FortiManager & FortiAnalyzer - Event Log Reference

VERSION 5.6.0

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

July 27, 2017

FortiManager & FortiAnalyzer 5.6.0 Event Log Reference

05-560-438656-20170727

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-07-27	Initial release.

Introduction

This reference provides detailed information about FortiManager & FortiAnalyzer log messages. This reference is intended for administrators that have enabled, and configured local logging on their FortiManager & FortiAnalyzer devices. The log types described in this document report log information useful for system administrators when recording, monitoring, and tracing the operation of FortiManager & FortiAnalyzer devices.

Log types and sub types

FortiManager log types and subtypes

FortiManager logs have only one log type and nine subtypes. The type and subtype numbers are combined in the `log_id` field. There are ten numbers; the first two identify the type of log, and the second two numbers identify the subtype. The last five numbers identify the log. For example, a Policy console log message contains the numbers 31001.

The following table includes only the log types that are supported by the FortiManager unit.

Type	Description	Sub Type	Subtype Category Number
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	System Manager	00
		FortiGuard-FortiManager protocol (fgfm)	01
		Script Manager	04
		Web Portal	05
		Policy Console	07
		Deployment Manager	11
		Real-Time Monitor	12
		High Availability (HA)	14
		FortiGuard Service	16
		Object Change (objcfg)	20
		Device Manager (dvm)	21

FortiAnalyzer log types and subtypes

The following table includes only the log types that are supported by the FortiAnalyzer unit.

Type	Description	Sub Type	Subtype Category Number
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	Admin	04
		Config	00
		Ipsec	01
		System	06

Log messages

All FortiAnalyzer and FortiManager log messages are comprised of a log header and a log body. The log header contains information that identifies the log type and subtype, along with the log message identification number, date and time. The log body contains information on where the log was recorded and what triggered the FortiManager unit to record the log.

FortiManager example:

```
2013-04-02 12:44:21 log_id=0016058001 type=event subtype=fgd
pri=information user=user_2 msg="Receive an update package from FDS,
type=OBLT00000, version=00000.00000-090571930"
```

Log message breakdown

Log Field	Description
Date: `2013-04-02`	The year, month, and day when the event occurred in the format: YY-MM-DD
Time: `12:44:21`	The hour, minute and second of when the event occurred.
Log ID: `0016058001`	A ten-digit number that identifies the log type. The first two digits represent the log type, and the following two digits represent the log subtype. The last five digits is the message ID number.
Type: `event`	The section of the system where the event occurred.
Subtype: `fgd`	The subtype of each log message.

Log Field	Description
Pri: `information`	The severity level, or priority, or the event. There are six ;priority severity levels.
User: `user_2`	The name of the user creating the traffic.
Msg: `Receive an update package from FDS, type=OBLT0000, version=00000.00000-090571930`	Explains the activity or event that the FortiManager unit recorded.

FortiAnalyzer example:

```
date=2009-12-22 time=13:15:01 log_id=0100000045 type=event subtype=config
pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.20.120.46)
action=config msg="User deleted device 'FGT5002803033050'"
```

Log message breakdown

Log Field	Description
Date: `2009-12-22`	The year, month, and day when the event occurred in the format: YY-MM-DD
Time: `13:15:01`	The hour, minute and second of when the event occurred.
Log ID: `0100000045`	A ten-digit number that identifies the log type. The first two digits represent the log type, and the following two digits represent the log subtype. The last five digits is the message ID number.
Type: `event`	The section of the system where the event occurred.
Subtype: `config`	The subtype of each log message.
Pri: `warning`	The severity level, or priority, or the event. There are six priority severity levels.
User: `admin`	The name of the user creating the traffic.
Msg: `User deleted device 'FGT5002803033050`	Explains the activity or event that the FortiAnalyzer unit recorded.

Priority levels

When a logging severity level is defined, the FortiManager unit logs all messages at and above the selected severity level. For example, if you select Error, the FortiManager unit logs Error, Critical, Alert, and Emergency

level messages.

The Debug log severity level is rarely used. Debug log messages are useful when the FortiManager is not functioning properly. Debug log messages are only generated if the log severity level is set to Debug. Debug log messages are generated by all subtypes of the event log.

Level (0 is highest)	Name	Description
0	Emergency	The system is unusable or not responding.
1	Alert	Immediate action required. Used in security logs.
2	Critical	Functionality is affected.
3	Error	An error exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notification	Information about normal events.
6	Information	General information about system operations. Used in event logs to record configuration changes.
7	Debug	Detailed information useful for debugging purposes.

FortiManager 5.6 Log Messages

The following tables list the FortiManager 5.6 log messages.

Event

DEVCFG

Log Field Name	Description	Data Type	Length
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64

DEVCFG Log Messages

The following table describes the log message IDs and messages of the DEVCFG log.

Message ID	Message	Severity
12002	LOG_ID_installcmd	Notice

DEVOPS

Log Field Name	Description	Data Type	Length
date	Date	string	10
device	Name of the Device	string	64
log_id	Log ID	uint32	10

Log Field Name	Description	Data Type	Length
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

DEVOPS Log Messages

The following table describes the log message IDs and messages of the DEVOPS log.

Message ID	Message	Severity
36002	LOG_ID_reboot	Critical
36003	LOG_ID_shutdown	Critical

DM

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
adom_oid	The OID of target ADOM	uint64	20
condition	DVM Dev Condition	string	9
confstatus	Conf Sync Status	string	128
connect_status	Status of connection to the device	string	7
constmsg	Constant Message	string	256
date	Date	string	10
dbstatus	DVM Device Status	string	128
device	Name of the Device	string	64

Log Field Name	Description	Data Type	Length
dev_oid	The OID of Target Device	uint64	20
dmstate	dvm dm states	string	12
instpkg	Name of Policy Package which is installed	string	64
log_id	Log ID	uint32	10
msg	Message	string	1024
pkg	Name of Policy Package which is installed	string	64
pkg_oid	The OID of the package to be installed	uint64	20
pri	Priority	string	11
result	The result of the operation	string	128
revision	The ID of the revision that is operated	uint64	20
script	Name of the script	string	128
serial	Serial Number of the device	string	32
status	Operation Result	string	4
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64
ustr	Extra log information	string	512
vdom	Virtual Domain of a device	string	128
vdoms	List of vdoms to which revision is installed	string	1024

DM Log Messages

The following table describes the log message IDs and messages of the DM log.

Message ID	Message	Severity
21002	LOG_ID_update_n_export_db	Error
21004	LOG_ID_schedule_install_adom	Information
21005	LOG_ID_schedule_install_global	Information
21006	LOG_ID_schedule_install_device	Information
21007	LOG_ID_install_script	Information
21008	LOG_ID_update_and_save	Information
21009	LOG_ID_cfg_checkin	Notice
21010	LOG_ID_cfg_retrieve	Notice
21011	LOG_ID_cfg_import	Notice
21012	LOG_ID_cfg_sync	Notice
21013	LOG_ID_cfg_edit	Notice
21014	LOG_ID_cfg_revert	Notice
21015	LOG_ID_cfg_install	Notice
21016	LOG_ID_cfg_delrev	Notice
21017	LOG_ID_cfg_download	Notice
21018	LOG_ID_dev_state	Information
21019	LOG_ID_adom_rev_import_info	Information
21020	LOG_ID_adom_rev_import_error	Error
21021	LOG_ID_add_fortiap	Notice
21022	LOG_ID_connect_status	Alert
21023	LOG_ID_policy_package_install	Information
21024	LOG_ID_policy_package_install_failure	Error
21025	LOG_ID_cfg_install_preview	Notice

DVM

Log Field Name	Description	Data Type	Length
action	Action towards this device	string	6
adom	The name of Admin ADOM	string	64
date	Date	string	10
device	Name of the Device	string	64
dvm_adom	The name of ADOM which contains target device	string	64
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

DVM Log Messages

The following table describes the log message IDs and messages of the DVM log.

Message ID	Message	Severity
31002	LOG_ID_dev_reload	Notice
31003	LOG_ID_generic_info	Information
31004	LOG_ID_dvmlog_emerg	Emergency
31005	LOG_ID_dvmlog_alert	Alert
31006	LOG_ID_dvmlog_critical	Critical
31007	LOG_ID_dvmlog_error	Error
31008	LOG_ID_dvmlog_warning	Warning

Message ID	Message	Severity
31009	LOG_ID_dvmlog_notif	Notice
31010	LOG_ID_dvmlog_info	Information
31011	LOG_ID_dvmlog_debug	Debug

FAZ

Log Field Name	Description	Data Type	Length
action	Action of faz log	string	6
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

FAZ Log Messages

The following table describes the log message IDs and messages of the FAZ log.

Message ID	Message	Severity
33002	LOG_ID_add_device	Information
33003	LOG_ID_aggregation	Information
33004	LOG_ID_del_archive	Warning
33005	LOG_ID_del_log	Warning
33006	LOG_ID_log	Notice

Message ID	Message	Severity
33007	LOG_ID_report	Information
33008	LOG_ID_sql	Information
33009	LOG_ID_send_mail	Information
33010	LOG_ID_upgrade	Information
33011	LOG_ID_upload	Notice
33012	LOG_ID_generic	Information
33013	LOG_ID_daemon_suspended	Emergency
33014	LOG_ID_daemon_resumed	Notice
33015	LOG_ID_license_limit	Warning
33016	LOG_ID_device_offline	Warning
33017	LOG_ID_device_online	Notice
33018	LOG_ID_QUOTA_ABNORMAL	Warning
33019	LOG_ID_cdb_obj_change	Information
33020	LOG_ID_cdb_obj_change_failure	Warning
33021	LOG_ID_log_ratelimit	Alert

FGD

Log Field Name	Description	Data Type	Length
constmsg	Constant Message	string	256
date	Date	string	10
dbver	The Service Database Version	string	32
expiration	Expiration Time of the License	uint64	20
file	Filename of package to be imported or exported	string	128
license_type	License Type	uint8	3

Log Field Name	Description	Data Type	Length
log_id	Log ID	uint32	10
msg	Message	string	1024
new_version	New available version of the requested object	string	64
object	Filename of the requested object	string	256
package_desc		string	20
package_type	Identifier of Package Type	string	64
pre_version	Previous version of the requested object	string	64
pri	Priority	string	11
quota	Disk Quota Ratio in Percentage	uint8	3
rate	How many requests are handled per minute	uint64	20
remote_host		string	128
remote_ip	Remote Peer IP in String Presentation	string	64
remote_port	Remote Peer Port Number	uint16	5
rundb_ver	Version of the Running Database	string	32
serial	Serial Number of the device	string	32
service	Name of the starting service	string	128
setup	Whether it needs to setup or not	uint8	3
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
uid	UID of a FortiClient installation	string	64
upddb_ver	Version of the updating database	string	32
url	Webfiltering requested URL	string	1024
user	User Name	string	64

Log Field Name	Description	Data Type	Length
version	The new version of updated object	string	32
whitelist_size	The size of white list table	string	32

FGD Log Messages

The following table describes the log message IDs and messages of the FGD log.

Message ID	Message	Severity
26002	LOG_ID_fmupdate_info	Information
26003	LOG_ID_fmupdate_error	Error
26004	LOG_ID_config	Information
26005	LOG_ID_linkdcmd	Information
26006	LOG_ID_recv_connect_request	Information
26007	LOG_ID_recv_update_request	Information
26008	LOG_ID_send_announcement	Information
26009	LOG_ID_recv_update_response	Information
26010	LOG_ID_send_uppull_request	Error
26011	LOG_ID_append_subscriber	Information
26012	LOG_ID_disk_quota	Critical
26013	LOG_ID_uppull_error	Error
26014	LOG_ID_fguard_throughput	Information
26015	LOG_ID_url_hit	Debug
26016	LOG_ID_url_miss	Warning
26017	LOG_ID_spam	Warning
26018	LOG_ID_nonspam	Warning
26019	LOG_ID_fgdsvr_service	Debug
26020	LOG_ID_fgdsvr_statistic	Debug

Message ID	Message	Severity
26021	LOG_ID_fgdsvr_license	Warning
26022	LOG_ID_fgdsvr_debug	Debug
26023	LOG_ID_fgdsvr_warning	Warning
26024	LOG_ID_fgdsvr_error	Warning
26025	LOG_ID_fgdsvr_db_update	Warning

FGFM

Log Field Name	Description	Data Type	Length
date	Date	string	10
device	Name of the Device	string	64
log_id	Log ID	uint32	10
msg	Message	string	1024
offline_stat	Offline Mode Enabled or Disabled	string	8
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64

FGFM Log Messages

The following table describes the log message IDs and messages of the FGFM log.

Message ID	Message	Severity
11002	LOG_ID_connection_up	Information
11003	LOG_ID_connection_down	Warning
11004	LOG_ID_offline_mode	Alert

FIPS

Log Field Name	Description	Data Type	Length
constmsg	Constant Message	string	256
date	Date	string	10
fips_err	FIPS test error code	string	12
fips_method	FIPS self-test method	string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
operstat	Operation Result	string	12
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64
when	FIPS test stage	string	7

FIPS Log Messages

The following table describes the log message IDs and messages of the FIPS log.

Message ID	Message	Severity
34002	LOG_ID_error_mode	Emergency
34003	LOG_ID_enable_fips_mode	Notice
34004	LOG_ID_self_test	Notice
34005	LOG_ID_encryption	Alert
34006	LOG_ID_decryption	Alert
34007	LOG_ID_prng	Alert

FMGWS

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
constmsg	Constant Message	string	256
date	Date	string	10
log_id	Log ID	uint32	10
pri	Priority	string	11
remote_host	Remote Host Name or Host IP in string presentation	string	128
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64

FMGWS Log Messages

The following table describes the log message IDs and messages of the FMGWS log.

Message ID	Message	Severity
32002	LOG_ID_connection	Error
32003	LOG_ID_login_notif	Notice
32004	LOG_ID_login_error	Error

FMWMGR

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024

Log Field Name	Description	Data Type	Length
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

FMWMGR Log Messages

The following table describes the log message IDs and messages of the FMWMGR log.

Message ID	Message	Severity
25002	LOG_ID_emerg	Emergency
25003	LOG_ID_alert	Alert
25004	LOG_ID_critical	Critical
25005	LOG_ID_error	Error
25006	LOG_ID_warning	Warning
25007	LOG_ID_notif	Notice
25008	LOG_ID_info	Information
25009	LOG_ID_debug	Debug

GLBCFG

Log Field Name	Description	Data Type	Length
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64

GLBCFG Log Messages

The following table describes the log message IDs and messages of the GLBCFG log.

Message ID	Message	Severity
13002	LOG_ID_installcmd	Notice

HA

Log Field Name	Description	Data Type	Length
cause	Reason that causes HA status down	string	256
constmsg	Constant Message	string	256
date	Date	string	10
log_id	Log ID	uint32	10
module	Identifier of the HA Sync Module	uint32	10
msg	Message	string	1024
operstat	Operation Result	string	12
peer	Serial Number of HA peer	string	32
pri	Priority	string	11
status	HA status	string	4
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14

HA Log Messages

The following table describes the log message IDs and messages of the HA log.

Message ID	Message	Severity
24002	LOG_ID_status_chg_up	Information
24003	LOG_ID_status_chg_down	Alert
24004	LOG_ID_sync_info	Information
24005	LOG_ID_sync_alert	Alert
24006	LOG_ID_app_sync	Error
24007	LOG_ID_peer_status	Information
24008	LOG_ID_image_upgrade	Information

IOLOG

Log Field Name	Description	Data Type	Length
date	Date	string	10
function	The name of the Function Call	string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
pid	Process ID	uint64	20
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

IOLOG Log Messages

The following table describes the log message IDs and messages of the IOLOG log.

Message ID	Message	Severity
29002	LOG_ID_system_keymsg	Debug

LOGD

Log Field Name	Description	Data Type	Length
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64

LOGD Log Messages

The following table describes the log message IDs and messages of the LOGD log.

Message ID	Message	Severity
35002	LOG_ID_log_view_notif	Notice
35003	LOG_ID_logdaemon_updown_notif	Notice

OBJCFG

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

OBJCFG Log Messages

The following table describes the log message IDs and messages of the OBJCFG log.

Message ID	Message	Severity
30002	LOG_ID_cdbevlog	Notice

RTMON

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

RTMON Log Messages

The following table describes the log message IDs and messages of the RTMON log.

Message ID	Message	Severity
22002	LOG_ID_debug	Debug

SCPLY

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
date	Date	string	10
detail	The task details	string	256
errno	The Error Code of the task	uint8	3
inst_adom	The name of ADOM which contains target device	string	64
inst_dev	The name of device on which policy is installed	string	64
log_id	Log ID	uint32	10
msg	Message	string	1024
percent	The percentage of this task being running	uint8	3
pkgadom	Name of ADOM to which this global policy package is assigned	string	64
ppkgname	Name of the global policy package that is assigned	string	128
pri	Priority	string	11
state	The state of the task	string	64
subtype	Log Subtype	string	7
time	Time	string	8
title	The task title	string	64
type	Log Type	string	14
user	User Name	string	64

SCPLY Log Messages

The following table describes the log message IDs and messages of the SCPLY log.

Message ID	Message	Severity
17002	LOG_ID_task_error	Error
17003	LOG_ID_task_debug	Debug
17004	LOG_ID_install_policy	Information
17005	LOG_ID_generic_error	Error
17006	LOG_ID_global_policy_package	Information

SCRMGR

Log Field Name	Description	Data Type	Length
date	Date	string	10
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

SCRMGR Log Messages

The following table describes the log message IDs and messages of the SCRMGR log.

Message ID	Message	Severity
14002	LOG_ID_scm2	Information

SYSTEM

Log Field Name	Description	Data Type	Length
address	IP address of login user	string	32

Log Field Name	Description	Data Type	Length
adminprof	Login User Admin Profile	string	64
adom	The name of Admin ADOM	string	64
adomlock	Name of adom which is locked/unlocked	string	64
attrname	Variable name of which value is changed	string	64
authmsg	SSH Authentication Message.	string	512
capacity	The percentage of Memory Capacity is used	uint8	3
category	Log Category	string	9
certname	Name of Certificate	string	64
certtype	Type of Certificate	string	27
cli_act	CLI Command Action	string	6
cmd_from	CLI Command From	string	8
comment	The description of this policy package	string	128
constmsg	Constant Message	string	256
date	Date	string	10
date_time	String Representation of date and time in Local Timezone	string	128
devlog	Name of the Device	string	64
dev_oid	The OID of Target Device	uint64	20
disk_label	Raid Disk Label	uint8	3
disk_stat_before	RAID Disk Status Before Change	string	11
disk_stat_current	RAID Disk Status After Change	string	11
dvmdb_obj	dvm_db object type	string	15
extrainfo	SSH Authentication extra information	string	512
file	The name of log file that is rolling and uploaded	string	128
importance	dvm_db Metafield Mtype	string	8

Log Field Name	Description	Data Type	Length
instpkg	Name of Policy Package which is installed	string	64
intfname	Interface Name	string	32
lickey_type	License Key Type	string	13
lnk_path	The name of the link file being transferred to the server	string	128
local_file	Local File include its path	string	128
log_id	Log ID	uint32	10
log_path	The original log file	string	128
log_size	The size of log file that is rolling and uploaded	uint64	20
max_mb	License Allowed Maximum Capacity in MB	uint32	10
metafield	dvm_db Metafield Name	string	128
metafield_leng	dvm_db Metafield Value Size	uint16	5
metafield_stat	dvm_db Metafield Status	string	8
msg	Message	string	1024
newname	New object name being renamed to	string	128
new_value	String representation of vlaue after being changed	string	64
objattr	CMDB Config Object Attribute	string	64
objname	Object Name	string	128
objtype	Object Type	string	64
old_value	String representation of value before being changed	string	64
operstat	Operation Result	string	12
path	CMDB Config Object Path	string	256
pkgadom	Name of ADOM this policy package belongs to	string	64
pkgname	Name of the Policy Package which is locked/un-locked	string	128

Log Field Name	Description	Data Type	Length
power_stat	Power Supplier Status	string	7
ppkgname	Name of the Policy Package which is locked/un-locked	string	128
pri	Priority	string	11
profname	Device Profile Object Name	string	64
protocol	Transmission Protocol used to backup all settings	string	10
pty_err	pty operation errno	string	12
pty_oper	pty operation type, get or put	string	3
pty_sess	pty session server type	string	4
pty_step	pty operation step	string	13
raid_stat_before	RAID Status Before Change	string	23
raid_stat_current	RAID Status After Change	string	23
reboot_reason	The reason for system reboot	string	128
remote_filename	Remote Filename on server side	string	128
remote_ip	Remote Peer IP in String Presentation	string	64
remote_path	Remote Path on server side	string	128
remote_port	Remote Peer Port Number	uint16	5
rolling_cur_number	Log Rolling Number that currently reached	uint32	10
rolling_max_ allowed	Log Rolling Max Number that is allowed	uint32	10
shutdown_reason	The reason for system shutdown	string	128
sid	Session ID	uint32	10
state	Status	string	64
status	Interface Status	string	4
subtype	Log Subtype	string	7

Log Field Name	Description	Data Type	Length
supplier_id	Power Supplier ID	uint8	3
sw_version	Current Firmware Software Version	string	64
time	Time	string	8
to_build	The build no of the firmware that is upgraded to	uint16	5
to_release	The release of the firmware that is upgraded to	string	32
to_version	The version of the firmware that is upgraded to	string	32
type	Log Type	string	14
upgrade_adom	The name of ADOM to be upgraded	string	64
upgrade_from	The version, mr, build or branchpoint before upgrade	string	128
upgrade_to	The version, mr, build or branchpoint after upgrade	string	128
upg_act	Operation that is Failed	string	64
uploading_cur_number	The number of uploading process that currently reached	uint32	10
uploading_max_allowed	Max number of uploading process that is allowed	uint32	10
uploading_oper	Upload Operations	string	8
uploading_pid	Process ID of the uploading child process	uint64	20
uploading_server_type	The type of server that accepts the uploaded log	string	4
user	User Name	string	64
userfrom	Login Session User From	string	64
userid	pty operation login user id	string	64
user_type	Access restriction of session admin profile	string	8
use_mb	Used Capacity in MB	uint32	10
valid	If ssh user is valid or not	uint8	3
zip_path	The name of the gzip file being transferred to the server	string	128

SYSTEM Log Messages

The following table describes the log message IDs and messages of the SYSTEM log.

Message ID	Message	Severity
10002	LOG_ID_hwmon_intf	Warning
10003	LOG_ID_hwmon_raid_error	Error
10004	LOG_ID_hwmon_raid_info	Information
10005	LOG_ID_hwmon_raid_disk_error	Error
10006	LOG_ID_hwmon_raid_disk_info	Information
10007	LOG_ID_hwmon_power_status	Critical
10008	LOG_ID_hwmon_power_button	Critical
10009	LOG_ID_schedule_backup_notif	Notice
10010	LOG_ID_schedule_backup_warning	Warning
10011	LOG_ID_license_GB_trap	Critical
10012	LOG_ID_device_quota_trap	Debug
10013	LOG_ID_ssh_auth_profile	Alert
10014	LOG_ID_ssh_auth_login_failure	Alert
10015	LOG_ID_dvm_db	Notice
10016	LOG_ID_devprof_obj	Notice
10017	LOG_ID_policy_obj	Notice
10018	LOG_ID_login_info	Information
10019	LOG_ID_login_alert	Alert
10020	LOG_ID_pm_chkpoint	Notice
10021	LOG_ID_sessionmgr	Information
10022	LOG_ID_restart_upgrade	Critical
10025	LOG_ID_upgrade_failure	Critical

Message ID	Message	Severity
10026	LOG_ID_cli_command	Notice
10027	LOG_ID_reboot	Critical
10028	LOG_ID_shutdown	Critical
10029	LOG_ID_setting_changed	Notice
10030	LOG_ID_backup_all_settings	Critical
10031	LOG_ID_restore_all_settings	Critical
10032	LOG_ID_adom_lock	Information
10033	LOG_ID_fwm_upgrade	Information
10034	LOG_ID_policy_package_install	Information
10035	LOG_ID_log_rolling_reach_max	Emergency
10036	LOG_ID_log_rolling_uploading	Information
10037	LOG_ID_log_uploading_process_reach_max	Warning
10038	LOG_ID_log_uploading_info	Information
10039	LOG_ID_log_uploading_warning	Warning
10040	LOG_ID_lost_power_at	Critical
10041	LOG_ID_pty_operation	Warning
10042	LOG_ID_memlog_capacity_info	Information
10043	LOG_ID_memlog_capacity_warning	Warning
10049	LOG_ID_exec_shell	Information
10050	LOG_ID_exit_shell	Information
10051	LOG_ID_vm_license_changed	Notice
10052	LOG_ID_vm_license_invalid	Warning
10053	LOG_ID_export_ssl_cert	Notice
10054	LOG_ID_clean_local_log	Notice

Message ID	Message	Severity
10055	LOG_ID_cdb_upgrade	Notice
10056	LOG_ID_policy_package_lock	Information
10057	LOG_ID_policy_package_install_target_change	Notice
10058	LOG_ID_pm3_object_rename	Notice
10059	LOG_ID_image_upgrade	Critical
10060	LOG_ID_protocol_failed	Warning
10061	LOG_ID_lickey_changed	Notice
10062	LOG_ID_lickey_invalid	Warning
10063	LOG_ID_ssh_auth_login_accept	Information
10064	LOG_ID_check_integrity_error	Alert
10065	LOG_ID_adom_upgrade_info	Information
10066	LOG_ID_adom_upgrade_error	Error
10067	LOG_ID_check_integrity	Information
10068	LOG_ID_ssl_connect	Information
10069	LOG_ID_time_modified	Warning
10070	LOG_ID_disk_full	Warning
10071	LOG_ID_connect_debug	Debug
10072	LOG_ID_reset_all_settings	Critical

WEBPORT

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
date	Date	string	10
log_id	Log ID	uint32	10

Log Field Name	Description	Data Type	Length
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	7
time	Time	string	8
type	Log Type	string	14
user	User Name	string	64
userfrom	Login Session User From	string	64

WEBPORT Log Messages

The following table describes the log message IDs and messages of the WEBPORT log.

Message ID	Message	Severity
15002	LOG_ID_install	Information
15003	LOG_ID_notification	Notice

Appendix A: Log field diff - 5.4.3 and 5.6.0

Refer to the *FortiManager & Analyzer Event Log Reference Guide* for a complete list of log field details related to version 5.6. This section covers changes applicable to the 5.6.0 version only. It is recommended you keep both the 5.4.3 and 5.6.0 *FortiManager & FortiAnalyzer Event Log Reference Guides* available for a comparison of log field delta between the versions.

For all reference purposes, in the tables provided below (see tables) , the term **Removed** indicates a log field was removed in version 5.6.0 but exists in version 5.4.3. Similarly, the term **Added** indicates a log file was added in version 5.6.0 but does not exist in version 5.4.3.

There is no log field difference between 5.4.3 and 5.6.0.

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.