
| <id> | The ID of the FortiMail domain. |
| devices <string> | The device IDs seperated by commas, or All_FortiMails,for domain to VDOM mapping. For example: 'FEVM020000000000,FEVM020000000001' |
| domain <string> | The FortiMail domain. |
| vdom <string> | The VDOM name that is mapping to the FortiMail domain. |

log settings

Use this command to configure settings for logs.

Syntax

```
config system log settings
    set dns-resolve-dstip {disable | enable}
    set download-max-logs <integer>
    set FAC-custom-field1 <string>
```

```

set FCH-custom-field1 <string>
set FCT-custom-field1 <string>
set FDD-custom-field1 <string>
set FGT-custom-field1 <string>
set FML-custom-field1 <string>
set FMG-custom-field1 <string>
set FWB-custom-field1 <string>
set FAZ-custom-field1 <string>
set FSA-custom-field1 <string>
set ha-auto-migrate {disable | enable}
set import-max-logfiles <integer>
set log-file-archive-name {basic | extended}
set sync-search-timeout <integer>
config rolling-regular
    set days {fri | mon | sat | sun | thu | tue | wed}
    set del-files {disable | enable}
    set directory <string>
    set file-size <integer>
    set gzip-format {disable | enable}
    set hour <integer>
    set ip <ipv4_address>
    set ip2 <ipv4_address>
    set ip3 <ipv4_address>
    set log-format {csv | native | text}
    set min <integer>
    set password <passwd>
    set password2 <passwd>
    set password3 <passwd>
    set server-type {ftp | scp | sftp}
    set upload {disable | enable}
    set upload-hour <integer>
    set upload-mode {backup | mirror}
    set upload-trigger {on-roll | on-schedule}
    set username <string>
    set username2 <string>
    set username3 <string>
    set when {daily | none | weekly}
end
end

```

| Variable | Description |
|--------------------------------------|--|
| dns-resolve-dstip {disable enable} | Enabled/Disable resolving destination IP by DNS. Default: enabled. |
| download-max-logs <integer> | Maximum number of logs for each log download attempt. Default: 500000. |
| FAC-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FCH-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FCT-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FDD-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |

| Variable | Description |
|--|---|
| FGT-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FML-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FMG-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FWB-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FAZ-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| FSA-custom-field1 <string> | Enter a name of the custom log field to index. Character limit: 31 |
| ha-auto-migrate {disable enable} | Enabled/Disable automatically merging HA member's logs to HA cluster. Default: disabled. |
| import-max-logfiles <integer> | Maximum number of log files for each log import attempt. Default: 10000. |
| log-file-archive-name {basic extended} | Log file name format for archiving. <ul style="list-style-type: none"> basic: (Default) Basic format for log archive file name, for example: FGT20C0000000001.tlog.1417797247.log. extended: Extended format for log archive file name, for example: FGT20C0000000001.2014-12-05-08:34:58.tlog.1417797247.log. |
| sync-search-timeout <integer> | The maximum number of seconds that a log search session can run in synchronous mode. Default: 60 seconds. |
| Variables for <code>config rolling-regular</code> subcommand: | |
| days {fri mon sat sun thu tue wed} | Log files rolling schedule (days of the week). When <code>when</code> is set to <code>weekly</code> , you can configure <code>days</code> , <code>hour</code> , and <code>min</code> values. the following options are available: <ul style="list-style-type: none"> <code>fri</code>: Friday. <code>mon</code>: Monday. <code>sat</code>: Saturday. <code>sun</code>: Sunday. <code>thu</code>: Thursday. <code>tue</code>: Tuesday. <code>wed</code>: Wednesday. |
| del-files {disable enable} | Enable/disable log file deletion after uploading. |
| directory <string> | The upload server directory. Character limit: 127 |
| file-size <integer> | Roll log files when they reach this size (MB). Range: 10 to 500 (MB). Default: 200 (MB) |

| Variable | Description |
|---|---|
| gzip-format {disable enable} | Enable/disable compression of uploaded log files. |
| hour <integer> | Log files rolling schedule (hour). |
| ip <ipv4_address> ip2 <ipv4_address> ip3 <ipv4_address> | Upload server IPv4 addresses. Configure up to three servers. |
| log-format {csv native text} | Format of uploaded log files. The following options are available: <ul style="list-style-type: none"> <code>csv</code>: CSV (comma-separated value) format. <code>native</code>: Native format (text or compact). <code>text</code>: Text format (convert if necessary). |
| min <integer> | Log files rolling schedule (minutes). |
| password <passwd> password2 <passwd> password3 <passwd> | Upload server login passwords. Character limit: 128 |
| server-type {ftp scp sftp} | Upload server type: <code>ftp</code> , <code>scp</code> , or <code>sftp</code> . |
| upload {disable enable} | Enable/disable log file uploads. |
| upload-hour <integer> | Log files upload schedule (hour). |
| upload-mode {backup mirror} | Configure upload mode with multiple servers. Servers are attempted and used one after the other upon failure to connect. The following options are available: <ul style="list-style-type: none"> <code>backup</code>: Servers are attempted and used one after the other upon failure to connect. <code>mirror</code>: All configured servers are attempted and used. |
| upload-trigger {on-roll on-schedule} | Event triggering log files upload: <ul style="list-style-type: none"> <code>on-roll</code>: Upload log files after they are rolled. <code>on-schedule</code>: Upload log files daily. |
| username <string> username2 <string> username3 <string> | Upload server login usernames. Character limit: 35 |
| when {daily none weekly} | Roll log files periodically. The following options are available: <ul style="list-style-type: none"> <code>daily</code>: Roll log files daily. <code>none</code>: Do not roll log files periodically. <code>weekly</code>: Roll log files on certain days of week. |

log-fetch

Use the following commands to configure log fetching.

log-fetch client-profile

Use this command to configure the fetching client settings.

Syntax

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

| Variable | Description |
|--------------------------------|---|
| id | The log-fetch client profile ID. |
| client-adom | Set the client ADOM. |
| data-range {custom} | The data range settings for the fetched logs, which is always custom. |
| data-range-value <integer> | An integer representing the data range value. |
| end-time <hh:mm> <yyyy/m-m/dd> | Set the end date and time of the data-range. |

| Variable | Description |
|--|--|
| index-fetch-logs {enable disable} | Enable/disable indexing logs automatically after fetching logs. Default: enabled. |
| log-filter-status {enable disable} | Enable/Disable log-filter. Default: disabled. |
| log-filter-logic {and or} | Set the logic for the log filters. |
| name <string> | The name of log-fetch client profile. |
| password <passwd> | The log-fetch server password. |
| secure-connection {enable disable} | Enable/disable protecting log-fetch connection with TLS/SSL. Default: enabled. |
| server-adom | Set the server ADOM. |
| server-ip <ip> | The log fetch server IPv4 address. |
| start-time <hh:mm> <yyyy/mm/dd> | Set the start date and time of the data-range. The start date should be earlier than the end date. |
| sync-adom-config | Synchronize the ADOM configuration. |
| user <string> | The log-fetch server username. |
| Variables for <code>config device-filter</code> subcommand: | |
| <id> | Add or edit a device filter. |
| adom <string> | Enter the ADOM name. |
| device <device> | Enter the device name or serial number. |
| vdom <string> | Enter the VDOM, if required. |
| Variables for <code>config log-filter</code> subcommand: | |
| <id> | The log filter ID. |
| field <string> | Enter the field name. |

| Variable | Description |
|---|--|
| oper {= != < > <= >= contain not-contain match} | Set the filter operator: <ul style="list-style-type: none"> • = - Equal to • != - Not equal to • < - Less than • > - Greater than • <= - Less than or equal to • >= - Greater than or equal to • contain - Contain • not-contain - Not contain • match - Match (expression) |
| value <string> | Enter the field filter operand or free-text matching expression. |

log-fetch server-setting

Use this command to configure the fetching server settings.

Syntax

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

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

mail

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

Syntax

```
config system mail
    edit <id>
        set auth {enable | disable}
        set passwd <passwd>
        set port <integer>
        set secure-option {default | none | smtps | starttls}
```

```

    set server <string>
    set user <string>
end

```

| Variable | Description |
|---|--|
| <id> | Enter the mail service ID of the entry you would like to edit or type a new name to create an entry. Character limit: 63 |
| <server> | Enter the name of the mail server. |
| auth {enable disable} | Enable/disable authentication. |
| passwd <passwd> | Enter the SMTP account password value. Character limit: 63 |
| port <integer> | Enter the SMTP server port. Range: 1 to 65535 |
| secure-option {default none smtps starttls} | Select the communication secure option. One of: <ul style="list-style-type: none"> • default: Try STARTTLS, proceed as plain text communication otherwise. • none: Communication will be in plain text format. • smtps: Communication will be protected by SMTPS. • starttls: Communication will be protected by STARTTLS. |
| server <string> | Enter the SMTP server name. |
| user <string> | Enter the SMTP account user name. |

metadata

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



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

Syntax

```

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

```

| Variable | Description |
|------------------------------|--|
| <fieldname> | Enter the name of the field. |
| field_length {20 50 255} | Select the maximum number of characters allowed in this field. Default: 50 |

| Variable | Description |
|----------------------------------|---|
| importance {optional required} | Select if this field is required or optional when entering standard information. Default: <code>optional</code> |
| status {enabled disabled} | Enable/disable the metadata. Default: <code>disable</code> |

ntp

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

Syntax

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

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

password-policy

Use this command to configure access password policies.

Syntax

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

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

report

Use the following command to configure report related settings.

report auto-cache

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

Syntax

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

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

report est-browse-time

Use this command to view or configure report settings.

Syntax

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

| Variable | Description |
|---------------------------|--|
| max-read-time <integer> | Set the read time threshold for each page view. Range: 1 to 3600 |
| status {enable disable} | Enable/disable estimating browse time. |

report group

Use these commands to configure report groups.

Syntax

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

| Variable | Description |
|--|---|
| <group-id> | The identification number of the group to be edited or created. |
| adom <adom-name> | The ADOM that contains the report group. |
| case-insensitive {enable disable} | Enable or disable case sensitivity. |
| report-like <string> | Report pattern |
| Variables for <code>config chart-alternative</code> subcommand: | |
| <chart-name> | The chart name. |
| chart-replace <string> | Chart replacement. |
| Variables for <code>config group-by</code> subcommand: | |
| <var-name> | The variable name. |
| var-expression <string> | Variable expression. |
| var-type | Variable type. |

report setting

Use these commands to view or configure report settings.

Syntax

```

config system report setting
    set aggregate-report {enable | disable}
    set hcache-lossless {enable | disable}
    set ldap-cache-timeout <integer>
    set max-table-rows <integer>
    set report-priority {low | normal}
    set week-start {mon | sun}
end

```

| Variable | Description |
|-------------------------------------|--|
| aggregate-report {enable disable} | Enable/disable including a group report along with the per-device reports. |
| hcache-lossless {enable disable} | Enable or disable ready-with-loss hcache. |
| ldap-cache-timeout <integer> | Set the LDAP cache timeout in minutes. Set to 0 to not use the cache. Default: 60. |

| Variable | Description |
|--------------------------------|---|
| max-table-rows <integer> | Set the maximum number of rows that can be generated in a single table. Range: 10 000 to 100 000 |
| report-priority {low normal} | Set the Priority of the SQL report. |
| week-start {mon sun} | Set the day that the week starts on, either Sunday or Monday. The following options are available: <ul style="list-style-type: none"> mon: Monday. sun: Sunday. |

Use the `show` command to display the current configuration if it has been changed from its default value:

```
show system report settings
```

route

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

Syntax

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

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

route6

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

Syntax

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

```

    set gateway <ipv6_address>
end

```

| Variable | Description |
|------------------------|---|
| <seq_int> | Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route. |
| device <string> | Enter the port (interface) used for this route. |
| dst <ipv6_prefix> | Enter the IPv4 address and mask for the destination network. |
| gateway <ipv6_address> | Enter the default gateway IPv6 address for this network. |

snmp

Use the following commands to configure SNMP related settings.

snmp community

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

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

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

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

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



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

Syntax

```

config system snmp community
  edit <index_number>
    set events <events_list>
    set name <community_name>
    set query-v1-port <integer>
    set query-v1-status {enable | disable}
    set query-v2c-port <integer>
    set query-v2c-status {enable | disable}
    set status {enable | disable}
    set trap-v1-rport <integer>
  end
end

```

```

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

```

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

| Variable | Description |
|---|--|
| query-v2c-port <integer> | Enter the SNMP v2c query port number used when SNMP managers query the FortiManager unit. SNMP v2c queries will include the name of the community. Default: 161. Range: 1 to 65535 |
| query-v2c-status {enable disable} | Enable/disable SNMPv2c queries for this SNMP community. Default: enable |
| status {enable disable} | Enable/disable this SNMP community. Default: enable |
| trap-v1-rport <integer> | Enter the SNMPv1 remote port number used for sending traps to the SNMP managers. Default: 162. Range: 1 to 65535 |
| trap-v1-status {enable disable} | Enable/disable SNMPv1 traps for this SNMP community. Default: enable |
| trap-v2c-rport <integer> | Enter the SNMPv2c remote port number used for sending traps to the SNMP managers. Default: 162. Range: 1 to 65535 |
| trap-v2c-status {enable disable} | Enable/disable SNMPv2c traps for this SNMP community. SNMP v2c traps sent out to SNMP managers include the community name. Default: enable |
| Variables for <code>config hosts</code> subcommand: | |
| <host_number> | Enter the index number of the host in the table. Enter an unused index number to create a new host. |
| interface <interface_name> | Enter the name of the FortiManager unit that connects to the SNMP manager. |
| ip <ipv4_address> | Enter the IPv4 address of the SNMP manager. Default: 0.0.0.0 |
| Variables for <code>config hosts6</code> subcommand: | |
| <host_number> | Enter the index number of the host in the table. Enter an unused index number to create a new host. |
| interface <interface_name> | Enter the name of the FortiManager unit that connects to the SNMP manager. |
| ip <ipv6_address> | Enter the IPv6 address of the SNMP manager. |

Example

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

```
config system snmp community
edit 1
```

```

set name SNMP_Com1
set query-v2c-status disable
set trap-v2c-status disable
  config hosts
    edit 1
      set interface internal
      set ip 192.168.10.34
    end
  end
end

```

snmp sysinfo

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

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

Syntax

```

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

```

| Variable | Description |
|---|--|
| contact-info <string> | Add the contact information for the person responsible for this FortiManager unit. Character limit: 35 |
| description <description> | Add a name or description of the FortiManager unit. Character limit: 35 |
| engine-id <string> | Local SNMP engine ID string. Character limit: 24 |
| location <location> | Describe the physical location of the FortiManager unit. Character limit: 35 |
| status {enable disable} | Enable/disable the FortiManager SNMP agent. Default: <code>disable</code> |
| trap-high-cpu-threshold <percentage> | CPU usage when trap is set. Default: 80 |
| trap-low-memory-threshold <percentage> | Memory usage when trap is set. Default: 80 |
| trap-cpu-high-exclude-nice-threshold <percentage> | CPU high usage excludes nice when the trap is sent. |

Example

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

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

snmp user

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

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

Syntax

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

| Variable | Description |
|------------------------|---|
| <name> | Enter a SNMPv3 user name to add, edit, or delete. |
| auth-proto {md5 sha} | Authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. The following options are available: <ul style="list-style-type: none"><code>md5</code>: HMAC-MD5-96 authentication protocol<code>sha</code>: HMAC-SHA-96 authentication protocol |
| auth-pwd <passwd> | Password for the authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. |

| Variable | Description |
|---|--|
| events <events_list> | <p>Enable the events for which the FortiManager unit should send traps to the SNMPv3 managers in this community. The <code>raid_changed</code> event is only available for devices which support RAID.</p> <ul style="list-style-type: none"> <code>cpu-high-exclude-nice</code>: CPU usage exclude nice threshold. <code>cpu_high</code>: The CPU usage is too high. <code>disk_low</code>: The log disk is getting close to being full. <code>ha_switch</code>: A new unit has become the HA master. <code>intf_ip_chg</code>: An interface IP address has changed. <code>lic-dev-quota</code>: High licensed device quota detected. <code>lic-gbday</code>: High licensed log GB/Day detected. <code>log-alert</code>: Log base alert message. <code>log-data-rate</code>: High incoming log data rate detected. <code>log-rate</code>: High incoming log rate detected. <code>mem_low</code>: The available memory is low. <code>raid_changed</code>: RAID status changed. <code>sys_reboot</code>: The FortiManager unit has rebooted. <p>Default: All events enabled.</p> |
| notify-hosts <ipv4_address> | Hosts to send notifications (traps) to. |
| notify-hosts6 <ipv6_address> | Hosts to send notifications (traps) to. |
| priv-proto {aes des} | <p>Privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. The following options are available:</p> <ul style="list-style-type: none"> <code>aes</code>: CFB128-AES-128 symmetric encryption protocol <code>des</code>: CBC-DES symmetric encryption protocol |
| priv-pwd <passwd> | Password for the privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. |
| queries {enable disable} | Enable/disable queries for this user. Default: <code>enable</code> |
| query-port <integer> | SNMPv3 query port. Default: 161. Range: 1 to 65535 |
| security-level {auth-no-priv auth-priv no-auth-no-priv} | <p>Security level for message authentication and encryption. The following options are available:</p> <ul style="list-style-type: none"> <code>auth-no-priv</code>: Message with authentication but no privacy (encryption). <code>auth-priv</code>: Message with authentication and privacy (encryption). <code>no-auth-no-priv</code>: Message with no authentication and no privacy (encryption) (default). |

sql

Configure Structured Query Language (SQL) settings.

Syntax

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

| Variable | Description |
|---------------------------------------|--|
| background-rebuild {enable disable} | Disable or enable rebuilding the SQL database in the background. |
| database-name <string> | Database name. Command only available when <code>status</code> is set to <code>remote</code> . |
| database-type <postgres> | Database type. Command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> . |

| Variable | Description |
|---|---|
| device-count-high {enable disable} | <p>You must set to enable if the count of registered devices is greater than 8000. The following options are available:</p> <ul style="list-style-type: none"> <code>disable</code>: Set to disable if device count is less than 8000. <code>enable</code>: Set to enable if device count is equal to or greater than 8000. <p>Caution: Enabling or disabling this command will result in an SQL database rebuild. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. This operation will also result in a device reboot.</p> |
| event-table-partition-time <integer> | Maximum SQL database table partitioning time range, in minutes, for event logs. 0 to 525600 (minutes), or Enter 0 for unlimited. |
| fct-table-partition-time <integer> | Maximum SQL database table partitioning time range, in minute, for FortiClient logs. 0 to 525600 (minutes), or Enter 0 for unlimited. |
| logtype {none app-ctrl attack content dlp emailfilter event generic history traffic virus voip webfilter netscan} | Log type. Command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> . |
| password <passwd> | The password that the Fortinet unit will use to authenticate with the remote database. Command only available when <code>status</code> is set to <code>remote</code> . |
| prompt-sql-upgrade {enable disable} | Prompt to convert log database into SQL database at start time on GUI. |
| rebuild-event {enable disable} | Enable/disable a rebuild event during SQL database rebuilding. |
| rebuild-event-start-time <hh:mm> <yyyy/mm/dd> | The rebuild event starting date and time. |
| server <string> | Set the database ip or hostname. |
| start-time <hh>:<mm> <yyyy>/<mm>/<dd> | Start date and time <hh:mm yyyy/mm/dd>. Command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> . |
| status {disable local remote} | <p>SQL database status. The following options are available:</p> <ul style="list-style-type: none"> <code>disable</code>: Disable SQL database. <code>local</code>: Enable local database. <code>remote</code>: Enable remote database. |
| text-search-index {disable enable} | Disable or enable the creation of a text search index. |
| traffic-table-partition-time <integer> | Maximum SQL database table partitioning time range for traffic logs. Range: 0 to 525 600 (minutes) enter 0 for unlimited |

| Variable | Description |
|---|---|
| utm-table-partition-time <integer> | Maximum SQL database table partitioning time range in minutes for UTM logs. Range: 0 to 525600 (minutes). Enter 0 for unlimited |
| username <string> | User name for login remote database. |
| Variables for <code>config custom-index</code> subcommand: | |
| device-type {FortiCache FortiGate FortiMail FortiManager FortiSandbox FortiWeb} | Set the device type. The following options are available: <ul style="list-style-type: none"> • <code>FortiCache</code>: Set device type to FortiCache • <code>FortiGate</code>: Set device type to FortiGate. • <code>FortiMail</code>: Set device type to FortiMail. • <code>FortiManager</code>: Set device type to FortiManager. • <code>FortiSandbox</code>: Set device type to FortiSandbox • <code>FortiWeb</code>: Set device type to FortiWeb. |
| index-field <Field-Name> | Enter a valid field name. Select one of the available field names. The available options for <code>index-field</code> is dependent on the <code>device-type</code> entry. |
| log-type <Log-Enter> | Enter the log type. The available options for <code>log-type</code> is dependent on the <code>device-type</code> entry. Enter one of the available log types. <ul style="list-style-type: none"> • <code>FortiCache</code>: N/A • <code>FortiGate</code>: app-ctrl, content, dlp, emailfilter, event, netscan, traffic, virus, voip, webfilter • <code>FortiMail</code>: emailfilter, event, history, virus • <code>FortiManager</code>: N/A • <code>FortiSandbox</code>: N/A • <code>FortiWeb</code>: attack, event, traffic |

| Variable | Description |
|---|---|
| Variables for <code>config ts-index-field</code> subcommand: | |
| <category> | <p>Category of the text search index fields. The following is the list of categories and their default fields. The following options are available:</p> <ul style="list-style-type: none"> FGT-app-ctrl: user, group, srcip, dstip, dstport, service, app, action, status, hostname FGT-attack: severity, srcip, proto, user, attackname FGT-content: from, to, subject, action, srcip, dstip, hostname, status FGT-dlp: user, srcip, service, action, file FGT-emailfilter: user, srcip, from, to, subject FGT-event: subtype, ui, action, msg FGT-traffic: user, srcip, dstip, service, app, utmaction, utmevent FGT-virus: service, srcip, file, virus, user FGT-voip: action, user, src, dst, from, to FGT-webfilter: user, srcip, status, catdesc FGT-netscan: user, dstip, vuln, severity, os FGT-fct-event FGT-fct-traffic FGT-fct-netscan FML-emailfilter: client_name, dst_ip, from, to, subject FML-event: subtype, msg FML-history: classifier, disposition, from, to, client_name, direction, domain, virus FML-virus: src, msg, from, to FWB-attack: http_host, http_url, src, dst, msg, action FWB-event: ui, action, msg FWB-traffic: src, dst, service, http_method, msg |
| <value> | Fields of the text search filter. |
| <string> | Select one or more field names separated with a comma. The available field names is dependent on the category selected. |

syslog

Use this command to configure syslog servers.

Syntax

```
config system syslog
```

```

    edit <name>
        set ip <string>
        set port <integer>
    end
end

```

| Variable | Description |
|----------------|---|
| ip <string> | Enter the syslog server IPv4 address or hostname. |
| port <integer> | Enter the syslog server port. Range: 1 to 65535 |

workflow approval-matrix

Use this command to configure workflow settings.

Syntax

```

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

```

| Variable | Description |
|--|---|
| mail-server <string> | Enter the mail server IPv4 address or hostname. |
| notify <string> | Enter the notified users. Use a comma as a separator. |
| Variables for config approver subcommand: | |
| <sequence_number> | Enter the entry number. |
| member <string> | Enter the member of the approval group. Use a comma as a separator. |

fmupdate

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



CLI commands and variables are case sensitive.

| | | |
|-----------------------------------|---------------------------------------|-------------------------------------|
| <code>analyzer virusreport</code> | <code>fct-services</code> | <code>server-override-status</code> |
| <code>av-ips</code> | <code>fds-setting</code> | <code>service</code> |
| <code>custom-url-list</code> | <code>multilayer</code> | <code>support-pre-fgt43</code> |
| <code>device-version</code> | <code>publicnetwork</code> | <code>web-spam</code> |
| <code>disk-quota</code> | <code>server-access-priorities</code> | |

analyzer virusreport

Use this command to Enable/disable notification of virus detection to FortiGuard.

Syntax

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

| Variable | Description |
|--|---|
| <code>status {enable disable}</code> | Enable/disable sending virus detection notification to FortiGuard. Default: <code>enable</code> |

Example

This example enables virus detection notifications to FortiGuard.

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

av-ips

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

av-ips advanced-log

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

Syntax

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

| Variable | Description |
|----------------------------------|--|
| log-fortigate {enable disable} | Enable/disable logging of FortiGuard antivirus and IPS service updates of FortiGate devices. Default: <code>disable</code> |
| log-server {enable disable} | Enable/disable logging of update packages received by the built-in FDS server. Default: <code>disable</code> |

Example

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

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

av-ips fct server-override

Use this command to override the default IPv4 or IPv6 address and port that the built-in FDS contacts when requesting FortiGuard antivirus updates for FortiClient from the FDS.

Syntax

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

| Variable | Description |
|---|--|
| status {enable disable} | Enable/disable the override. Default: <code>disable</code> |
| Variables for <code>config servlist</code> subcommand: | |
| <id> | Override server ID (1-10). |

| Variable | Description |
|--------------------|--|
| ip <ipv4_address> | Enter the IPv4 address of the override server. Default: 0.0.0.0 |
| ip6 <ipv6_address> | Enter the IPv6 address of the override server. |
| port <integer> | Enter the port number to use when contacting the FDS. Default: 443. Range: 1 to 65535 |

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 FDS.

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

av-ips fgt server-override

Use this command to override the default IPv4 or IPv6 address and port that the built-in FDS contacts when requesting FortiGuard antivirus and IPS updates for FortiGate units from the FDS.

Syntax

```
config fmupdate av-ips fgt server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <ipv4_address>
      set ip6 <ipv6_address>
      set port <integer>
    end
  end
```

| Variable | Description |
|---|--|
| status {enable disable} | Enable/disable the override. Default: disable |
| Variable for config servlist subcommand: | |
| <id> | Override server ID (1-10). |
| ip <ipv4_address> | Enter the IPv4 address of the override server. Default: 0.0.0.0 |
| ip6 <ipv6_address> | Enter the IPv6 address of the override server. |
| port <integer> | Enter the port number to use when contacting the FDS. Default: 443. Range: 1 to 65535 |

Example

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

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

av-ips push-override

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

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

Syntax

```
config fmupdate av-ips push-override
  set ip <ipv4_address>
  set ip6 <ipv6_address>
  set port <integer>
  set status {enable | disable}
end
```

| Variable | Description |
|---------------------------|---|
| ip <ipv4_address> | Enter the external or virtual IPv4 address of the NAT device that will forward push messages to the FortiManager unit. Default: 0 . 0 . 0 . 0 |
| ip6 <ipv6_address> | Enter the external or virtual IPv6 address of the NAT device that will forward push messages to the FortiManager unit. |
| port <integer> | Enter the receiving port number on the NAT device. Default: 9443. Range: 1 to 65535 |
| status {enable disable} | Enable/disable the push updates. Default: <i>disable</i> |

Example

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

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

```
config fmupdate 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 User Datagram Protocol (UDP) port 9000 to the FortiManager unit on UDP port 9443.

av-ips push-override-to-client

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

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

Syntax

```
config fmupdate av-ips push-override-to-client
  set status {enable | disable}
  config <announce-ip>
    edit <id>
      set ip <ipv4_address>
      set ip6 <ipv6_address>
      set port <integer>
    end
  end
end
```

| Variable | Description |
|---|--|
| status {enable disable} | Enable/disable the push updates. Default: disable |
| <announce-ip> | Configure the IP address information of the device. |
| Variables for config announce-ip subcommand: | |
| <id> | Edit the announce IP address ID. |
| ip <ipv4_address> | Enter the announce IPv4 address. Default: 0.0.0.0 |
| ip6 <ipv6_address> | Enter the announce IPv6 address. |
| port <integer> | Enter the announce IP port. Default: 9443. Range: 1 to 65535 |

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
```

| Variable | Description |
|--|--|
| 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 <code>frequency</code> is <code>weekly</code> . |
| frequency {every daily weekly} | Enter to configure the frequency of the updates. The following options are available: <ul style="list-style-type: none"> <code>every</code>: Time interval (default) <code>daily</code>: Every day <code>weekly</code>: Every week |
| status {enable disable} | Enable/disable regularly scheduled updates. Default: <code>enable</code> |
| 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 <code>18:00</code> . The time period format is the 24-hour clock: hh=0-23, mm=0-59. If the minute is <code>60</code> , the updates will begin at a random minute within the hour. If the <code>frequency</code> is <code>every</code> , the time is interpreted as an hour and minute interval, rather than a time of day. Default: <code>01:60</code> |

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
```

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 <ipv4_address>
  set ip6 <ipv6_address>
  set mode {proxy | tunnel}
  set password <passwd>
  set port <integer>
  set status {enable | disable}
  set username <string>
end
```

| Variable | Description |
|---------------------------|--|
| ip <ipv4_address> | Enter the IPv4 address of the web proxy. Default: 0.0.0.0 |
| ip6 <ipv6_address> | Enter the IPv6 address of the web proxy. |
| mode {proxy tunnel} | Enter the web proxy mode. The following options are available: <ul style="list-style-type: none">• proxy: HTTP proxy.• tunnel: HTTP tunnel. |
| password <passwd> | If the web proxy requires authentication, enter the password for the user name. Character limit: 63 |
| port <integer> | Enter the port number of the web proxy. Default: 80. Range: 1 to 65535 |
| status {enable disable} | Enable/disable connections through the web proxy. Default: disable |
| username <string> | If the web proxy requires authentication, enter the user name. Character limit: 63 |

Example

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

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

custom-url-list

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

Syntax

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

| Variable | Description |
|--|---|
| db_selection {both custom-url fortiguard-db} | Manage the FortiGuard URL database. The following options are available: <ul style="list-style-type: none"> <code>both</code>: Support both custom URL database and the FortiGuard database <code>custom-url</code>: Customer imported URL list. <code>fortiguard-db</code>: Fortinet's FortiGuard database Default setting: <code>both</code> |

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 megabytes (MB). The default size is 10 gigabytes (GB). If you set the disk-quota smaller than the size of an update package, the update package will not download and you will get a disk full alert.

fct-services

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

Syntax

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

| Variable | Description |
|---------------------------|---|
| status {enable disable} | Enable/disable built-in FDS service to FortiClient installations. Default: <code>enable</code> |
| port <integer> | Enter the port number on which the built-in FDS should provide updates to FortiClient installations. Default: <code>80</code> . Range: 1 to 65535 |

Example

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

```
config fmupdate fct-services
```

```

    set status enable
    set port 80
end

```

fds-setting

Use this command to set FDS settings.

Syntax

```

config fmupdate fds-settings
    set fds-pull-interval <integer>
    set fds-ssl-protocol
    set linkd-log {alert | critical | debug | disable | emergency | error | info |
        notice | warn}
    set max-av-ips-version <integer>
    set max-work <integer>
    set system-support-faz {4.x | 5.0 | 5.2 | 5.4}
    set system-support-fct {4.x | 5.0 | 5.2 | 5.4}
    set system-support-fgt {4.x | 5.0 | 5.2 | 5.4}
    set system-support-fml {4.x | 5.0 | 5.2 | 5.4}
    set system-support-fsa {1.x | 2.x}
    set system-support-fsw {4.x | 5.0 | 5.2 | 5.4}
    set umsvc-log {alert | critical | debug | disable | emergency | error | info |
        notice | warn}
    set unreg-dev-option {add-service | ignore | svc-only}
    set User-Agent <text>
end

```

| Variable | Description |
|--|---|
| <code>fds-pull-interval <integer></code> | Time interval FortiManager may pull updates from FDS. Range: 1 to 120 (minutes). Default: 10. |
| <code>set fds-ssl-protocol {sslsv3 tlsv1.0 tlsv1.1 tlsv1.2}</code> | Set the SSL protocols version for FDS service. Default: <code>tlsv1.0</code> . |
| <code>linkd-log {alert critical debug disable emergency error info notice warn}</code> | The linkd log level. Default: <code>info</code> . |
| <code>max-av-ips-version <integer></code> | The maximum number of AV/IPS full version downloadable packages. Range: 1 to 1000. Default: 20. |
| <code>max-work <integer></code> | The maximum number of worker processing downlink requests. Range: 1 to 32. Default: 1. |
| <code>system-support-faz {4.x 5.0 5.2 5.4}</code> | Set the FortiAnalyzer support version. |

| Variable | Description |
|---|--|
| system-support-fct {4.x 5.0 5.2 5.4} | Set the FortiClient support version. |
| system-support-fgt {4.x 5.0 5.2 5.4} | Set the FortiGate support version. |
| system-support-fml {4.x 5.0 5.2 5.4} | Set the FortiMail support version. |
| system-support-fsa {1.x 2.x} | Set the FortiSandbox support version. |
| system-support-fsw {4.x 5.0 5.2 5.4} | Set the FortiSwitch support version. |
| umsvc-log {alert critical debug disable emergency error info notice warn} | The um_service log level. Default: <code>info</code> . |
| unreg-dev-option {add-service ignore svc-only} | Set the option for unregistered devices: <ul style="list-style-type: none"> <code>add-service</code>: Add unregistered devices and allow update request (default). <code>ignore</code>: Ignore all unregistered devices. <code>svc-only</code>: Allow update request without add unregistered device. |
| User-Agent <text> | Configure the User-Agent string. |

multilayer

Use this command to set multilayer mode configuration.

Syntax

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

| Variable | Description |
|-----------------------------------|---|
| webspam-rating {disable enable} | URL/Antispam rating service. Default: <code>enable</code> |

publicnetwork

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

Syntax

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

| Variable | Description |
|---------------------------|---|
| status {disable enable} | Enable/disable the public network. Default: <i>enable</i> |

Example

The following example shows how to enable public network.

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

server-access-priorities

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

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



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

Syntax

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

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

| Variable | Description |
|---|--|
| Variables for <code>config private-server</code> subcommand: | |
| <id> | Enter a number to identify the FortiManager unit or private server. Range: 1 to 10 |
| ip <ipv4_address> | Enter the IPv4 address of the FortiManager unit or private server. |
| ip6 <ipv6_address> | Enter the IPv6 address of the FortiManager unit or private server. |
| time_zone <integer> | Enter the correct time zone of the private server. Using -24 indicates that the server is using the local time zone. |

Example

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

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

server-override-status

Syntax

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

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

service

Use this command to Enable/disable the services provided by the built-in FDS.

Syntax

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

| Variable | Description |
|--|--|
| avips {enable disable} | Enable/disable the built-in FDS to provide FortiGuard antivirus and IPS updates. Default: <code>disable</code> |
| query-antispam {disable enable} | Enable/disable antispam service. |
| query-antivirus {disable enable} | Enable/disable antivirus service. |
| query-filequery {disable enable} | Enable/disable file query service. |
| query-webfilter {disable enable} | Enable/disable web filter service. |
| webfilter-https-traversal {disable enable} | Enable/disable Web Filter HTTPS traversal. |

Example

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

web-spam

Use the following commands to configure FortiGuard antispam related settings.

web-spam fct server-override

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

Syntax

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

| Variable | Description |
|---|--|
| status {enable disable} | Enable/disable the override. Default: disable |
| Variable for config servlist subcommand: | |
| <id> | Override server ID. Range: 1 to 10 |
| ip <ipv4_address> | Enter the IPv4 address of the override server. Default: 0.0.0.0 |
| ip6 <ipv6_address> | Enter the IPv6 address of the override server. |
| port <integer> | Enter the port number to use when contacting the FDS. Default: 443. Range: 1 to 65535 |

web-spam fgd-log

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

Syntax

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

| Variable | Description |
|----------------------------------|---|
| spamlog {all disable nospam} | Configure the anti spam log settings. The following options are available: <ul style="list-style-type: none"> all: Log all Spam lookups disable: Disable Spam log nospam: Log Non-spam events. |
| status {disable enable} | Enable/disable the FortiGuard server event log status. |
| urllog {all disable miss} | Configure the web filter log setting. The following options are available: <ul style="list-style-type: none"> all: Log all URL lookups disable: Disable URL log miss: Log URL rating misses. |

web-spam fgd-setting

Use this command to configure FortiGuard run parameters.

Syntax

```
config fmupdate web-spam fgd-setting
  set as-cache <integer>
  set as-log {all | disable | nospam}
  set as-preload {disable | enable}
  set av-cache <integer>
  set av-log {all | disable | novirus}
  set av-preload {disable | enable}
  set eventlog-query {disable | enable}
  set fq-cache <integer>
  set fq-log {all | disable | nofilequery}
  set fq-preload {disable | enable}
  set linkd-log {disable | enable}
  set max-log-quota <integer>
  set max-unrated-size <integer>
  set restrict-as1-dbver <string>
  set restrict-as2-dbver <string>
  set restrict-as4-dbver <string>
  set restrict-av-dbver <string>
  set restrict-fq-dbver <string>
  set restrict-wf-dbver <string>
  set stat-log-interval <integer>
  set stat-sync-interval <integer>
  set update-interval <integer>
  set update-log {disable | enable}
  set wf-cache <integer>
  set wf-log {all | disable | nourel}
  set wf-preload {disable | enable}
end
```

| Variable | Description |
|---------------------------------|---|
| as-cache <integer> | Set the antispam service maximum memory usage. Range: 100 to 2800 (MB) |
| as-log {all disable nospam} | Antispam log setting. The following options are available: <ul style="list-style-type: none"> all: Log all spam lookups. disable: Disable spam log. nospam: Log non-spam events. |
| as-preload {disable enable} | Enable/disable preloading the antispam database into memory. |
| av-cache <integer> | Set the web filter service maximum memory usage. Range: 100 to 500 (MB) |

| Variable | Description |
|--------------------------------------|--|
| av-log {all disable novirus} | Antivirus log settings. The following options are available: <ul style="list-style-type: none"> all: Log all virus lookups. disable: Disable virus log. novirus: Log non-virus events. |
| av-preload {disable enable} | Enable/disable preloading the antivirus database into memory. |
| eventlog-query {disable enable} | Enable or disable record query to event-log besides fgd-log. |
| fq-cache <integer> | Set the file query service maximum memory usage. Range: 100 to 500MB |
| fq-log {all disable nofilequery} | Filequery log settings. The following options are available: <ul style="list-style-type: none"> all: Log all file query. disable: Disable file query log. nofilequery: Log non-file query events. |
| fq-preload {disable enable} | Enable/disable preloading the filequery database to memory. |
| linkd-log {disable enable} | Enable/disable the linkd log. |
| max-log-quota <integer> | Maximum log quota setting. Range: 100 to 20480MB |
| max-unrated-size <integer> | Maximum number of unrated site in memory. Range: 10 to 5120K Default: 500K |
| restrict-as1-dbver <string> | Restrict the system update to the indicated antispam(1) database version. Character limit: 127 |
| restrict-as2-dbver <string> | Restrict the system update to the indicated antispam(2) database version. Character limit: 127 |
| restrict-as4-dbver <string> | Restrict the system update to the indicated antispam(4) database version. Character limit: 127 |
| restrict-av-dbver <string> | Restrict the system update to the indicated antivirus database version. Character limit: 127 |
| restrict-fq-dbver <string> | Restrict the system update to the indicated filequery database version. Character limit: 127 |
| restrict-wf-dbver <string> | Restrict the system update to the indicated webfilter database version. Character limit: 127 |
| stat-log-interval <integer> | Statistic log interval setting. Range: 1 to 1440 (minutes) |
| stat-sync-interval <integer> | Synchronization interval for statistics of unrated sites. Range: 1 to 60 (minutes) |

| Variable | Description |
|--------------------------------|---|
| update-interval <integer> | Enter the FortiGuard database update wait time if there are not enough delta files. Range: 2 to 24 (hours) |
| update-log {disable enable} | Enable/disable update log setting. |
| wf-cache <integer> | Enter the web filter service maximum memory usage. Range: 100 to 2800 (MB) |
| wf-log {all disable nouri} | Web filter log setting. The following options are available: <ul style="list-style-type: none"> all: Log all URL lookups. disable: Disable URL log. nouri: Log non-URL events. |
| wf-preload {disable enable} | Enable/disable preloading the web filter database into memory. |

web-spam fgt server-override

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

Syntax

```
config fmupdate web-spam fgt server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <ipv4_address>
      set ip6 <ipv6_address>
      set port <integer>
    end
  end
```

| Variable | Description |
|---|---|
| status {enable disable} | Enable/disable the override. Default: disable |
| Variable for config servlist subcommand: | |
| <id> | Enter the override server ID. Range: 1 to 10 |
| ip <ipv4_address> | Enter the IPv4 address of the override server address. Default: 0.0.0.0 |
| ip6 <ipv6_address> | Enter the IPv6 address of the override server address. |
| port <integer> | Enter the port number to use when contacting the FDS. Default: 443. Range: 1 to 65535 |

web-spam fsa server-override

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

Syntax

```
config fmupdate web-spam fsa server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <ipv4_address>
      set ip6 <ipv6_address>
      set port <integer>
    end
  end
end
```

| Variable | Description |
|---|--|
| status {enable disable} | Enable/disable the override. Default: disable |
| Variable for config servlist subcommand: | |
| <id> | Override server ID. Range: 1 to 10 |
| ip <ipv4_address> | Enter the IPv4 address of the override server. Default: 0.0.0.0 |
| ip6 <ipv6_address> | Enter the IPv6 address of the override server. |
| port <integer> | Enter the port number to use when contacting the FDS. Default: 443. Range: 1 to 65535 |

web-spam poll-frequency

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

Syntax

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

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

web-spam web-proxy

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

Syntax

```
config fmupdate web-spam web-proxy
  set time <hh:mm>
```

```

    set ip <proxy_ipv4_address>
    set ip6 <proxy_ipv6_address>
    set mode {proxy | tunnel}
    set password <passwd>
    set port <integer>
    set status {disable | enable}
end

```

| Variable | Description |
|---------------------------|---|
| ip <proxy_ipv4_address> | Enter the IPv4 address of the web proxy. Default: 0.0.0.0 |
| ip6 <proxy_ipv6_address> | Enter the IPv6 address of the web proxy. |
| mode {proxy tunnel} | Enter the web proxy mode. The following options are available: <ul style="list-style-type: none"> • proxy: HTTP proxy. • tunnel: HTTP tunnel. |
| password <passwd> | If the web proxy requires authentication, type the password for the user name. |
| port <integer> | Enter the port number of the web proxy. Default: 80. Range: 1 to 65535 |
| status {disable enable} | Enable/disable connections through the web proxy. Default: disable |
| username <string> | If the web proxy requires authentication, enter the user name. |

execute

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

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



FortiManager CLI commands and variables are case sensitive.

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

add-on-licence

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



This command is only available on high end FortiManager hardware models, including the 3900E, 3000F, and 4000E.

Syntax

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

add-vm-license

Add a VM license to the FortiManager.



This command is only available on FortiManager VM models.

Syntax

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

| Variable | Description |
|--------------|------------------------|
| <vm_license> | The VM license string. |

Example

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

```
execute add-vm-license "-----BEGIN FMG VM LICENSE-----
QAAAAJ09s+LTe...ISJTTYpCkOdMm6
-----END FAZ VM LICENSE-----"
```

backup

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

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

Syntax

```
execute backup all-settings {ftp | scp | sftp} <ip> <string> <username> <passwd> <ssh-
cert> <crptpasswd>
execute backup logs <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
<directory> <vdlst>
execute backup logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
<directory> <vdlst>
execute backup logs-rescue <device serial number(s)> {ftp | scp | sftp} <ip> <username>
<passwd> <directory> <vdlst>
```

```
execute backup reports <report schedule name(s)> {ftp | scp | sftp} <ip> <username>
<passwd> <directory> <vdlst>
execute backup reports-config <adom name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
<directory> <vdlst>
```

| Variable | Description |
|---------------------------|--|
| all-settings | Backup all FortiManager settings to a file on a server. |
| logs | Backup the device logs to a specified server. |
| logs-only | Backup device logs only to a specified server. |
| logs-rescue | Use this hidden command to backup logs regardless of DVM database for emergency reasons. This command will scan folders under /Storage/Logs/ for possible device logs to backup. |
| reports | Backup the reports to a specified server. |
| reports-config | Backup reports configuration to a specified server. |
| <device name(s)> | Enter the device name(s) separated by a comma, or enter <code>all</code> for all devices. |
| <device serial number(s)> | Enter the device serial number(s) separated by a comma, or enter <code>all</code> for all devices. |
| <report schedule name(s)> | Enter the report schedule name(s) separated by a comma, or enter <code>all</code> for all reports schedules. |
| <adom name(s)> | Enter the ADOM name(s) separated by a comma, or enter <code>all</code> for all ADOMs. |
| {ftp scp sftp} | Enter the server type: <code>ftp</code> , <code>scp</code> , or <code>sftp</code> . |
| <ip> | Enter the server IP address. |
| <string> | Enter the path and file name for the backup. |
| <username> | Enter username to use to log on the backup server. |
| <passwd> | Enter the password for the username on the backup server. |
| <ssh-cert> | Enter the SSH certification for the server. This option is only available for backup operations to SCP servers. |
| <crtpasswd> | Optional password to protect backup content. Use <code>any</code> for no password. |
| <directory> | Enter the path to where the file will be backed up to on the backup server. |
| <vdlst> | List of VDOMs. |

Example

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

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

bootimage

Use this command to set the boot image partition.



This command is only available on FortiManager hardware models.

Syntax

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

certificate

Use these commands to manage certificates.

certificate ca

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

Syntax

To list the CA certificates installed on the FortiManager unit:

```
execute certificate ca list
```

To export or import CA certificates:

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

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

certificate local

Use these commands to list local certificates, and to import or export local certificates. To generate a certificate request, see “certificate local generate” on page 170.

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>
```

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

certificate local generate

Use this command to generate a certificate request.

Syntax

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

| Variable | Description |
|------------------------|---|
| <certificate-name_str> | Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed. |
| <number> | Enter 512, 1024, 1536, or 2048 for the size, in bits, of the encryption key. |
| <subject> | Enter one of the following pieces of information to identify the FortiManager unit being certified: <ul style="list-style-type: none"> The FortiManager unit IP address The fully qualified domain name of the FortiManager unit An email address that identifies the FortiManager unit An IP address or domain name is preferable to an email address. |

| Variable | Description |
|--------------------------|--|
| [<optional_information>] | <p>Enter <code>optional_information</code> as required to further identify the unit. See the below table 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.</p> <p>For example, to enter the <code>organization_name_str</code>, you must first enter the <code>country_code_str</code>, <code>state_name_str</code>, and <code>city_name_str</code>.</p> <p>While entering optional variables, you can type <code>?</code> for help on the next required variable.</p> |

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 email address for the FortiManager unit. |
| <ca_server_url> | Enter the URL of the CA (SCEP) certificate server that allows auto-signing of the request. |
| <challenge_password> | Enter the challenge password for the SCEP certificate server. |

chassis

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

Syntax

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

| Variable | Description |
|----------|-------------------------------|
| <pw> | Replace the chassis password. |



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

console baudrate

Use this command to get or set the console baudrate.

Syntax

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

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

Setting the baudrate will disconnect your console session.

Example

Get the baudrate:

```
execute console baudrate
```

The response is displayed:

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

Set the baudrate to 9600:

```
execute console baudrate 9600
```

date

Get or set the FortiManagersystem date.

Syntax

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

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

- `mm` is the month and can be 01 to 12
- `dd` is the day of the month and can be 01 to 31
- `yyyy` is the year and can be 2001 to 2100

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

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

Example

This example sets the date to 17 September 2010:

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

device

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

Syntax

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

| Variable | Description |
|-----------------|-------------------------|
| <device_name> | The name of the device. |
| <password> | The device password. |
| <device_name> | The name of the device. |
| <serial_number> | The new serial number. |

Example

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

dmserver

Use these commands to manage devices and revisions.

| | |
|---------------------|------------------|
| dmserver | dmserver showdev |
| dmserver revlist | dmserver showrev |
| dmserver showconfig | |

dmserver delrev

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

Syntax

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

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

dmserver revlist

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

Syntax

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

| Variable | Description |
|---------------|-------------------------|
| <device_name> | The name of the device. |

dmserver showconfig

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

Syntax

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

| Variable | Description |
|---------------|-------------------------|
| <device_name> | The name of the device. |

dmserver showdev

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

Syntax

```
execute dmserver showdev
```

dmserver showrev

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

Syntax

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

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

erasedisk

Use this command to overwrite the flash with random data.

Syntax

```
execute erase-disk flash
```

| Variable | Description |
|---------------|---|
| <erase-times> | Number of time to overwrite flash. Valid range: 1-35 with the default set to 1. |

factory-license

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

Syntax

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

The following table lists command variables, description, and default values where applicable.

| Variables | Description |
|-----------|--------------------------------|
| <key> | Enter the factory license key. |

fgfm reclaim-dev-tunnel

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

Syntax

```
execute fgfm reclaim-dev-tunnel <device_name> force
```

| Variable | Description |
|---------------|--|
| <device_name> | Enter the device name. |
| force | Optionally, force the tunnel to be reclaimed |

fmpolicy

Use these commands to perform policy and object related actions:

fmpolicy check-upgrade-object

Use this command to check/upgrade objects by syntax.

Syntax

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

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

fmgpolicy clone-adom-object

Use this command to clone an ADOM object.

Syntax

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

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

fmpolicy copy-adom-object

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

Syntax

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

| Variable | Description |
|------------|---|
| <adom> | Enter the name of the ADOM. |
| <category> | Enter the name of the category in the ADOM. |
| <key> | Enter the name of the object key. |
| <device> | Enter the name of the device. |
| <vdom> | Enter the name of the VDOM. |

fmpolicy install-config

Use this command to install the configuration for an ADOM.

Syntax

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

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

fmpolicy print-adom-database

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

Syntax

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

fmpolicy print-adom-object

Use this command to display the device objects.

Syntax

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

| Variable | Description |
|-------------|---|
| <adom_name> | Enter the name of the ADOM or "Global". |

| Variable | Description |
|--------------|---|
| <category> | Enter the category name. |
| {all list} | The following options are available: <ul style="list-style-type: none"> all: Show all objects. list: Get all objects. |
| <output> | Output file name (output dump to file: [/tmp/pl]). |

fmpolicy print-adom-package

Use this command to display the package for an ADOM.

Syntax

```
execute fmpolicy print-adom-package <adom> <package_name> <category_name> <object_name>
<output>
execute fmpolicy print-adom-package Global <package_name> <category_name> {all | list}
<output>
```

| Variable | Description |
|-----------------|---|
| <adom> | Enter the name of the ADOM or "Global". |
| <package_name> | Enter the package name ID. |
| <category_name> | Enter the category name. |
| {all list} | The following options are available: <ul style="list-style-type: none"> all: Show all objects. list: Get all objects. |
| <object_name> | Show object by name. Enter all to show all objects, or enter list to get all objects. |
| <output> | Output file name (output dump to file: [/tmp/pl]). |

fmpolicy print-device-database

Use this command to print the device database configuration.

Syntax

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

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

fmpolicy print-device-object

Use this command to display the device objects.

Syntax

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

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

fmpolicy print-prov-templates

Use this command to print provisioning templates.

Syntax

```
execute fmpolicy print-prov-templates <adom> <prov> <package> <category> {<key> | list |
all} <output>
```

| Variable | Description |
|----------------------|--|
| <adom> | Enter the name of the ADOM. |
| <prov> | Enter the provisioning template name. The following options are available: <ul style="list-style-type: none"> 5: System Templates 8: FortiClient Templates 9: Threat Weight Templates 10: WiFi Templates |
| <package> | Enter the package name. |
| <category> | Enter the category name. |
| {<key> list all} | The following options are available: <ul style="list-style-type: none"> all: Show all objects. list: Get all objects. |
| <output> | Output file name (output dump to file: [/tmp/pl]). |

fmpolicy print-prov-database

Use this command to print provisioning databases.

Syntax

```
execute fmpolicy print-prov-database <adom> <output>
```

| Variable | Description |
|----------|--|
| <adom> | Enter the name of the ADOM. |
| <output> | Output file name (output dump to file: [/tmp/pl]). |

fmpolicy promote-adom-object

Use this command to promote an ADOM object.

Syntax

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

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

fmpolicy upload print log

Use this command to upload print logs.

Syntax

```
execute fmpolicy-upload-print-log
```

| Variable | Description |
|----------|--------------------|
| <IP> | Enter IP address. |
| <port> | Enter port number. |
| <path> | Enter path. |
| <user> | Enter user. |
| <passwd. | Enter password. |

fmprofile

Use these commands to perform profile related actions:

```
fmprofile copy-to-device
```

```
fmprofile import-profile
```

```
fmprofile export-profile
```

```
fmprofile list-profiles
```

```
fmprofile import-from-device
```

fmprofile copy-to-device

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

Syntax

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

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

fmprofile delete-profile

Use this command to delete a profile.

Syntax

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

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

fmprofile export-profile

Use this command to export profile configurations.

Syntax

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

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

fmprofile import-from-device

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

Syntax

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

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

fmprofile import-profile

Use this command to import profile configurations.

Syntax

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

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

fmprofile list-profiles

Use this command to list all profiles in an ADOM.

Syntax

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

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

fmscript

Use these commands to perform script related actions:

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

fmscript clean-sched

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

Syntax

```
execute fmscript clean-sched
```

fmscript copy

Copy a script or scripts between ADOMs.

Syntax

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

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

fmscript delete

Delete a script from FortiManager.

Syntax

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

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

fmscript import

Import a script from an FTP server to FortiManager.

Syntax

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

| Variable | Description |
|-----------------|--|
| <ftpsrvr_ip4> | The IPv4 address of the FTP server. |
| <filename> | The filename of the script to be imported to the FortiManager system. |
| <username> | The user name used to access the FTP server. |
| <password> | The password used to access the FTP server. |
| <scriptname> | The name of the script to import. |
| <scripttype> | The type of script as one of CLI or TCL. |
| <comment> | A comment about the script being imported, such as a brief description. |
| <adom_name> | Name of the administrative domain. |
| <os_type> | The operating system type, such as FortiOS. Options include <i>any</i> , <i>FortiOS</i> , and others. |
| <os_version> | The operating system version, such as FortiOS. Options include <i>any</i> , 400, and 500. |
| <platform> | The hardware platform this script can be run on. Options include <i>any</i> , or the model of the device such as <i>Fortigate 60C</i> . |
| <device_name> | The device name to run this script on. Options include <i>any</i> , or the specific device name as it is displayed on the FortiManager system |
| <build_number> | The specific build number this script can be run on. Options include <i>any</i> , 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 <i>any</i> , or the specific host name. |
| <serial_number> | The serial number of the device this script can be run on. Options include <i>any</i> , or the specific serial number of the device, such as <i>FGT60C3G28033042</i> . |

fmscript list

List the scripts on the FortiManager device.

Syntax

```
execute fmscript list
```

Example

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

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

fmscript run

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

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

Syntax

```
execute fmscript run <scriptid_int> <run_on> <device_name> <adom_name>
```

| Variable | Description |
|----------------|--|
| <scriptid_int> | The ID number of the script to run. |
| <run_on> | Select where to run the script. The following options are available: <ul style="list-style-type: none"> • device: on the device • group: on a group • devicedb: on the device's object database • globaldb: on the global database |
| <device_name> | Enter the device name to run the script on. This is required if <code>device</code> or <code>devicedb</code> were chosen for where to run the script. |
| <adom_name> | Name of the administrative domain. |

fmscript showlog

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

Syntax

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

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

Example

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

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

fmupdate

Import or export packages using the FTP, SCP, or TFTP servers, and import database files from a CD-ROM

Syntax

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

| Variables | Description |
|--------------------|---|
| {ftp scp tftp} | Select the file transfer protocol to use: ftp, scp, or tftp. |
| <type> | Select the type of file to export or import. The following options are available: av-ips, fct-av, url, spam, file-query, license-fgt, license-fct, custom-url, or domp. |
| <remote_file> | Update manager packet file name on the server or host. |
| <ip> | Enter the FQDN or the IP address of the server. |
| <port> | Enter the port to connect to on the remote SCP host. Range: 1 to 65535 |
| <remote_path> | Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead. |
| <user> | Enter the user name to log into the FTP server or SCP host |
| <password> | Enter the password to log into the FTP server or SCP host |

fmupdate cdrom

Import database files from a CD-ROM. The CD-ROM must be mounted first.



This command is only available on FortiManager hardware models that have CD-ROM drives.

Syntax

```
execute fmupdate cdrom import <type> <string>
execute fmupdate cdrom list <folder>
execute fmupdate cdrom mount
execute fmupdate cdrom unmount
```

| Variables | Description |
|-----------|--|
| import | Import database files. |
| <type> | Set the packet type: url, spam, or file-query. |
| <string> | The FortiGuard packet file name on the CD TFTP driver. |
| list | List the packets in a specific folder. |
| <folder> | The name of the folder to list. |
| mount | Mount the CD-ROM. |
| unmount | Unmount the CD-ROM. |

format

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

Syntax

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

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



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

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

iotop

Use this command to set the delay between iterations.

Syntax

```
execute iotop
```

| Variable | Description |
|----------|---|
| [delay] | Enter the delay between iteration in seconds. (Default: two seconds). |

iotps

Use this command to set the delay between iterations.

Syntax

```
execute iotps
```

| Command | Description |
|---------|---|
| Z,B | Global: 'Z' change color mappings; 'B' disable/enable bold. |

| Command | Description |
|---------|--|
| l,t,m | Toggle Summaries: 'l' load average; 't' task/cpu statistics; 'm' memory information. |
| 1,l | Toggle SMP view: '1' single/separate states; 'l' Irix/Solaris mode. |
| f,o | Fields/Columns: 'f' add or remove; 'o' change display order. |
| F or O | Select sort field. |
| <,> | Move sort field: '<' next column left; '>' next column right. |
| R,H | Toggle: 'R' normal/reverse sort; 'H' show threads. |
| c,i,S | Toggle: 'c' command name/line; 'i' idle tasks; 'S' cumulative time. |
| x,y | Toggle highlights: 'x' sort field; 'y' running tasks. |
| z,b | Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y'). |
| u | Show specific user only. |
| n or # | Set maximum tasks displayed. |
| k,r | Manipulate tasks: 'k' kill; 'r' renice. |
| d or s | Set update interval. |
| W | Write configuration file. |
| q | Quit. |

log

Use these commands to manage device logs:

| | |
|------------------------|----------------------------|
| log device disk_quota | log import |
| log device permissions | log ips-pkt clear |
| log device vdom | log quarantine-files clear |
| log dlp-files clear | |

log device disk_quota

Set the log device disk quota.

Syntax

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

| Variable | Description |
|-------------|--|
| <device_id> | Enter the log device ID number, or All for all devices. |
| <value> | Enter the disk quota value, in MB. Range: 100 to 5655 (MB) |

log device permissions

Set or view the log device permissions.

Syntax

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

| Variable | Description |
|--------------------|--|
| <device_id> | Enter the log device ID number, or All for all devices. |
| <permission> | The following options are available: <ul style="list-style-type: none"> all: All permissions logs: Log permission content: Content permission quar: Quarantine permission ips: IPS permission |
| {enable disable} | Enable/disable the option. |

log device vdom

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

Syntax

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

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

log dlp-files clear

Delete log DLP files.

Syntax

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

| Variable | Description |
|----------|--|
| <string> | Enter the device name. |
| <string> | Enter the device archive type. The following options are available: <ul style="list-style-type: none"> • all • email • im • ftp • http • mms |

log import

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

Syntax

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

| Variable | Description |
|--------------|--|
| <service> | Select the file transfer protocol to use: ftp, sftp, scp, or tftp. |
| <ip_address> | Enter the server IP address. |
| <user-name> | Enter the username. |
| <password> | Enter the password or – for no password. The <password> field is not required when <service> is tftp. |
| <file-name> | The file name (e.g. dir/fgt.alog.log) or directory name (e.g. dir/subdir/). |
| <device-id> | Replace the device ID on imported logs. Enter a device serial number of one of your log devices. For example: FG100A2104400006. |

log ips-pkt clear

Delete IPS packet files.

Syntax

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

| Variable | Description |
|----------|------------------------|
| <string> | Enter the device name. |

log quarantine-files clear

Delete log quarantine files.

Syntax

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

| Variable | Description |
|----------|------------------------|
| <string> | Enter the device name. |

log-fetch

Use the following commands to fetch logs.

log-fetch client

Use these commands to manage client sessions.

Syntax

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

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

log-fetch server

Use this command to manager the log fetching server.

Syntax

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

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

log-integrity

Query the log file's MD5 checksum and timestamp.

Syntax

```
execute log-integrity <device_name> <string>
```

| Variable | Description |
|---------------|---|
| <device_name> | Enter the name of the log device. Example: FWF40C3911000061 |
| <string> | The log file name |

lvm

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



This command is only available on FortiManager VM models.

Syntax

```
execute lvm extend [Disk1 Disk2 ...]
execute lvm info
execute lvm start
```

The following table lists command variables, description, and default values where applicable.

| Variables | Description |
|-------------------|--------------------------------|
| extend | Extend the LVM logical volume. |
| [Disk1 Disk2 ...] | Disk(s). |
| info | Get system LVM information. |
| start | Start using LVM. |

Example

View LVM information:

```
execute lvm info
Disk 1: Used 62GB
Disk 2: Used 20GB
Disk 3: Unavailable 0GB
Disk 4: Unavailable 0GB
Disk 5: Unavailable 0GB
Disk 6: Unavailable 0GB
Disk 7: Unavailable 0GB
Disk 8: Unavailable 0GB
Disk 9: Unavailable 0GB
Disk 10: Unavailable 0GB
Disk 11: Unavailable 0GB
Disk 12: Unavailable 0GB
```

max-dev-licence

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



This command is only available on FortiManager VM models.

Syntax

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

migrate

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

Syntax

```
execute migrate all-settings {ftp | scp | sftp}
```

| Variable | Description |
|--------------------|---|
| {ftp scp sftp} | Enter the server type: ftp, scp, or sftp. |
| <ip> | Enter the server IP address. |
| <string> | Enter the path and file name for the backup. |
| <username> | Enter username to use to log on the backup server. |
| <passwd> | Enter the password for the username on the backup server. |
| <ssh-cert> | Enter the SSH certification for the server. This option is only available for backup operations to SCP servers. |
| <crtpasswd> | Optional password to protect backup content. Use <code>any</code> for no password. |

ping

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

Syntax

```
execute ping <ipv4_address | hostname>
```

| Variable | Description |
|---------------------------|---|
| <ipv4_address hostname> | IPv4 address or DNS resolvable hostname of network device to contact. |

Example

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

```
execute ping 192.168.1.23
```

ping6

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

Syntax

```
execute ping6 <ipv6_address | hostname>
```

| Variable | Description |
|---------------------------|---|
| <ipv6_address hostname> | Enter the IPv6 address or DNS resolvable hostname of network device to contact. |

Example

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

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

raid

Use these commands to add or delete a hard disk to RAID.



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

Syntax

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

reboot

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

Syntax

```
execute reboot
```

Example

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

remove

Use this command to remove all reports for a specific device from the FortiManager system.

Syntax

```
execute remove reports <device-id>
```

| Variable | Description |
|-------------|-----------------------------|
| <device-id> | Enter the device identifier |

Example

```
execute remove reports FGT60C3G00000002
This operation will ERASE ALL reports that include FGT60C3G00000002!
Do you want to continue? (y/n)y

All reports that include FGT60C3G00000002 were removed.
```

reset

Use this command to reset the FortiManager unit to factory defaults. Use the `all-except-ip` command to reset to factory defaults while maintaining the current IP address and route information. Use the `adom-settings` command to reset a specified ADOM's settings.

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

Syntax

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

| Variable | Description |
|-----------|--|
| <adom> | The ADOM name. |
| <version> | The ADOM version. For example, 5 for 5.x releases. |
| <mr> | The major release number. |

Example

```
execute reset all-settings
This operation will reset all settings to factory defaults
Do you want to continue? (y/n)
```

reset-sqllog-transfer

Use this command to resend SQL logs to the database.

Syntax

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

restore

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

Syntax

```
execute restore all-settings {ftp | scp | sftp} <ip_address> <string> <username>
    <password> <ssh-cert> <crpt_password> [option1+option2+...]
execute restore image {ftp | tftp} <filepath> <ip_address> <username> <password>
execute restore logs <device name(s)> {ftp | scp | sftp} <ip_address> <username>
    <password> <directory> <vdlist>
execute restore logs-only <device name(s)> {ftp | scp | sftp} <ip_address> <username>
    <password> <directory> <vdlist>
execute restore reports <report schedule name(s)> {ftp | scp | sftp} <ip_address>
    <username> <password> <directory> <vdlist>
execute restore reports-config <adom name(s)> {ftp | scp | sftp} <ip_address> <username>
    <password> <directory> <vdlist>
```

| Variable | Description |
|---------------------------|--|
| all-settings | Restore all FortiManager settings from a file on a server. The new settings replace the existing settings, including administrator accounts and passwords. |
| image | Upload a firmware image from a TFTP server to the FortiManager unit. The FortiManager unit reboots, loading the new firmware. |
| logs | Restore the device logs. |
| logs-only | Restore only the device logs. |
| reports | Restore device reports. |
| reports-config | Restore the reports configuration. |
| {ftp tftp} | Enter the type of server to retrieve the image from: <code>ftp</code> or <code>tftp</code> . |
| {ftp scp sftp} | Enter the type of server: <code>ftp</code> , <code>scp</code> , or <code>sftp</code> . |
| <device name(s)> | Enter the device name(s) separated by a comma, or enter <code>all</code> for all devices. |
| <report schedule name(s)> | Enter the report schedule name(s) separated by a comma, or enter <code>all</code> for all reports schedules. |
| <adom name(s)> | Enter the ADOM name(s) separated by a comma, or enter <code>all</code> for all ADOMs. |
| <filepath> | Enter the file to get from the server. You can enter a path with the filename, if required. |

| Variable | Description |
|-----------------------|---|
| <ip_address> | Enter the IP address of the server to get the file from. |
| <string> | The file to get from the server. You can enter a path with the filename, if required. |
| <username> | The username to log on to the server. This option is not available for restore operations from TFTP servers. |
| <password> | The password for username on the server. This option is not available for restore operations from TFTP servers. |
| <ssh-cert> | The SSH certification for the server. This option is only available for restore operations from SCP servers. |
| <crpt_password> | Optional password to protect backup content. Use <code>any</code> for no password. |
| <directory> | Enter the directory. |
| <vdlist> | List of VDOMs. |
| [option1+option2+...] | Select whether to keep IP, routing, and HA info on the original unit. |

Example

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

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

sdns

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



This command is only available on FortiManager hardware models.

Syntax

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

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

sensor

This command lists sensors and readings.



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

Syntax

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

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

shutdown

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

Syntax

```
execute shutdown
```

Example

```
execute shutdown
The system will be halted.
Do you want to continue? (y/n)
```

sql-local

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

```
sql-local rebuild-adom
```

```
sql-local rebuild-adom
```

```
sql-local rebuild-adom
```

```
sql-local remove-db
```

```
sql-local remove-logs
```



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

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

sql-local rebuild-adom

Rebuild the log SQL database from log data for particular ADOMs.

Syntax

```
execute sql-local rebuild-adom
```

| Variable | Description |
|----------|--|
| <adom> | The ADOM name. Multiple ADOM names can be entered. |

sql-local rebuild-db

Rebuild the entire local SQL database. This operation will remove the SQL database and rebuild from log data. This operation will also reboot the device.

Syntax

```
execute sql-local rebuild-db
```

sql-local rebuild-index

Rebuild the index from log data for particular ADOMs.

Syntax

```
execute sql-local rebuild-index
```

| Variable | Description |
|--------------|--|
| <adom> | The ADOM name. Multiple ADOM names can be entered. |
| <start-time> | The start date and time of the rebuild (a time stamp, or in the format: <code>yyyy-mm-dd hh:mm:ss</code>). |
| <end-time> | The end date and time of the rebuild (a timestamp, or in the format: <code>yyyy-mm-dd hh:mm:ss</code>). |

sql-local remove-db

Remove entire local SQL database.

Syntax

```
execute sql-local remove-db
```

sql-local remove-logs

Remove SQL logs within a time period.

Syntax

```
execute sql-local remove-logs <Device ID>
```

| Variable | Description |
|-------------|--|
| <Device ID> | Enter the device ID. Example: FG300A3907552101 |

sql-query-dataset

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

Syntax

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

| Variable | Description |
|---------------------|---|
| <adom_name> | Enter the ADOM name. |
| <dataset-name> | Enter the dataset name. |
| <device/group name> | Enter the name of the device or device group. |
| <faz/dev> | Enter the name of the FortiAnalyzer. |
| <start-time> | Enter the log start time. |
| <end-time> | Enter the log end time. |

sql-query-generic

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

Syntax

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

| Variable | Description |
|----------|---------------------------------|
| <string> | Enter the SQL statement to run. |

sql-report

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

Syntax

```
execute sql-report del-font <font-name>
execute sql-report hcache-build <adom> <schedule-name> <start-time> <end-time>
execute sql-report hcache-check <adom> <schedule-name> <start-time> <end-time>
execute sql-report import-font <service> <ip> <argument 1> <argument 2> <argument 3>
execute sql-report import-lang <name> <service> <ip> <argument 1> <argument 2> <argument 3>
execute sql-report list <adom> [days-range] [layout-name]
execute sql-report list-fonts
execute sql-report list-lang
execute sql-report list-schedule <adom> [sched-only | autocache-only | detail] [detail]
execute sql-report run <adom> <schedule-name> <num-threads>
execute sql-report view <data-type> <adom> <report-name>
```

| Variable | Description |
|---------------|---|
| del-font | Delete one font. |
| hcache-build | Build report hcache. |
| hcache-check | Check report hcache. |
| import-font | Import one font. |
| import-lang | Import a user-defined language translation file. |
| list | List recent generated reports. |
| list-fonts | List all imported fonts. |
| list-lang | Display all supported language translation files. |
| list-schedule | List report schedule and autocache information. |
| run | Run a report once. |
| view | View report data. |
| <font-name> | The name of a font. |

| Variable | Description |
|-----------------|---|
| <name> | Enter the new language name to import a new language translation file or select one of the following options: <ul style="list-style-type: none"> • English • French • Japanese • Korean • Portuguese • Simplified_Chinese • Spanish • Traditional_Chinese |
| <service> | Enter the transfer protocol: ftp, sftp, scp, or tftp. |
| <ip> | Enter the server IP address. |
| <argument 1> | For FTP, SFTP, or SCP, type a user name. For TFTP, enter a file name. |
| <argument 2> | For FTP, SFTP, or SCP, type a password or '-'. For TFTP, press <enter>. |
| <argument 3> | Enter a file name and press <enter>. |
| <adom> | Enter the ADOM name to run the report. |
| <data-type> | The data type to view. Must be report-data. |
| <report-name> | The name of the report to view. |
| <schedule-name> | Select one of the available report schedule names. |
| <num-threads> | Select the number of threads. |
| <start-time> | The start date and time of the report schedule, in the format: "HH:MM yyyy/mm/dd" |
| <end-time> | The enddate and time of the report schedule, in the format: "HH:MM yyyy/mm/dd" |
| [days-range] | The recent n days to list reports, from 1 to 99. |
| [layout-name] | One of the available SQL report layout names. |

ssh

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

Syntax

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

| Variable | Description |
|---------------|--|
| <destination> | Enter the IP address or fully qualified DNS resolvable hostname of the system you are connecting to. |
| <username> | Enter 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.

ssh-known-hosts

Use these commands to remove all known SSH hosts.

Syntax

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

| Variable | Description |
|-----------|---|
| <host/ip> | Enter the hostname or IP address of the SSH host to remove. |

tac

Use this command to run a TAC report.

Syntax

```
execute tac report <file_name>
```

| Variable | Description |
|-------------|----------------------------|
| <file_name> | Optional output file name. |

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.

```
execute time <enter>
current time is: 12:54:22
```

top

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

Syntax

```
execute top
```

execute top help menu

| Command | Description |
|---------|--|
| Z,B | Global: 'z' change color mappings; 'B' disable/enable bold. |
| l,t,m | Toggle Summaries: 'l' load average; 't' task/cpu statistics; 'm' memory information. |
| 1,l | Toggle SMP view: '1' single/separate states; 'I' Irix/Solaris mode. |
| f,o | Fields/Columns: 'f' add or remove; 'o' change display order. |
| F or O | Select sort field. |
| <,> | Move sort field: '<' next column left; '>' next column right. |
| R,H | Toggle: 'R' normal/reverse sort; 'H' show threads. |
| c,i,S | Toggle: 'c' command name/line; 'i' idle tasks; 'S' cumulative time. |
| x,y | Toggle highlights: 'x' sort field; 'y' running tasks. |
| z,b | Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y'). |
| u | Show specific user only. |
| n or # | Set maximum tasks displayed. |
| k,r | Manipulate tasks: 'k' kill; 'r' renice. |
| d or s | Set update interval. |
| W | Write configuration file. |
| q | Quit. |

traceroute

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

Syntax

```
execute traceroute <host>
```

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

traceroute6

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

Syntax

```
execute traceroute6 <host>
```

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

diagnose

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



CLI commands and variables are case sensitive.

| | | |
|--------------|-----------|---------|
| auto-delete | fmupdate | report |
| cdb check | fortilogd | sniffer |
| debug | fwmanager | sql |
| dlp-archives | ha | system |
| dvm | hardware | test |
| fgfm | log | upload |
| fmnetwork | pm2 | vpn |

auto-delete

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

Syntax

```
diagnose auto-delete dlp-files {delete-now | list}
diagnose auto-delete log-files {delete-now | list}
diagnose auto-delete quar-files {delete-now | list}
diagnose auto-delete report-files {delete-now | list}
```

| Variable | Description |
|-------------------------------|--|
| dlp-files {delete-now list} | Delete DLP files right now according to the system automatic deletion policy or list DLP files. The following options are available: <ul style="list-style-type: none"><code>delete-now</code>: Delete DLP files right now according to system automatic deletion policy.<code>list</code>: List DLP files according to system automatic deletion policy. |

| Variable | Description |
|----------------------------------|---|
| log-files {delete-now list} | Delete log files right now according to the system automatic deletion policy or list log files. The following options are available: <ul style="list-style-type: none"> <code>delete-now</code>: Delete log files right now according to system automatic deletion policy. <code>list</code>: List log files according to system automatic deletion policy. |
| quar-files {delete-now list} | Delete quarantine files right now according to the system automatic deletion policy or list quarantine files. The following options are available: <ul style="list-style-type: none"> <code>delete-now</code>: Delete quarantine files right now according to system automatic deletion policy. <code>list</code>: List quarantine files according to system automatic deletion policy. |
| report-files {delete-now list} | Delete report files right now according to the system automatic deletion policy or list report files. The following options are available: <ul style="list-style-type: none"> <code>delete-now</code>: Delete report files right now according to system automatic deletion policy. <code>list</code>: List report files according to system automatic deletion policy. |

cdb check

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

Syntax

```
diagnose cdb check adom-integrity [adom]
diagnose cdb check adom-revision [adom] [preview]
diagnose cdb check db-schema-version {get | reset | upgrade} [version]
diagnose cdb check objcfg-integrity [preview]
diagnose cdb check policy-assignment [preview]
diagnose cdb check policy-packages [adom]
diagnose cdb check reference-integrity [preview]
diagnose cdb check update-devinfo <item> [new value] [0 | 1] [model-name]
```

| Variable | Description |
|---|---|
| adom-integrity [adom] | Check and repair the specified ADOM's database. |
| adom-revision [adom] | Check or remove invalid ADOM revision database. |
| db-schema-version {get reset upgrade} [version] | Get, reset, or upgrade the database schema version. |
| objcfg-integrity | Check object configuration database integrity. |
| policy-assignment | Check the global policy assignment table. |

| Variable | Description |
|--|--|
| policy-packages | Check the policy packages. |
| reference-integrity | Check the ADOM reference table integrity. |
| update-devinfo <item> [new value] [0 1] [model-name] | Update device information by directly changing the database. <ul style="list-style-type: none"> • <code>item</code>: Device information item • <code>new value</code>: Item new value. Default sump summary only. • <code>0 1</code>: update only empty values (default), or always update (1) • <code>model-name</code>: Only update on model name. Default: all models |
| [preview] | Optionally, preview the check before running it. |

debug

Use the following commands to debug the FortiManager.

debug application

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



The `diagnose debug application vmtools` command is only available on FortiManager VM for VMware environments.

Syntax

```

diagnose debug application alertmail <integer>
diagnose debug application curl <integer>
diagnose debug application ddmd <integer> [deviceName]
diagnose debug application depmanager <integer>
diagnose debug application dmapi <integer>
diagnose debug application dns <integer>
diagnose debug application fazcfgd <integer>
diagnose debug application fazmaild <integer>
diagnose debug application fazsvcd <integer>
diagnose debug application fdssvr <integer>
diagnose debug application fgdsrv <integer>
diagnose debug application fgdupd <integer>
diagnose debug application fgfmsd <integer> [deviceName]
diagnose debug application fnbam <integer>
diagnose debug application fortilogd <integer>
diagnose debug application FortiManagerws <integer>
diagnose debug application fortimeter <integer>
diagnose debug application gui <integer>
diagnose debug application ha <integer>
diagnose debug application ipsec <integer>
diagnose debug application localmod <integer>
diagnose debug application logd <integer>
diagnose debug application log-fetchd <integer>

```

```

diagnose debug application logfiled <integer>
diagnose debug application logfwd <integer>
diagnose debug application lrm <integer>
diagnose debug application ntpd <integer>
diagnose debug application oftpd <integer> [IP/deviceSerial/deviceName]
diagnose debug application ptmgr <integer>
diagnose debug application ptsessionmgr <integer>
diagnose debug application securityconsole <integer>
diagnose debug application snmpd <integer>
diagnose debug application sql_dashboard_rpt <integer>
diagnose debug application sql-integration <integer>
diagnose debug application sqllogd <integer>
diagnose debug application sqlplugind <integer>
diagnose debug application sqlrptcached <integer>
diagnose debug application srchd <integer>
diagnose debug application ssh <integer>
diagnose debug application sshd <integer>
diagnose debug application stored <integer>
diagnose debug application uploadd <integer>
diagnose debug application vmtools <integer>

```

| Variable | Description | Default |
|-------------------------------|--|---------|
| alertmail <integer> | Set the debug level of the alert email daemon. | 0 |
| curl <integer> | Set the debug level of the curl daemon. Use this CLI command to enable debug for monitoring progress when performing a backup/restore of a large database via FTP. | 0 |
| ddmd <integer> [deviceName] | Set the debug level of the dynamic data monitor. Enter a device name to only show messages related to that device. | 0 |
| depmanager <integer> | Set the debug level of the deployment manager. | 0 |
| dmworker <integer> | Set the debug level of the deployment manager worker. | 0 |
| dmapi <integer> | Set the debug level of the dmapi daemon. | 0 |
| dns <integer> | Set the debug level of the DNS daemon | 0 |
| fazcfgd <integer> | Set the debug level of the fazcfgd daemon. | 0 |
| fazmaild <integer> | Set the debug level of the fazmaild daemon. | 0 |
| fazsvcd <integer> | Set the debug level of the fazsvcd daemon. | 0 |
| fdssvrd <integer> | Set the debug level of the FDS server daemon. | 0 |
| fgdsrv <integer> | Set the debug level of the FortiGuard query daemon. | 0 |
| fgdupd <integer> | Set the debug level of the FortiGuard update daemon. | 0 |
| fgfmsd <integer> [deviceName] | Set the debug level of FGFM daemon. Enter a device name to only show messages related to that device. | 0 |

| Variable | Description | Default |
|--|--|---------|
| fnbam <integer> | Set the debug level of the Fortinet authentication module. | 0 |
| fortilogd <integer> | Set the debug level of the fortilogd daemon. | 0 |
| fortimanagerws <integer> | Set the debug level of the FortiManager Web Service. | 0 |
| fortimeter <integer> | Set the debug level of the Fortimeter. | 0 |
| gui <integer> | Set the debug level of the GUI. | 0 |
| ha <integer> | Set the debug level of high availability daemon. | 0 |
| ipsec <integer> | Set the debug level of the IPsec daemon. | 0 |
| localmod <integer> | Set the debug level of the localmod daemon. | 0 |
| logd <integer> | Set the debug level of the log daemon. | 0 |
| log-fetched <integer> | Set the debug level for the log-fetched. | 0 |
| logfiled <integer> | Set the debug level of the logfiled daemon. | 0 |
| logfwd <integer> | Set the debug level of the logfwd daemon. | 0 |
| lrm <integer> | Set the debug level of the Log and Report Manager. | 0 |
| ntpd <integer> | Set the debug level of the NTP daemon. | 0 |
| oftpd <integer> [IP/deviceSerial/deviceName] | Set the debug level of the oftpd daemon. Enter an IPv4 address, device serial number, or device name to only show messages related to that device or IPv4 address. | 0 |
| ptmgr <integer> | Set the debug level of the Portal Manager. | 0 |
| ptsessionmgr <integer> | Set the debug level of the Portal Session Manager. | 0 |
| securityconsole <integer> | Set the debug level of the security console daemon. | 0 |
| snmpd <integer> | Set the debug level of the SNMP daemon. | 0 |
| sql_dashboard_rpt <integer> | Set the debug level of the SQL dashboard report daemon. | 0 |
| sql-integration <integer> | Set the debug level of SQL applications. | 0 |
| sqllogd <integer> | Set the debug level of SQL log daemon.. | 0 |
| sqlplugind <integer> | Set the debug level of the SQL plugin daemon. | 0 |
| sqlrptcached <integer> | Set the debug level of the SQL report caching daemon. | 0 |
| srchd <integer> | Set the debug level of the SRCH daemon. | 0 |

| Variable | Description | Default |
|-------------------|---|---------|
| ssh <integer> | Set the debug level of SSH protocol transactions. | 0 |
| sshd <integer> | Set the debug level of the SSH daemon. | 0 |
| stored <integer> | Set the debug level of communication with java clients. | 0 |
| uploadd <integer> | Set the debug level of the upload daemon. | 0 |
| vmtools <integer> | Set the debug level for vmtools. | 0 |

Example

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

```
diagnose debug application uploadd 7
```

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <integer>
```

| Variable | Description |
|-----------|---|
| <integer> | Set the debug level of the CLI. Range: 0 to 8. Default: 3 |

debug console

Use this command to Enable/disable console debugging.

Syntax

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

| Variable | Description |
|--------------------|--------------------------------------|
| {enable disable} | Enable or disable console debugging. |

debug crashlog

Use this command to manage crash logs.

Syntax

```
diagnose debug crashlog clear  
diagnose debug crashlog read
```

| Variable | Description |
|----------|--|
| clear | Delete backtrace and core files. |
| read | Show the crash logs. This command is hidden. |

debug disable

Use this command to disable debug.

Syntax

```
diagnose debug disable
```

debug dpm

Use this command to manage the deployment manager.

Syntax

```
diagnose debug dpm comm-trace {enable | disable | status}
diagnose debug dpm conf-trace {enable | disable | status}
diagnose debug dpm probe-device <ip>
```

| Variable | Description |
|--|--|
| comm-trace {enable disable status} | Enable a DPM to FortiGate communication trace: enable, disable, or status. |
| conf-trace {enable disable status} | Enable a DPM to FortiGate configuration trace: enable, disable, or status. |
| probe-device <ip> | Check device status. |

debug enable

Use this command to enable debug.

Syntax

```
diagnose debug enable
```

debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

debug reset

Use this command reset the debug level settings. All debug settings will be reset.

Syntax

```
diagnose debug reset
```

debug service

Use this command to debug services.

Syntax

```
diagnose debug service cdb <integer>
diagnose debug service cmdb <integer>
diagnose debug service dvmcmd <integer>
diagnose debug service dvmdb <integer>
diagnose debug service fazconf <integer>
diagnose debug service main <integer>
diagnose debug service sys <integer>
diagnose debug service task <integer>
```

| Variable | Description |
|-------------------|---|
| cdb <integer> | Debug the CDB daemon service. Enter the debug level. |
| cmdb <integer> | Debug the CMDB daemon service. Enter the debug level. |
| dvmcmd <integer> | Debug the DVMCMD daemon service. Enter the debug level. |
| dvmdb <integer> | Debug the DVMDDB (Device Manager Database) daemon service. Enter the debug level. |
| fazconf <integer> | Debug the NCMDDB daemon service. Enter the debug level. |
| main <integer> | Debug the Main daemon service. Enter the debug level. |
| sys <integer> | Debug the SYS daemon service. Enter the debug level. |
| task <integer> | Debug the Task daemon service. Enter the debug level. |

debug sysinfo

Use this command to show system information.

Syntax

```
diagnose debug sysinfo
```

debug sysinfo-log

Use this command to generate one system log information log file every two minutes.

Syntax

```
diagnose debug sysinfo-log {on | off}
```

debug sysinfo-log-backup

Use this command to backup all system information log files to an FTP server.

Syntax

```
diagnose debug sysinfo-log-backup <ip> <string> <username> <password>
```

| Variable | Description |
|------------|---|
| <ip> | Enter the FTP server IPv4 address. |
| <string> | Enter the path or filename to save to the FTP server. |
| <username> | Enter the user name for the FTP server. |
| <password> | Enter the password for the FTP server. |

debug sysinfo-log-list

Use this command to show system information elogs.

Syntax

```
diagnose debug sysinfo-log-list <integer>
```

| Variable | Description |
|-----------|--|
| <integer> | Display the last n elogs. Default: The default value of n is 10. |

debug timestamp

Use this command to enable/disable debug timestamp.

Syntax

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

debug vminfo

Use this command to show VM license information.



This command is only available on FortiManager VM models.

Syntax

```
diagnose debug vminfo
```

dlp-archives

Use this command to manage the DLP archives.

Syntax

```
diagnose dlp-archives quar-cache list-all-process
diagnose dlp-archives quar-cache kill-process <pid>
diagnose dlp-archives rebuild-quar-db
diagnose dlp-archives remove
diagnose dlp-archives statistics {show | flush}
diagnose dlp-archives status
diagnose dlp-archives upgrade
```

| Variable | Description |
|-------------------------------|--|
| quar-cache list-all-process | List all processes that are using the quarantine cache. |
| quar-cache kill-process <pid> | Kill a process that is using the quarantine cache. |
| rebuild-quar-db | Rebuild Quarantine Cache DB |
| remove | Remove all upgrading DLP archives. |
| statistics {show flush} | Display or flush the quarantined and DLP archived file statistics. The following options are available: <ul style="list-style-type: none"><code>flush</code>: Flush quarantined and DLP archived file statistics.<code>show</code>: Display quarantined and DLP archived file statistics. |
| status | Running status. |
| upgrade | Upgrade the DLP archives. |

dvm

Use the following commands for DVM related settings.

dvm adom

Use this command to list ADOMs.

Syntax

```
diagnose dvm adom list
```

| Variable | Description |
|----------|---|
| list | List ADOMs, state, product, OS version (OSVER), major release (MR), name, mode, and VPN management. |

dvm capability

Use this command to set the DVM capability.

Syntax

```
diagnose dvm capability set {all | standard}
diagnose dvm capability show
```

| Variable | Description |
|----------------------|--|
| set {all standard} | Set the capability to all or standard: <code>all</code> or <code>standard</code> . |
| show | Show what the capability is set to. |

dvm chassis

Use this command to list chassis.

Syntax

```
diagnose dvm chassis list
```

| Variable | Description |
|----------|---------------|
| list | List chassis. |

dvm check-integrity

Use this command to check the DVM database integrity.

Syntax

```
diagnose dvm check-integrity
```

dvm debug

Use this command to enable/disable debug channels.

Syntax

```
diagnose dvm debug {enable | disable} <channel> <channel> <channel>
```

| Variable | Description |
|--------------------|-----------------------------------|
| {enable disable} | Enable or disable debug channels. |

| Variable | Description |
|-----------|--|
| <channel> | <p>The following options are available:</p> <ul style="list-style-type: none"> • All • dvm_db • dvm_dev • shelfmgr • ipmi • lib • dvmcmd • dvmcore • gui • monitor |

dvm device

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

Syntax

```
diagnose dvm device dynobj <device>
diagnose dvm device list <device> <vdom>
diagnose dvm device delete <adom> <device>
diagnose dvm device monitor <device> <api>
```

| Variable | Description |
|------------------------|--|
| dynobj <device> | List dynamic objects on this device. |
| list <device> <vdom> | List devices. Optionally, enter a device or VDOM name. |
| delete <adom> <device> | Delete devices for a specific ADOM. |
| monitor <device> <api> | JSON API for device monitor. Specify the device name and the monitor API name. |

Example

The following example shows the results of running the monitor command for WiFi clients.

```
FMG-VM64 # diagnose dvm device monitor FortiGate-VM64 wifi/client
Request :
{
  "id": 1473975442,
  "method": "exec",
  "params": [
    {
      "data": {
        "action": "get",
        "resource": "/api/v2/monitor/wifi/client",
        "target": [
          "adom/root/device/FortiGate-VM64"
```

```

    ]
    },
    "url": "sys/proxy/json"
  }
]
}
Response :
{
  "id": 1473975442,
  "result": [
    {
      "data": [
        {
          "response": {
            "action": "select",
            "build": 1081,
            "http_method": "GET",
            "name": "client",
            "path": "wifi",
            "results": null,
            "serial": "FGVMEV0000000000",
            "status": "success",
            "vdom": "root",
            "version": "v5.4.0"
          },
          "status": {
            "code": 0,
            "message": "OK"
          },
          "target": "FortiGate-VM64"
        }
      ],
      "status": {
        "code": 0,
        "message": "OK"
      },
      "url": "sys/proxy/json"
    }
  ]
}

```

dvm device-tree-update

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

Syntax

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

| Variable | Description |
|--------------------|---|
| {enable disable} | Enable or disable device tree autoupdate. |

dvm extender

Use these commands to list FortiExtender devices and synchronize FortiExtender data via JSON.

Syntax

```
diagnose dvm extender list
diagnose dvm extender sync-extender-data <device>
diagnose dvm extender get-extender-modem-ip <device> <id>
```

| Variable | Description |
|-----------------------|---|
| list | List FortiExtender devices. |
| sync-extender-data | Synchronize FortiExtender data by JSON. |
| get-extender-modem-ip | Get the FortiExtender modem IPv4 address by JSON. |
| <device> | Enter the device name. |
| <id> | Enter the FortiExtender ID. |

dvm group

Use this command to list groups.

Syntax

```
diagnose dvm group list
```

| Variable | Description |
|----------|--------------|
| list | List groups. |

dvm lock

Use this command to print the DVM lock states.

Syntax

```
diagnose dvm lock
```

dvm proc

Use this command to list DVM processes.

Syntax

```
diagnose dvm proc list
```

| Variable | Description |
|----------|-----------------|
| list | List processes. |

dvm supported-platforms

Use this command to list supported platforms and firmware versions.

Syntax

```
diagnose dvm supported-platforms list detail
diagnose dvm supported-platforms mr-list
```

| Variable | Description |
|----------|--|
| list | List support platforms. |
| detail | Show detail with syntax support. |
| mr-list | List support platforms by major release. |

dvm task

Use this command to repair or reset the task database.

Syntax

```
diagnose dvm task list <adom> <type>
diagnose dvm task repair
diagnose dvm task reset
```

| Variable | Description |
|--------------------|---|
| list <adom> <type> | List task database information. |
| repair | Repair the task database while preserving existing data where possible. The FortiManager will reboot after the repairs. |
| reset | Reset the task database to its factory default state. All existing tasks and the task history will be erased. The FortiManager will reboot after the reset. |

dvm transaction-flag

Use this command to edit or display DVM transaction flags.

Syntax

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

| Variable | Description |
|------------------------|---|
| {abort debug none} | The following options are available: abort, debug, or none. |

dvm workflow

Use this command to edit or display workflow information.

Syntax

```
diagnose dvm workflow log-list <ADOM_name> <workflow_session_ID>
diagnose dvm workflow session-list <ADOM_name>
```

| Variable | Description |
|---------------------------|--|
| {log-list session-list} | The following options are available: <ul style="list-style-type: none">log-list: List workflow session log.session-list: List workflow session. |

fgfm

Use this command to get installation session, object, and session lists.

Syntax

```
diagnose fgfm install-session
diagnose fgfm object-list
diagnose fgfm session-list <device ID>
```

| Variable | Description |
|--------------------------|----------------------------------|
| install-session | Get installations session lists. |
| object-list | Get object lists. |
| session-list <device ID> | Get session lists. |

fmnetwork

Use the following commands for network related settings.

fmnetwork arp

Use this command to manage ARP.

Syntax

```
diagnose fmnetwork arp del <intf-name> <IP>
diagnose fmnetwork arp list
```

| Variable | Description |
|----------------------|----------------------|
| del <intf-name> <IP> | Delete an ARP entry. |
| list | List ARP entries. |

fmnetwork interface

Use this command to view interface information.

Syntax

```
diagnose fmnetwork interface detail <portX>
diagnose fmnetwork interface list <portX>
```

| Variable | Description |
|----------------|--|
| detail <portX> | View a specific interface's details. For example: port1. |
| list <portX> | List all interface details. For example: port1. |

fmnetwork netstat

Use this command to view network statistics.

Syntax

```
diagnose fmnetwork netstat list
diagnose fmnetwork netstat list [-r]
diagnose fmnetwork netstat tcp
diagnose fmnetwork netstat tcp [-r]
diagnose fmnetwork netstat udp
diagnose fmnetwork netstat udp [-r]
```

| Variable | Description |
|-----------|--|
| list | List all connections. |
| list [-r] | Use -r to list only resolved IPv4 addresses. |
| tcp | List all TCP connections. |
| tcp [-r] | Use -r to list only resolved IPv4 addresses. |
| udp | List all UDP connections. |
| udp [-r] | Use -r to list only resolved IPv4 addresses. |

fmupdate

Use this command to diagnose update services.

Syntax

```
diagnose fmupdate dbcontract
diagnose fmupdate deldevice {fct | fds | fgd | fgc} <serialnum> <uid>
diagnose fmupdate del-log
diagnose fmupdate del-object
diagnose fmupdate del-serverlist
diagnose fmupdate fct-getobject
diagnose fmupdate fds-dump-breg
diagnose fmupdate fds-dump-srul
diagnose fmupdate fds-get-downstream-device <serialnum>
diagnose fmupdate fds-getobject
```

```

diagnose fmupdate fds-service-info
diagnose fmupdate fds-update-info
diagnose fmupdate fgd-asdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} {all |
    <serial>} <integer>
diagnose fmupdate fgd-asserver-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d}
diagnose fmupdate fgd-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fgd-dbver {wf | as | av-query}
diagnose fmupdate fgd-get-downstream-device
diagnose fmupdate fgd-test-client <ip> <serialnum> <string> <integer>
diagnose fmupdate fgd-url-rating <serialnum> <version> <url>
diagnose fmupdate fgd-wfas-clear-log
diagnose fmupdate fgd-wfas-log {name | ip} <string>
diagnose fmupdate fgd-wfas-rate {wf | av | as_ip | as_url | as_hash}
diagnose fmupdate fgd-wfdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} <serialnum>
diagnose fmupdate fgd-wfserver-stat {top10sites | top10devices} {10m | 30m | 1h | 6h |
    12h | 24h | 7d}
diagnose fmupdate fgt-del-statistics
diagnose fmupdate fgt-del-um-db
diagnose fmupdate fmg-statistic-info
diagnose fmupdate fortitoken {seriallist | add | del} {add | del | required}
diagnose fmupdate getdevice {fct | fds | fgd | fgc} <serialnum>
diagnose fmupdate list-object
diagnose fmupdate service-restart {fds | fct | fgd | fgc}
diagnose fmupdate show-bandwidth {fct | fgt | fml | faz} <string>
diagnose fmupdate show-dev-obj <serialnum>
diagnose fmupdate updatenow {Service[fds | fgd | fct]} <string>
diagnose fmupdate update-status
diagnose fmupdate view-linkd-log {fct | fds | fgd | fgc}
diagnose fmupdate view-configure
diagnose fmupdate view-serverlist
diagnose fmupdate view-service-info
diagnose fmupdate vm-license

```

| Variable | Description |
|---|--|
| dbcontract | Serial number of the device. |
| deldevice {fct fds fgd fgc} <serialnum> <uid> | Delete a device. The UID applies only to FortiClient devices. |
| del-log | Delete log for FDS and FortiGuard update events. |
| del-object | Remove all objects. |
| del-serverlist | Delete server list. |
| fct-getobject | Get the version of all FortiClient objects. |
| fds-dump-breg | Dump the FDS beta serial numbers. |
| fds-dump-srul | Dump the FDS select filtering rules. |
| fds-get-downstream-device <serialnum> | Get information of all downstream FortiGate antivirus-IPS devices. Optionally, enter the device serial number. |

| Variable | Description |
|--|--|
| fds-getobject | Get the version of all FortiGate objects. |
| fds-update-info | Display the FDS update information. |
| fgd-asdevice-stat {10m 30m 1h 6h 12h 24h 7d} {all <serial>} <integer> | Display antispam device statistics for single or all devices. <integer>: Number of time periods to display (optional, default is 1). |
| fgd-asserver-stat {10m 30m 1h 6h 12h 24h 7d} | Display antispam server statistics. |
| fgd-bandwidth {1h 6h 12h 24h 7d 30d} | Display the download bandwidth. |
| fgd-dbver {wf as av-query} | Get the version of the database. Optionally, enter the database type. |
| fgd-get-downstream-device | Get information on all downstream FortiGate web filter and spam devices. |
| fgd-test-client <ip> <serialnum> <string> <integer> | Execute FortiGuard test client. Optionally, enter the hostname or IPv4 address of the FGD server, the serial number of the device, and the query number per second or URL. |
| fgd-url-rating <serialnum> <version> <url> | Rate URLs within the FortiManager database using the FortiGate serial number. Optionally, enter the category version and URL. |
| fgd-wfas-clear-log | Clear the FortiGuard service log file. |
| fgd-wfas-log {name ip} <string> | View the FortiGuard service log file. Optionally, enter the device filter type, and device name or IPv4 address. |
| fgd-wfas-rate {wf av as_ip as_url as_hash} | Get the web filter / antispam rating speed. Optionally, enter the server type. |
| fgd-wfdevice-stat {10m 30m 1h 6h 12h 24h 7d} <serialnum> | Display web filter device statistics. Optionally, enter a specific device's serial number. |
| fgd-wfserver-stat {top10sites top10devices} {10m 30m 1h 6h 12h 24h 7d} | Display web filter server statistics for the top 10 sites or devices. Optionally, enter the time frame to cover. |
| fgt-del-statistics | Remove all statistics (antivirus / IPS and web filter / antispam). This command requires a reboot. |
| fgt-del-um-db | Remove UM and UM-GUI databases. This command requires a reboot. Note: um.db is a sqlite3 database that update manager uses internally. It will store AV/IPS package information of downloaded packages. This command removed the database file information. The package is not removed. After the reboot, the database will be recreated. Use this command if you suspect the database file is corrupted. |

| Variable | Description |
|---|--|
| fmg-statistic-info | Display statistic information for FortiManager and Java Client. |
| fortitoken {seriallist add del} {add del required} | FortiToken related operations. |
| getdevice {fct fds fgd fgc} <serialnum> | Get device information. Optionally, enter a serial number. |
| list-object | List downloaded linkd service objects. |
| service-restart {fds fct fgd fgc} | Restart <code>linkd</code> service. |
| show-bandwidth {fct fgt fml faz} <string> | Display download bandwidth. Enter the device type and type a value for <string>. The following options are available: <ul style="list-style-type: none"> 1h: 1 hours 6h: 6 hours 12h: 12 hours 24h: 24 hours 7d: 7 days 30d: 30 days |
| show-dev-obj <serialnum> | Display an objects version of a device. Optionally, enter a serial number. |
| updatenow {Service[fds fgd fct]} <string> | Update <code>fds</code> , <code>fgd</code> or <code>fct</code> immediately. |
| update-status | Display the update status. |
| view-linkd-log {fct fds fgd fgc} | View the <code>linkd</code> log file. |
| view-configure | View running configurations. The string value includes the type <code>fct</code> <code>fds</code> <code>fgd</code> <code>fgc</code>]. |
| view-serverlist | View the server list. The string value includes the type <code>fct</code> <code>fds</code> <code>fgd</code> <code>fgc</code>]. |
| view-service-info | Display the service information. |
| vm-license | Dump the FortiGate VM license. |

fortilogd

Use this command to view FortiLog daemon information.

Syntax

```
diagnose fortilogd msgrate
diagnose fortilogd msgrate-device
```

```

diagnose fortilogd msgrate-total
diagnose fortilogd msgrate-type
diagnose fortilogd msgstat <flush>
diagnose fortilogd lograte
diagnose fortilogd status

```

| Variable | Description |
|----------------|-----------------------------------|
| msgrate | Display log message rate. |
| msgrate-device | Display log message rate devices. |
| msgrate-total | Display log message rate totals. |
| msgrate-type | Display log message rate types. |
| msgstat | Display log message status. |
| lograte | Display the log rate. |
| <flush> | Reset the log message status. |
| status | Running status. |

fwmanager

Use this command to manage firmware.

Syntax

```

diagnose fwmanager cancel-devsched <string> <firmware_version> <release_type> <build_
num> <date_time>
diagnose fwmanager cancel-grpsched <string> <firmware_version> <release_type> <build_
num> <date_time>
diagnose fwmanager delete-all
diagnose fwmanager delete-imported-images
diagnose fwmanager delete-official-images
diagnose fwmanager delete-serverlist
diagnose fwmanager fwm-log
diagnose fwmanager getall-schedule
diagnose fwmanager getdev-schedule <string>
diagnose fwmanager getgrp-schedule <string>
diagnose fwmanager imported-imagelist
diagnose fwmanager official-imagelist <platform>
diagnose fwmanager reset-schedule-database
diagnose fwmanager set-devsched <string> <firmware_version> <release_type> <build_num>
<date_time>
diagnose fwmanager set-grpsched <string> <firmware_version> <release_type> <build_num>
<date_time>

```

| Variable | Description |
|---|--|
| cancel-devsched <string> <firmware_version> <release_type> <build_num> <date_time> | Cancel an upgrade schedule for a device. For special branches, the release type is the branch point. The build number for official releases is always -1, for special releases it is the build number. The date and time format is: YYYY/MM/DD_hh:mm:ss |
| cancel-grpsched <string> <firmware_version> <release_type> <build_num> <date_time> | Cancel an upgrade schedule for a group. For special branches, the release type is the branch point. The build number for official releases is always -1, for special releases it is the build number. The date and time format is: YYYY/MM/DD_hh:mm:ss |
| delete-all | Remove everything in the firmware manager folder. This command requires a reboot. |
| delete-imported-images | Remove all imported images. This command requires a reboot. |
| delete-official-images | Remove all official images. This command requires a reboot. |
| delete-serverlist | Remove the server list file (fdni.dat). This command requires a reboot. |
| fwm-log | View the firmware manager log file. |
| getall-schedule | Display all upgrade schedules recorded. |
| getdev-schedule <string> | Get scheduled upgrades for the device. |
| getgrp-schedule <string> | Get scheduled upgrades for this group. |
| imported-imagelist | Get the imported firmware image list |
| official-imagelist <platform> | Get the official firmware image list for the platform. |
| reset-schedule-database | Cleanup and initialize the schedule database and restart the server. |
| set-devsched <string> <firmware_version> <release_type> <build_num> <date_time> | Create an upgrade schedule for a device. |
| set-grpsched <string> <firmware_version> <release_type> <build_num> <date_time> | Create an upgrade schedule for a group. |

ha

Use this command to manage high availability.

Syntax

```
diagnose ha debug-sync {on | off}
diagnose ha dump-datalog
diagnose ha force-resync
```

```
diagnose ha stats
```

| Variable | Description |
|-----------------------|----------------------------------|
| debug-sync {on off} | Turn on synchronized data debug. |
| dump-datalog | Dump the HA data log. |
| force-resync | Force re-synchronization. |
| stats | Get HA statistics. |

hardware

Use this command to view hardware information.

Syntax

```
diagnose hardware info
```

| Variable | Description |
|----------|------------------------------------|
| info | Show hardware related information. |

log

Use this command to view and manage device logging.

log device

Use this command to manage device logging.

Syntax

```
diagnose log device
```

log device <DEVICE ID>

Optionally filter by device ID,

Syntax

```
diagnose log device <DEVICE ID>
```

pm2

Use this command to print from and check the integrity of the policy manager database.

Syntax

```
diagnose pm2 check-integrity {all adom device global ips task ncldb}
diagnose pm2 print <log-type>
```

| Variable | Description |
|---|---|
| check-integrity {all adom device global ips task ncldb} | Check policy manager database integrity. Multiple database categories can be checked at once. |
| print <log-type> | Print policy manager database log messages. |

report

Use these commands to check the SQL database.

Syntax

```
diagnose report clean {ldap-cache | report-queue}
diagnose report status {pending | running}
```

| Variable | Description |
|-----------------------------------|---|
| clean {ldap-cache report-queue} | Cleanup the SQL report queue of LDAP cache. |
| status {pending running} | Check status information on pending and running reports list. The following options are available: <ul style="list-style-type: none"> <code>pending</code>: Pending reports list. <code>running</code>: Running reports list. |

sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiManager units have a built-in sniffer. Packet capture on FortiManager units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output is printed to your CLI display until you stop it by pressing Control key + C, or until it reaches the number of packets that you have specified to capture.



Packet capture can be very resource intensive. To minimize the performance impact on your FortiManager unit, use packet capture only during periods of minimal traffic, with a serial console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

Syntax

```
diagnose sniffer packet <interface_name> <filter_str> <verbose> <count> <Timestamp
format>
```

| Variable | Description |
|--------------------|---|
| <interface_name> | Enter the name of a network interface whose packets you want to capture, such as <code>port1</code> , or type <code>any</code> to capture packets on all network interfaces. |
| <filter_str> | <p>Enter either <code>none</code> to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as <code>'tcp port 25'</code>. Surround the filter string in quotes.</p> <p>The filter uses the following syntax:</p> <pre>'[[src dst] host {<host1_fqdn> <host1_ipv4>}} [and or] [[src dst] host {<host2_fqdn> <host2_ ipv4>}} [and or] [[arp ip gre esp udp tcp] port <port1_int>] [and or] [[arp ip gre esp udp tcp] port <port2_int>]'</pre> <p>To display only the traffic between two hosts, specify the IPv4 addresses of both hosts. To display only forward or only reply packets, indicate which host is the source, and which is the destination.</p> <p>For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter:</p> <pre>'udp and port 1812 and src host 1.example.com and dst \(2.example.com or 2.example.com \)'</pre> |
| <verbose> | <p>Enter one of the following numbers indicating the depth of packet headers and payloads to capture:</p> <ul style="list-style-type: none"> 1: print header of packets (default) 2: print header and data from IP of packets 3: print header and data from ethernet of packets (if available) 4: print header of packets with interface name 5: print header and data from IP of packets with interface name 6: print header and data from ethernet of packets (if available) with intf name <p>For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).</p> |
| <count> | <p>Enter the number of packets to capture before stopping.</p> <p>If you do not specify a number, the command will continue to capture packets until you press the control key + C.</p> |
| <Timestamp format> | <p>Enter the timestamp format.</p> <ul style="list-style-type: none"> a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms otherwise: relative to the start of sniffing, ss.ms |

Example 1

The following example captures the first three packets' worth of traffic, of any port number or protocol and between any source and destination (a filter of `none`), that passes through the network interface named `port1`.

The capture uses a low level of verbosity (indicated by 1).

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
Packet capture can be very resource intensive. To minimize the performance impact on
your FortiManager unit, use packet capture only during periods of minimal traffic,
with a serial console CLI connection rather than a Telnet or SSH CLI connection,
and be sure to stop the command when you are finished.# diag sniffer packet port1
none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example 2

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by 1). Because the filter does not specify either host as the source or destination in the IPv4 header (`src` or `dst`), the sniffer captures both forward and reply traffic.

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses the control key + C. The sniffer then confirms that five packets were seen by that network interface.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
Packet capture can be very resource intensive. To minimize the performance impact on
your FortiManager unit, use packet capture only during periods of minimal traffic,
with a serial console CLI connection rather than a Telnet or SSH CLI connection,
and be sure to stop the command when you are finished.# diag sniffer packet port1
'host 192.168.0.2 or host 192.168.0.1 and tcp port 80' 1
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example 3

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IPv4 address. The capture uses a high level of verbosity (indicated by 3).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses the control key + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
Packet capture can be very resource intensive. To minimize the performance impact on
your FortiManager unit, use packet capture only during periods of minimal traffic,
```

```

with a serial console CLI connection rather than a Telnet or SSH CLI connection,
and be sure to stop the command when you are finished. # diag sniffer port1 'tcp
port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 .....E.
0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@.;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f.....
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or.....
0x0040 86bb 0000 0000 0103 0303 .....

```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encoding other than US-ASCII. It is usually preferable to analyze the output by loading it into a network protocol analyzer application such as Wireshark (<http://www.wireshark.org/>).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as PuTTY
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software such as [Wireshark](#)

To view packet capture output using PuTTY and Wireshark:

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the Fortinet appliance using either a local serial console, SSH, or Telnet connection.
3. Enter the packet capture command, such as:


```
diagnose sniffer packet port1 'tcp port 541' 3 100
```

 but do not press Enter yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*. A dialog appears where you can configure PuTTY to save output to a plain text file.
5. In the *Category* tree on the left, go to *Session > Logging*.
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)
8. Click *Apply*.
9. Press Enter to send the CLI command to the FortiMail unit, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press the control key + C to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.
13. Delete the first and last lines, which look like this:

```

===== PuTTY log 2017-09-18.07.25 11:34:40 =====
Fortinet-2000 #

```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.

14. Convert the plain text file to a format recognizable by your network protocol analyzer application. You can convert the plain text file to a format (`.pcap`) recognizable by Wireshark (formerly called Ethereal) using the `fgt2eth.pl` Perl script.



The `fgt2eth.pl` script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

To use `fgt2eth.pl`, open a command prompt, then enter a command such as the following:

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
 - `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
 - `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved
15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

sql

Use these commands to diagnose the SQL database.

Syntax

```
diagnose sql config auto-cache-delay [set <seconds>| reset]
diagnose sql config debug-filter [set | test] [string]
diagnose sql config deferred-index-timespan [set <value>]
diagnose sql config hcache-agg-step [reset | set <integer>]
diagnose sql config hcache-max-fv-row [reset | set <integer>]
diagnose sql config hcache-max-rpt-row [reset | set <integer>]
diagnose sql config report-engine [set {gen1 | gen2}]
diagnose sql config topdev-log-thres [reset | set <integer>]
diagnose sql config topdev-num-max [reset | set <integer>]
diagnose sql hcache agg-status [all | <adom>] [detail]
diagnose sql hcache rebuild-both <start-time> <end-time>
diagnose sql hcache rebuild-report <start-time> <end-time>
diagnose sql hcache rebuild-status
diagnose sql hcache status {all | <adom>}
diagnose sql process list [full]
diagnose sql process kill <pid>
diagnose sql remove {hcache <adom> [fast] | query-cache | rebuild-db-flag | tmp-tabe}
diagnose sql show {db-size | hcache-size | log-filters | log-stfile <device-id> <vdom>
| policy info <adom> }
diagnose sql status {rebuild-adom <adom> | rebuild-db | run_sql_rpt | sqlplugind |
sqlreportd}
```

```
diagnose sql upload <ftp_host_ip> <ftp_directory> <ftp_user_name> <ftp_password>
```

| Variable | Description |
|---|--|
| config auto-cache-delay [set <seconds> reset] | Show, set (in seconds), or reset the auto-cache delay. |
| config debug-filter {set test} <string> | Set or test the SQL plugin debug filter. |
| config deferred-index-timespan [set <value>] | View or set the time span for the deferred index. |
| config hcache-agg-step [reset set <integer>] | Show, set, or reset the hcache aggregation step. |
| config hcache-max-fv-row [reset set <integer>] | Show, set, or reset max row number for fortiview hcache. |
| config hcache-max-rpt-row [reset set <integer>] | Show, set, or reset max row number for report hcache. |
| config report-engine [set {gen1 gen2}] | Show or set switch report-engine version. |
| config topdev-log-thres [reset set <integer>] | Show, set, or reset log threshold of top devices. |
| config topdev-num-max [reset set <integer>] | Show, set, or reset max number of top devices. |
| hcache agg-status [all <adom>] [detail] | Show hcache aggregation info per ADOM or for all ADOMs. Enter <code>detail</code> to show detailed information. |
| hcache rebuild-both <start-time> <end-time> | Rebuild hcache for both report and FortiView. Start and end times are in the format yyyy-mm-dd hh:mm:ss. |
| hcache rebuild-report <start-time> <end-time> | Rebuild hcache for report. Start and end times are in the format yyyy-mm-dd hh:mm:ss. |
| hcache status {all <adom>} | Show detailed hcache information per ADOM or for all ADOMs. |
| process list [full] | List running query processes. |
| process kill <pid> | Kill a running query. |
| remove {hcache <adom> [fast] query-cache rebuild-db-flag tmp-table} | Remove the selected information. The following options are available: <ul style="list-style-type: none"> <code>hcache</code>: Remove the hcache tables created for the SQL report. <code>query-cache</code>: Remove the SQL query cache for log search. <code>rebuild-db-flag</code>: Remove the rebuild database flag. The system will exit the rebuild database state. <code>tmp-table</code>: Remove the SQL database temporary tables. |

| Variable | Description |
|--|--|
| <code>show {db-size hcache-size log-filters log-stfile <device-id> <vdom> policy-info <adom>}</code> | Show the database, hcache size, log filters, or log status file. The following options are available: <ul style="list-style-type: none"> <code>db-size</code>: Show database size. <code>hcache-size</code>: Show hcache size. <code>log-filters</code>: Show log view searching filters. <code>log-stfile</code>: Show logstatus file for the specified device. <code>policy-info</code>: Show policy uuid and name map. |
| <code>status {rebuild-adom <adom> rebuild-db run_sql_rpt sqlplugind sqlreportd}</code> | The following options are available: <ul style="list-style-type: none"> <code>rebuild-adom <adom></code>: Show SQL log database rebuild status of ADOMs. <code>rebuild-db</code>: Show SQL log database rebuild status. <code>run-sql-rpt</code>: Show <code>run_sql_rpt</code> status. <code>sqlplugind</code>: Show <code>sqlplugind</code> status. <code>sqlreportd</code>: Show <code>sqlreportd</code> status. |
| <code>upload <ftp_host_ip> <ftp_dir-ectory> <ftp_user_name> <ftp_password></code> | Upload <code>sqlplugind</code> messages / <code>pgsvr</code> logs via FTP. |

system

Use the following commands for system related settings.

system admin-session

Use this command to view login session information.

Syntax

```
diagnose system admin-session kill <sid>
diagnose system admin-session list
diagnose system admin-session status
```

| Variable | Description |
|-------------------------------|---------------------------|
| <code>kill <sid></code> | Kill a current session. |
| <code>list</code> | List login sessions. |
| <code>status</code> | Show the current session. |

system disk

Use this command to view disk diagnostic information.



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

Syntax

```
diagnose system disk attributes
diagnose system disk disable
diagnose system disk enable
diagnose system disk health
diagnose system disk info
diagnose system disk errors
```

| Variable | Description |
|------------|--|
| attributes | Show vendor specific SMART attributes. |
| disable | Disable SMART support. |
| enable | Enable SMART support. |
| health | Show the SMART health status. |
| info | Show the SMART information. |
| errors | Show the SMART error logs. |

system export

Use this command to export logs.

Syntax

```
diagnose system export crashlog <ftp server> <user> <password> [remote path] [filename]
diagnose system export dminstallog <devid> <server> <user> <password> [remote path]
[filename]
diagnose system export fmwslog <sftp | ftp> <type> <ftp server> <username> <password>
<directory> <filename>
diagnose system export raidlog <ftp server> <username> <password> <directory>
<filename>
diagnose system export umlog {ftp | sftp} <type> <server> <user> <password>
[remote path] [filename]
diagnose system export upgradelog <ftp server>
```

| Variable | Description |
|---|--|
| crashlog <ftp server> <user> <password> [remote path] [filename] | Export the crash log. |
| dminstallog <devid> <server> <user> <password> [remote path] [filename] | Export deployment manager install log. |

| Variable | Description |
|---|--|
| fmwslog <sftp ftp> <type> <ftp server> <username> <password> <directory> <filename> | Export web service log files. |
| raidlog <ftp server> <username> <password> <directory> <filename> | Export the RAID log. This command is only available on devices that support RAID. |
| umlog {ftp sftp} <type> <server> <user> <password> [remote path] [filename] | Export the update manager and firmware manager log files. The type options are: fdslinkd, fctlinkd, fgdlinkd, usvr, update, service, misc, umad, and fwmlinkd |
| upgradelog <ftp server> | Export the upgrade error log. |

system flash

Use this command to diagnose the flash memory.

Syntax

```
diagnose system flash list
```

| Variable | Description |
|----------|--------------------|
| list | List flash images. |

system fsck

Use this command to check and repair the filesystem.

Syntax

```
diagnose system fsck harddisk
```

| Variable | Description |
|----------|---|
| harddisk | Check and repair the file system, then reboot the system. |

system geoip

Use these commands to obtain geoip information. FortiManager uses a [MaxMind GeoLite](#) database of mappings between geographic regions and all public IPv4 addresses that are known to originate from them.

Syntax

```
diagnose system geoip {dump | info | ip}
```

| Variable | Description |
|--------------------|--|
| {dump info ip} | The following options are available: <ul style="list-style-type: none">• <code>dump</code>: All geography IP information.• <code>info</code>: Brief geography IP information.• <code>ip</code>: Find IP's country. |

system ntp

Use this command to list NTP server information.

Syntax

```
diagnose system ntp status
```

| Variable | Description |
|----------|--------------------------------|
| status | List NTP servers' information. |

system print

Use this command to print server information.

Syntax

```
diagnose system print certificate
diagnose system print cpuinfo
diagnose system print df
diagnose system print hosts
diagnose system print interface <interface>
diagnose system print loadavg
diagnose system print netstat
diagnose system print partitions
diagnose system print route
diagnose system print rtcache
diagnose system print slabinfo
diagnose system print sockets
diagnose system print uptime
```

| Variable | Description |
|-----------------------|---|
| certificate | Print the IPsec certificate. |
| cpuinfo | Print the CPU information. |
| df | Print the file system disk space usage. |
| hosts | Print the static table lookup for host names. |
| interface <interface> | Print the information of the interface |

| Variable | Description |
|------------|--|
| loadavg | Print the average load of the system. |
| netstat | Print the network statistics. |
| partitions | Print the partition information of the system. |
| route | Print the main route list. |
| rtcache | Print the contents of the routing cache. |
| slabinfo | Print the slab allocator statistics. |
| sockets | Print the currently used socket ports. |
| uptime | Print how long the system has been running. |

system process

Use this command to view and kill processes.

Syntax

```
diagnose system process kill <-signal> <pid>
diagnose system process killall <module>
diagnose system process list
```

| Variable | Description |
|----------------------|---------------------------------|
| kill <-signal> <pid> | Kill a process. |
| killall <module> | Kill all the related processes. |
| list | List all processes. |

system raid

Use this command to view RAID information.



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

Syntax

```
diagnose system raid hwinfo
diagnose system raid status
```

| Variable | Description |
|----------|---|
| hwinfo | Show RAID controller hardware information. |
| status | Show RAID status. This command displays the following information: RAID level, RAID status, RAID size, and hard disk information. |

system route

Use this command to diagnose routes.

Syntax

```
diagnose system route list
```

| Variable | Description |
|----------|--------------|
| list | List routes. |

system route6

Use this command to diagnose IPv6 routes.

Syntax

```
diagnose system route6 list
```

| Variable | Description |
|----------|--------------|
| list | List routes. |

system server

Use this command to start the FortiManager server.

Syntax

```
diagnose system server start
```

| Variable | Description |
|----------|---------------|
| start | Start system. |

test

Use the following commands to test the FortiManager.

test application

Use this command to test applications. Leave the integer value blank to see the available options for each command.

Syntax

```
diagnose test application fazcfgd <integer>
diagnose test application fazmaild <integer>
diagnose test application fazsvcg <integer>
diagnose test application fortilogd <integer>
diagnose test application logfiled <integer>
diagnose test application log-fetchd <integer>
diagnose test application logfwd <integer>
diagnose test application miglogd <integer>
diagnose test application oftpd <integer>
diagnose test application snmpd <integer>
diagnose test application sqllogd <integer>
diagnose test application sqlrptcached <integer>
```

| Variable | Description |
|--------------------|--|
| fazcfgd <integer> | Config Daemon Test Usage: <ul style="list-style-type: none"> • 1: show PID • 2: show statistics • 50: test get app icon • 51: test download app logo files • 52: dvm call stats • 53: dvm call stats clear • 54: check ips/app meta-data update • 55: log disk readahead get • 56: log disk readahead toggle • 99: restart daemon |
| fazmaild <integer> | Fazmail Daemon test. |
| fazsvcg <integer> | Service Daemon Test Usage: <ul style="list-style-type: none"> • 1: show PID • 2: list async search threads • 3: dump async search slot info • 4: show cache builder stats • 5: dump cache builder playlist • 6: dump log search filters • 50: enable or disable cache builder • 60: rawlog idx cache test • 51: enable or disable auto custom index • 99: restart daemon |

| Variable | Description |
|----------------------|--|
| fortilogd <integer> | Fortilogd Diag Test Usage: <ul style="list-style-type: none"> • 0: usage information • 1: show fortilogd pid • 2: dump message status • 3: logstat status test • 4: log forwarding status • 5: client devices status • 6: print log received • 10: pdfv2 debug enable/disable • 99: restart fortilogd |
| logfiled <integer> | Logfile Daemon Test Usage: <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 90: reset statistics and state • 99: restart daemon |
| log-fetchd <integer> | Test the log-fetchd integer. |
| logfwd <integer> | Logfwd Daemon Test. |
| miglogd <integer> | Miglogd Daemon Test Usage: <ul style="list-style-type: none"> • 1: show PID • 2: dump memory pool • 99: restart daemon |
| oftpd <integer> | Oftpd Daemon Test Usage: <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: show connected device name and IP • 4: show detailed session state • 5: show oftp request statistics • 6: show cmdb device cache • 99: restart daemon |
| snmpd <integer> | SNMP Daemon Test Usage <ul style="list-style-type: none"> • 1: display daemon pid • 2: display snmp statistics • 3: clear snmp statistics • 4: generate test trap (cpu high) • 5: generate test traps (log alert, rate, data rate) • 6: generate test traps (licensed gb/day, device quota) • 99: restart daemon |

| Variable | Description |
|------------------------|---|
| sqllogd <integer> | <p>SqlLog Daemon Test Usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: show worker init state • 4: show worker thread info • 5: show log device scan info, optionally filter by <devid> • 6: worker control setting • 7: show ADOM device list by <adom-name> • 8: show dev to sID bitmap • 41: show worker 1 info • 42: show worker 2 info • 43: show worker 3 info • 44: show worker 4 info • 45: show worker 5 info • 70: show SQL database building progress • 80: show daemon status flags • 82: show IPsec up tunnels • 84: show all unreg logdevs • 90: reset statistics and state • 91: backup all log status files • 99: restart daemon • 200: log based alert tests • 201: utmref cache tests • 221: estimated browsing time stats • 222: estimated browsing time cleanup • 223: estimated browsing time debug on/off |
| sqlrptcached <integer> | <p>Sqlrptcache Daemon Test Usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 99: restart daemon |

test connection

Use this command to test connections.

Syntax

```
diagnose test connection fortianalyzer <ip>
diagnose test connection mailserver <server-name> <mail-from> <mail-to>
diagnose test connection syslogserver <server-name>
```

| Variable | Description |
|---|---|
| fortianalyzer <ip> | Test the connection to the FortiAnalyzer. |
| mailserver <server-name> <mail-from> <mail-to> | Test the connection to the mail server. |
| syslogserver <server-name> | Test the connection to the syslog server. |

test deploymanager

Use this command to test the deployment manager.

Syntax

```
diagnose test deploymanager getcheckin <devid>
diagnose test deploymanager reloadconf <devid>
```

| Variable | Description |
|--------------------|--|
| getcheckin <devid> | Get configuration check-in information from the FortiGate. |
| reloadconf <devid> | Reload configuration from the FortiGate. |

test policy-check

Use this command to test applications.

Syntax

```
diagnose test policy-check flush
diagnose test policy-check list
```

| Variable | Description |
|----------|----------------------------------|
| flush | Flush all policy check sessions. |
| list | List all policy check sessions. |

test search

Use this command to test the search daemon.

Syntax

```
diagnose test search flush
diagnose test search list
```

| Variable | Description |
|----------|----------------------------|
| flush | Flush all search sessions. |
| list | List all search sessions. |

test sftp

Use this command to test the secure file transfer protocol (SFTP).

Syntax

```
diagnose test sftp auth <sftp server> <username> <password> <directory>
```

| Variable | Description |
|--|--|
| auth <sftp server> <username> <password> <directory> | Test the scheduled backup. The directory variable represents the directory on the SFTP server where you want to put the file. The default directory is "/". |

upload

Use these commands to perform request related actions.

upload clear

Use this command to clear the upload request.

Syntax

```
diagnose upload clear all
diagnose upload clear failed
```

| Variable | Description |
|----------|-----------------------------------|
| all | Clear all upload requests. |
| failed | Clear the failed upload requests. |

upload force-retry

Use this command to retry the last failed upload request.

Syntax

```
diagnose upload force-entry
```

upload status

Use this command to get the running status.

Syntax

```
diagnose upload status
```

vpn

Use this command to flush SAD entries and list tunnel information.

Syntax

```
diagnose vpn tunnel flush-SAD  
diagnose vpn tunnel list
```

| Variable | Description |
|-----------|--------------------------|
| flush-SAD | Flush the SAD entries. |
| list | List tunnel information. |

get

The `get` command displays all settings, even if they are still in their default state.



Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands that display that part of the configuration. Get and show commands use the same syntax as their related `config` command, unless otherwise specified.



CLI commands and variables are case sensitive.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

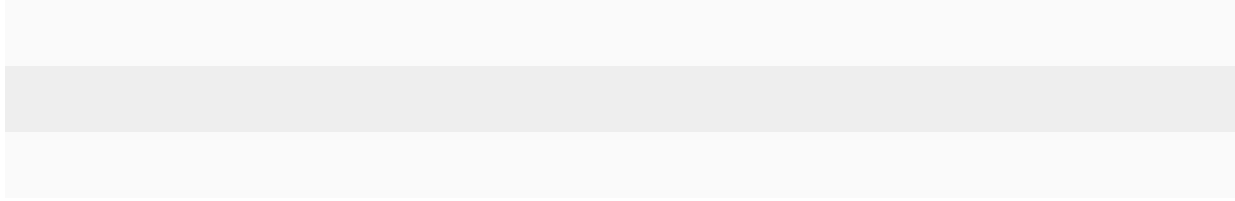
For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

| | | | |
|-----------------------------------|----------------------------|------------------|------------------------|
| fmupdate analyzer | fmupdate service | system dns | system ntp |
| fmupdate av-ips | fmupdate support-pre-fgt43 | system fips | system password-policy |
| fmupdate custom-url-list | fmupdate web-spam | system global | system performance |
| fmupdate device-version | system admin | system ha | system report |
| fmupdate disk-quota | system alert-console | system interface | system route |
| fmupdate fct-services | system alertemail | system locallog | system route6 |
| fmupdate fds-setting | system alert-event | system log | system snmp |
| fmupdate multilayer | system auto-delete | system log fetch | system sql |
| fmupdate publicnetwork | system backup | system loglimits | system status |
| fmupdate server-access-priorities | system certificate | system mail | system syslog |
| fmupdate server-over-ride-status | system dm | system metadata | system workflow |



fmupdate analyzer

Use this command to view forward virus report to FDS.

Syntax

```
get fmupdate analyzer virusreport
```

fmupdate av-ips

Use these commands to view AV/IPS update settings.

Syntax

```
get fmupdate av-ips advanced-log
get fmupdate av-ips fct server-override
get fmupdate av-ips fgt server-override
get fmupdate av-ips push-override
get fmupdate av-ips push-override-to-client
get fmupdate av-ips update-schedule
get fmupdate av-ips web-proxy
```

Example

This example shows the output for `get fmupdate av-ips web-proxy`:

```
ip : 0.0.0.0
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

fmupdate custom-url-list

Use this command to view the custom URL database.

Syntax

```
get fmupdate custom-url-list
```

fmupdate device-version

Use this command to view device version objects.

Syntax

```
get fmupdate device-version
```

Example

This example shows the output for `get fmupdate device-version`:

```
faz : 4.0 5.0
fct : 4.0 5.0
fgt : 3.0 4.0 5.0
fml : 3.0 4.0 5.0
fsa :
fsw :
```

fmupdate disk-quota

Use this command to view the disk quota for the update manager.

Syntax

```
get fmupdate disk-quota
```

fmupdate fct-services

Use this command to view FortiClient update services configuration.

Syntax

```
get fmupdate fct-services
```

Example

This example shows the output for `get fmupdate fct-services`:

```
status : enable
port : 80
```

fmupdate fds-setting

Use this command to view FDS parameters.

Syntax

```
get fmupdate fds-setting
```

Example

This example shows the output for `get fmupdate fds-setting:`

```
fds-pull-interval : 10
max-av-ips-version : 20
```

fmupdate multilayer

Use this command to view multilayer mode configuration.

Syntax

```
get fmupdate multilayer
```

fmupdate publicnetwork

Use this command to view public network configuration.

Syntax

```
get fmupdate publicnetwork
```

fmupdate server-access-priorities

Use this command to view server access priorities.

Syntax

```
get fmupdate server-access-priorities
```

Example

This example shows the output for `get fmupdate server-access-priorities:`

```
access-public : disable
av-ips : disable
private-server:
web-spam : enable
```

fmupdate server-override-status

Use this command to view server override status configuration.

Syntax

```
get fmupdate server-override status
```

fmupdate service

Use this command to view update manager service configuration.

Syntax

```
get fmupdate service
```

Example

This example shows the output for `get fmupdate service`:

```
avips : enable
query-antispam : disable
query-antivirus : disable
query-filequery : disable
query-webfilter : disable
use-cert : BIOS
webfilter-https-traversal : disable
```

fmupdate support-pre-fgt43

Use this command to view support for pre-fgt43 configuration.

Syntax

```
get fmupdate support-pre-fgt43
```

fmupdate web-spam

Use these commands to view web spam configuration.

Syntax

```
get fmupdate web-spam fct server-override
get fmupdate web-spam fgd-log
get fmupdate web-spam fgd-setting
get fmupdate web-spam fgt server-override
get fmupdate web-spam poll-frequency
get fmupdate web-spam web-proxy
```

Example

This example shows the output for `get fmupdate web-spam web-proxy`:

```
ip : 0.0.0.0
ip6 : ::
mode : proxy
password : *
port : 80
status : disable
```

```
username : (null)
```

system admin

Use these commands to view admin configuration.

Syntax

```
get system admin group <group name>
get system admin ldap <server entry name>
get system admin profile <profile ID>
get system admin radius <server entry name>
get system admin setting
get system admin tacacs <server entry name>
get system admin user <username>
```

Example

This example shows the output for `get system admin setting`:

```
access-banner : disable
admin-https-redirect: enable
admin-login-max : 256
admin_server_cert : server.crt
allow_register : disable
auto-update : enable
banner-message : (null)
device_sync_status : enable
http_port : 80
https_port : 443
idle_timeout : 15
install-ifpolicy-only: disable
mgmt-addr : (null)
mgmt-fqdn : (null)
offline_mode : disable
register_passwd : *
shell-password : *
show-add-multiple : disable
show-adom-devman : disable
show-adom-vpnman : enable
show-checkbox-in-table: disable
show-device-import-export: disable
show_automatic_script: disable
show_grouping_script: disable
show_schedule_script: disable
show_tcl_script : disable
unreg_dev_opt : add_allow_service
webadmin_language : auto_detect
```

system alert-console

Use this command to view alert console information.

Syntax

```
get system alert-console
```

Example

This example shows the output for `get system alert-console`:

```
period : 7
severity-level : emergency
```

system alertemail

Use this command to view alert email configuration.

Syntax

```
get system alertemail
```

Example

This example shows the output for `get system alertemail`:

```
authentication : enable
fromaddress : (null)
fromname : (null)
smtppassword : *
smtpport : 25
smtpserver : (null)
smtpuser : (null)
```

system alert-event

Use this command to view alert event information.

Syntax

```
get system alert-event <alert name>
```

system auto-delete

Use this command to view automatic deletion policies for logs, reports, archived and quarantined files.

Syntax

```
get system auto-delete
```

system backup

Use the following commands to view backups:

Syntax

```
get system backup all-settings
get system backup status
```

Example

This example shows the output for `get system backup status`:

```
All-Settings Backup
Last Backup: Tue Jan 15 16:55:35 2013
Next Backup: N/A
```

system certificate

Use these commands to view certificate configuration.

Syntax

```
get system certificate ca <certificate name>
get system certificate crl <crl name>
get system certificate local <certificate name>
get system certificate oftp <certificate name>
get system certificate ssh <certificate name>
```

Example

This example shows the output for `get system certificate local Fortinet_Local`:

```
name : Fortinet_Local
password : *
comment : Default local certificate
private-key :
certificate :
  Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN
    = FMG-VM0000000000, emailAddress = support@fortinet.com
  Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
    Authority, CN = support, emailAddress = support@fortinet.com
  Valid from: 2011-11-08 23:12:50 GMT
  Valid to: 2038-01-19 03:14:07 GMT
  Fingerprint:
  Root CA: No
  Version: 3
  Serial Num:
    01:cc:97
  Extensions:
    Name: X509v3 Basic Constraints
    Critical: no
    Content:
    CA:FALSE
```

```
csr :
```

system dm

Use this command to view device manager information on your FortiManager unit.

Syntax

```
get system dm
```

Example

This example shows the output for `get system dm`:

```
concurrent-install-limit: 480
concurrent-install-script-limit: 480
discover-timeout : 6
dpm-logsize : 10000
fgfm-sock-timeout : 360
fgfm_keepalive_itvl : 120
force-remote-diff : disable
fortiap-refresh-itvl: 60
max-revs : 100
nr-retry : 1
retry : enable
retry-intvl : 15
rollback-allow-reboot: disable
script-logsize : 100
verify-install : enable
```

system dns

Use this command to view DNS configuration.

Syntax

```
get system dns
```

system fips

Use this command to view FIPS configuration.

Syntax

```
get system fips
```

system global

Use this command to view global configuration.

Syntax

```
get system global
```

Example

This example shows the output for `get system global`:

```
admin-https-pki-required: disable
admin-lockout-duration: 60
admin-lockout-threshold: 3
admin-maintainer : enable
adom-mode : normal
adom-rev-auto-delete: by-revisions
adom-rev-max-revisions: 120
adom-status : enable
auto-register-device: enable
clt-cert-req : disable
console-output : standard
country-flag : enable
create-revision : disable
daylightsavetime : enable
default-disk-quota : 1000
enc-algorithm : low
faz-status : enable
hostname : FMG-VM64
language : english
ldapconntimeout : 60000
log-checksum : none
max-running-reports : 1
partial-install : disable
pre-login-banner : disable
remoteauthtimeout : 10
search-all-adoms : disable
ssl-low-encryption : enable
ssl-protocol : tlsv1
task-list-size : 2000
timezone : (GMT-8:00) Pacific Time (US & Canada).
vdom-mirror : disable
webservice-proto : tlsv1
workspace-mode : disabled
```

system ha

Use this command to view HA configuration.

Syntax

```
get system ha
```

Example

This example shows the output for `get system ha`:

```
clusterid : 1
file-quota : 4096
hb-interval : 5
hb-lost-threshold : 3
mode : standalone
password : *
peer:
```

system interface

Use this command to view interface configuration.

Syntax

```
get system interface
```

Example

This example shows the output for `get system interface`:

```
== [ port1 ]
name: port1 status: up ip: 172.172.172.222 255.255.0.0 speed: auto
== [ port2 ]
name: port2 status: up ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port3 ]
name: port3 status: up ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port4 ]
name: port4 status: up ip: 1.1.1.1 255.255.255.255 speed: auto
```

This example shows the output for `get system interface port1`:

```
name : port1
status : up
ip : 172.172.172.222 255.255.255.0
allowaccess : ping https ssh telnet http
serviceaccess :
speed : auto
description : (null)
alias : (null)
ipv6:
  ip6-address: ::/0 ip6-allowaccess:
```

system locallog

Use these commands to view local log configuration.

Syntax

```
get system locallog disk filter
get system locallog disk setting
```

```
get system locallog fortianalyzer filter
get system locallog fortianalyzer setting
get system locallog memory filter
get system locallog memory setting
get system locallog [syslogd | syslogd2 | syslogd3] filter
get system locallog [syslogd | syslogd2 | syslogd3] setting
```

Example

This example shows the output for `get system locallog disk setting`:

```
status : enable
severity : debug
upload : disable
server-type : FTP
max-log-file-size : 100
roll-schedule : none
diskfull : overwrite
log-disk-full-percentage: 80
```

system log

Use these commands to view log configuration.

Syntax

```
get system log alert
get system log fortianalyzer
get system log settings
```

Example

This example shows the output for `get system log settings`:

```
FAZ-custom-field1 : (null)
FCH-custom-field1 : (null)
FCT-custom-field1 : (null)
FDD-custom-field1 : (null)
FGT-custom-field1 : (null)
FMG-custom-field1 : (null)
FML-custom-field1 : (null)
FSA-custom-field1 : (null)
FWB-custom-field1 : (null)
download-max-logs : 500000
ha-auto-migrate : diasble
log-file-archive-name : basic
rolling-regular:
sync-search-timeout : 60
```

system log fetch

Use these commands to fetch logs.

Syntax

```
get system log-fetch
    server-profile
    client profile
```

Example

This example shows the output for `get system log-fetch`:

```
server-profile
client-profile
```

system loglimits

Use this command to view loglimits on your FortiManager unit.

Syntax

```
get system loglimits
```

| Information | Description |
|--------------------|-----------------------------|
| GB/day | Number of GBs used per day. |
| Peak Log Rate | Peak time of log rates. |
| Sustained Log Rate | Log rate average. |

system mail

Use this command to view alert email configuration.

Syntax

```
get system mail <server name>
```

system metadata

Use this command to view metadata configuration.

Syntax

```
get system metadata <admin name>
```

system ntp

Use this command to view NTP configuration.

Syntax

```
get system ntp
```

system password-policy

Use this command to view the password policy setting on your FortiAnalyzer.

Syntax

```
get system password-policy
```

Example

This example shows the output for `get system password-policy`:

```
status : enable
minimum-length : 11
must-contain : upper-case-letter lower-case-letter number non-alphanumeric
change-4-characters : disable
expire : 30
```

system performance

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

Syntax

```
get system performance
```

Example

This example shows the output for `get system performance`:

```
CPU:
  Used: 3.3%
  Used(Excluded NICE): 3.3%
  CPU_num: 1.
  CPU[0] usage: 3.03%
    Usage: %user %nice %sys %idle %iowait %irq %softirq
           2.52 0.00 0.45 96.97 0.00 0.00 0.05
Memory:
  Total: 4,136,236 KB
  Used: 819,164 KB 19.8%
Hard Disk:
  Total: 82,557,616 KB
  Used: 2,660,504 KB 3.2%
```

```
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
        2.8 0.1 2.7 2.9 58.9 0.0 7.7 0.7 0.2 7321.13
Flash Disk:
Total: 516,040 KB
Used: 87,960 KB 17.0%
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
        0.0 0.0 0.0 0.0 0.1 0.0 4.4 3.7 0.0 7321.17
```

system report

Use this command to view report configuration.

Syntax

```
get system report auto-cache
get system report est-browse-time
get system report setting
```

Example

This example shows the output for `get system report auto-cache`:

```
aggressive-drilldown: disable
aggressive-schedule : disable
drilldown-interval  : 168
drilldown-status    : enable
order : latest-first
status : enable
```

system route

Use this command to view IPv4 routing table configuration.

Syntax

```
get system route <entry number>
```

system route6

Use this command to view IPv6 routing table configuration.

Syntax

```
get system route6 <entry number>
```

system snmp

Use these commands to view SNMP configuration.

Syntax

```
get system snmp community <community ID>
get system snmp sysinfo
get system snmp user <SNMP user name>
```

Example

This example shows the output for `get system snmp sysinfo`:

```
contact_info : (null)
description : (null)
engine-id : (null)
location : (null)
status : disable
trap-cpu-high-exclude-nice-threshold: 80
trap-high-cpu-threshold: 80
trap-low-memory-threshold: 80
```

system sql

Use this command to view SQL configuration.

Syntax

```
get system sql
```

Example

This example shows the output for `get system sql`:

```
custom-index:
prompt-sql-upgrade : enable
status : local
text-search-index : disable
ts-index-field:
== [ FGT-app-ctrl ]
category: FGT-app-ctrl value:
    user,group,srcip,dstip,dstport,service,app,action,hostname
== [ FGT-attack ]
category: FGT-attack value: severity,srcip,dstip,action,user,attack
== [ FGT-content ]
category: FGT-content value: from,to,subject,action,srcip,dstip,hostname,status
== [ FGT-dlp ]
category: FGT-dlp value: user,srcip,service,action,filename
== [ FGT-emailfilter ]
category: FGT-emailfilter value: user,srcip,from,to,subject
== [ FGT-event ]
category: FGT-event value: subtype,ui,action,msg
== [ FGT-traffic ]
category: FGT-traffic value: user,srcip,dstip,service,app,utmaction
== [ FGT-virus ]
category: FGT-virus value: service,srcip,dstip,action,filename,virus,user
== [ FGT-voip ]
category: FGT-voip value: action,user,src,dst,from,to
== [ FGT-webfilter ]
```

```

category: FGT-webfilter value: user,srcip,dstip,service,action,catdesc,hostname
== [ FGT-netscan ]
category: FGT-netscan value: user,dstip,vuln,severity,os
== [ FML-emailfilter ]
category: FML-emailfilter value: client_name,dst_ip,from,to,subject
== [ FML-event ]
category: FML-event value: subtype,msg
== [ FML-history ]
category: FML-history value: classifier,disposition,from,to,client_
      name,direction,domain,virus
== [ FML-virus ]
category: FML-virus value: src,msg,from,to
== [ FWB-attack ]
category: FWB-attack value: http_host,http_url,src,dst,msg,action
== [ FWB-event ]
category: FWB-event value: ui,action,msg
== [ FWB-traffic ]
category: FWB-traffic value: src,dst,service,http_method,msg
background-rebuild : enable
database-type : postgres
device-count-high : disable
event-table-partition-time: 0
fct-table-partition-time: 1440
logtype : app-ctrl attack content dlp emailfilter event generic history traffic virus
      voip webfilter netscan fct-event fct-traffic fct-netscan
rebuild-event : enable
rebuild-event-start-time: 00:00 2000/01/01
start-time : 00:00 2000/01/01
traffic-table-partition-time: 0
utm-table-partition-time: 0

```

system status

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

Syntax

```
get system status
```

Example

This example shows the output for `get system status`:

```

Platform Type : FMG-VM64
Platform Full Name : FortiManager-VM64
Version : v5.4.0-build0926 150630 (Beta 1)
Serial Number : FMG-VM0000000000
BIOS version : 04000002
Hostname : FMG-VM64
Max Number of Admin Domains : 10
Max Number of Device Groups : 10
Admin Domain Configuration : Enabled
HA Mode : Stand Alone
Branch Point : 926
Release Version Information : Beta 1

```

```
Current Time : Thu Jul 02 14:03:14 PDT 2015
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 76.20GB, Total 78.73GB
File System : Ext4
License Status : Valid
```

system syslog

Use this command to view syslog information.

Syntax

```
get system syslog <syslog server name>
```

system workflow

Use this command to view workflow information.

Syntax

```
get system workflow approval-matrix <ADOM_name>
```

show

The `show` commands display a part of your Fortinet unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.



Although not explicitly shown in this section, for all `config` commands, there are related `show` commands that display that part of the configuration. The `show` commands use the same syntax as their related `config` command.



CLI commands and variables are case sensitive.

Unlike the `get` command, `show` does not display settings that are assumed to remain in their default state.

Appendix A - CLI Error Codes

Some FortiManager CLI commands issue numerical error codes. The following table lists the error codes and descriptions.

| Error Code | Description |
|------------|---|
| 0 | Success |
| 1 | Function called with illegal parameters |
| 2 | Unknown protocol |
| 3 | Failed to connect host |
| 4 | Memory failure |
| 5 | Session failure |
| 6 | Authentication failure |
| 7 | Generic file transfer failure |
| 8 | Failed to access local file |
| 9 | Failed to access remote file |
| 10 | Failed to read local file |
| 11 | Failed to write local file |
| 12 | Failed to read remote file |
| 13 | Failed to write remote file |
| 14 | Local directory failure |
| 15 | Remote directory failure |



FORTINET

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.