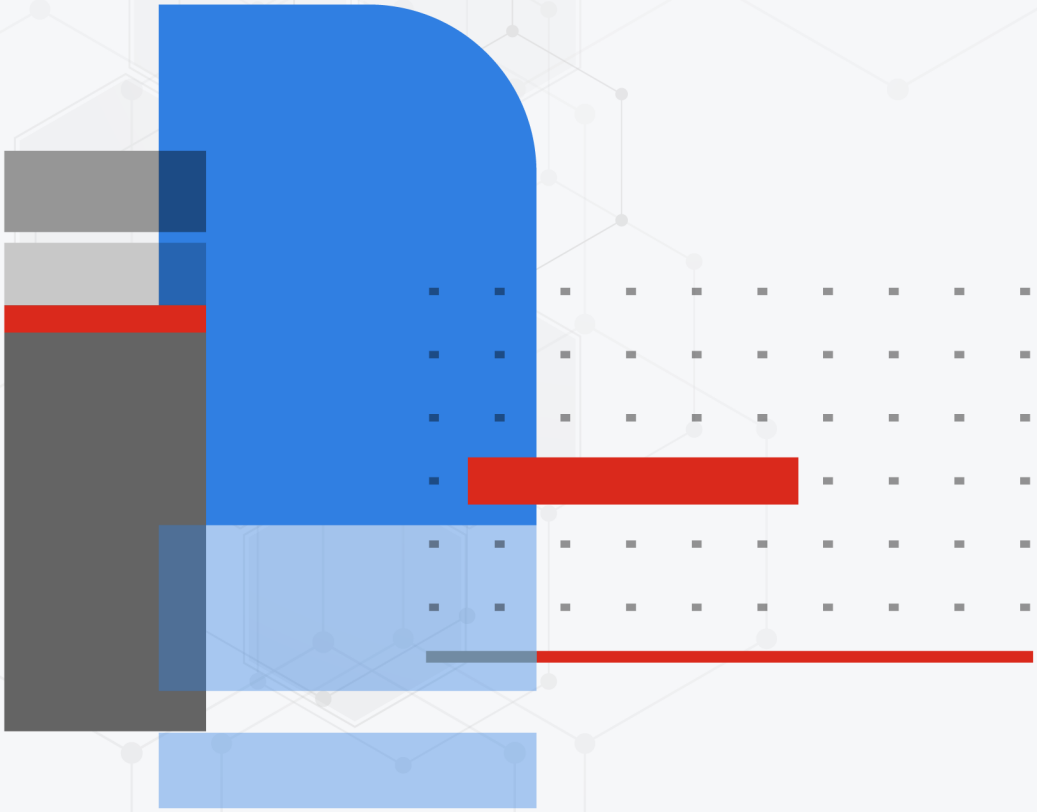
Log Reference

FortiManager & FortiAnalyzer 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 15, 2023
FortiManager & FortiAnalyzer 7.4.0 Log Reference
02-740-901298-20230515

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-05-15	Initial release of 7.4.0.

Introduction

This reference provides detailed information about FortiManager and FortiAnalyzer log messages. Log messages provide an audit log of actions made by users of FortiManager and FortiAnalyzer units. The information in this document is useful for system administrators when recording, monitoring, and tracing the operation of FortiManager and FortiAnalyzer units.

This section contains the following topics:

Log types and subtypes

FortiManager and FortiAnalyzer support the following log types:

Log Type	Description
Event	Supported by FortiManager and FortiAnalyzer.
Application	Supported by FortiAnalyzer. FortiAnalyzer applications such as incident management and automation playbooks generate local audit logs.

Each log type includes several subtypes.

The type, subtype, and message ID numbers are combined into a ten-digit `log_id` field, for example `log_id=0022031002`. The first two numbers identify the type of log, and the second two numbers identify the subtype. The last six numbers identify the message ID.

This section contains the following topics:

The message IDs displayed in this guide exclude the first digit of the message ID. The first digit is a zero (0). As a result, the message IDs in this guide display only the last 5 numbers. For example, the log message ID of 031002 displays as 31002 in this guide.

FortiManager log types and subtypes

The following table identifies the subtypes for the event log type that are supported by FortiManager. When FortiAnalyzer features are enabled on FortiManager, additional subtypes are supported. See FortiAnalyzer log types and subtypes on page 7.

Type	Description	Subtype	Subtype Category Number
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	System manager (system)	1
		FortiGate-FortiManager protocol (fgfm)	2
		Device configuration (devcfg)	3
		Global database (glbcfg)	4
		Script manager (scrmgr)	5
		Web portal (webport)	6
		Security console (scply)	8
		Deployment manager (dm)	12
		Real-time monitor (rtmon)	13
		High Availability (HA)	15
		Firmware manager (fmwmgr)	16
		FortiGuard service (fgd)	17
		Debug IO log (iolog)	20
		Object changes (objcfg)	21
		DVM (dvm)	22
		FortiManager web service (fmgws)	23
		Log daemon (logd)	25
		FIPS-CC (fips)	26
		Managed device operations (devops)	27
		Management extension applications (docker)	41

FortiAnalyzer log types and subtypes

The following table identifies all of the subtypes for the following log types that are specific to FortiAnalyzer:

- Event log type
- Application log type

For the event log type, some subtypes that are identified for FortiManager are also used by FortiAnalyzer, such as the System Manager (system) subtype. See also FortiManager log types and subtypes on page 6.

Type	Description	Subtype	Subtype Category Number
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	FortiAnalyzer system (fazsys)	28
		Logging device (logdev)	29
		Logging status/monitoring (logging)	30
		Log files (logfile)	31
		Report (report)	32
		Event management (eventmgmt)	33
		Logging database (logdb)	34
		Cache for data query (hcache)	35
		Disk/quota space (diskquota)	36
		Email Discovery (ediscovery)	38
		FortiAnalyzer High Availability (fazha)	39
		Incident (incident)	40
Appevent	Records event logs for each ADOM for applications, such as Playbooks.	Incident (incident)	1
		Playbook (playbook)	14
		Report (report)	17
		Logging device (logdev)	18
		Disk/quota space (diskquota)	20

Log message examples

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 or FortiAnalyzer unit to record the log.

This section contains the following topics:

FortiManager event log message example

```
2020-05-12 17:01:16 log_id=0001010018 type=event subtype=system pri=information desc="User
     login/logout successful" user="admin" userfrom="JSON(10.100.55.254)" msg="user 'admin'
```

```
with profile 'Super_User' logout from JSON(10.100.55.254)" session_id=5108
adminprof="Super_User"
```

Event log message breakdown

Log Field	Description
Date: `2020-05-12`	The year, month, and day when the event occurred in the format: YY-MM-DD
Time: `17:01:16`	The hour, minute, and second of when the event occurred.
Log ID: `0001010018`	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 six digits represent the message ID number.
Type: `event`	The section of the system where the event occurred.
Subtype: `system`	The subtype of each log message.
Pri: `information`	The severity level or priority of the event. There are several severity or priority levels. See Priority levels on page 12.
Desc: `User login/logout successful`	A description of the activity or event recorded by the FortiManager unit.
User: `admin`	The name of the user creating the traffic.
Userfrom: `JSON (10.100.55.254)`	Where the user initiated the activity or event, if applicable.
Msg: `user 'admin' with profile 'Super_User' logout from JSON (10.100.55.254)`	The activity or event recorded by the FortiManager unit.
session_id: `5108`	The session identification number.
adminprof: `Super_User`	The administrator profile associated with the administrator account.

FortiAnalyzer event log message example

```
log_id=0032041002 type=event subtype=report pri=information desc=Run report user=system
     userfrom=system msg=Start generating SQL report [S-10025_t10025-Cyber Threat
     Assessment-2020-05-13-1505_1be4cb8e-664d-44f3-a41a-cb32497bf094_199] at Wed (3) 2020-
     05-13 15:05:14, adom=root. action=run devid=FAZ-VMTM20004698 itime=2020-05-13 15:05:14
     date=2020-05-13 time=15:05:14 dtime=2020-05-13 15:05:14 itime_t=1589407514
```

Event log message breakdown

Log Field	Description
Action: `run`	Records the action taken, if applicable.

Log Field	Description
Date: `2020-05-13`	The year, month, and day when the event occurred in the format: YY-MM-DD
Time: `15:05:14`	The hour, minute, and second of when the event occurred.
Description: `Run report`	The activity or event recorded by the FortiAnalyzer unit.
Device ID: `FAZ-VMTM20004698`	An identification number for the device that recorded the event.
Device Time: `2020-05-13 15:05:14`	The year, month, and day when the event occurred in the format: YY-MM-DD. It also includes the hour, minute, and second of when the event occurred.
ID: `0032041002`	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 six digits represent the message ID number.
Level: `information`	The severity level or priority of the event. There are several severity or priority levels. See Priority levels on page 12.
Msg: `Start generating SQL report [S-10025_t10025-Cyber Threat Assessment-2020-05-13-1505_ 1be4cb8e-664d-44f3-a41a-cb32497bf094_199] at Wed (3) 2020-05-13 15:05:14,`	A description of the activity or event recorded by the FortiAnalyzer unit.
Subtype: `report`	The subtype of each log message.
Type: `event`	The section of the system where the event occurred.
User: `system`	The name of the user creating the traffic.
User From: `system`	Where the user initiated the activity or event, if applicable.

FortiAnalyzer application log message example

```
id=6826113487735881741 itime=2020-05-12 17:06:37 euid=1 epid=1 dsteuid=1 dstepid=1 vd=root
     logid=110269 type=appevent subtype=playbook eventtype=run-stat level=notice date=2020-
     05-12 time=17:06:38 user=system user_from=system desc=Incident Attachment Added
     msg=Task 'Attach Events to Incident' executed successfully. status=success playbook_
     name=Demo Playbook- Compromised Host Incident trigger_type=event trigger_
     name=202005121000000012 task_name=Attach Events to Incident event_
     id=202005121000000012 devid=FAZ-VMTM20004698 devname=FAZ-VMTM20004698 dtime=2020-05-12
     17:06:37 itime_t=1589328397
```

application log message breakdown

Log Field	Description
Date/Time: `17:06:37`	The hour, minute, and second of when the event occurred.
Description (desc): `Incident Attachment Added`	A description of the activity or event recorded by the FortiAnalyzer unit.

Log Field	Description
Destination End User ID (dsteuid): `1`	An identification number for the destination end user.
Destination Endpoint ID (dstepid): `1`	An identification number for the destination endpoint.
Device ID (devid): `FAZ-VMTM20004698`	An identification number for the device that recorded the event.
Device Name (devname): `FAZ-VMTM20004698`	The name of the device that recorded the event.
Device Time (dtime): `2020-05-12 17:06:37`	The year, month, and day when the event occurred in the format: YY-MM-DD. It also includes the hour, minute, and second of when the event occurred.
End User ID (euid): `1`	An identification number for the end user.
Endpoint ID (epid): `1`	An identification number for the endpoint user.
Event ID (id): `6826113487735881741`	An identification number for the event.
Event Type (eventtype): `run-stat`	The type of event recorded.
Level (level): `notice`	The severity level or priority of the event. There are several severity or priority levels. See Priority levels on page 12.
Log ID (logid): `110269`	The message ID number.
Message (msg): `Task 'Attach Events to Incident' executed successfully.`	Explains the activity or event that the FortiAnalyzer unit recorded.
Playbook name (playbook_name): `Demo Playbook-Compromised Host Incident`	The name of the playbook.
Status (status): `success`	The status of the playbook.
Subtype (subtype): `playbook`	The subtype of each log message.
Task Name (task_name): `Attach Events to Incident event_`	The name of the playbook task.
Trigger Name (trigger_name): `202005121000000012`	The identification number for the trigger.
Trigger Type (trigger_type): `event`	The type of trigger.
Type (type): `appevent`	The section of the system where the event occurred.

Log Field	Description
User (user): `system`	The name of the user creating the traffic.
User From (user_from): `system`	Where the user initiated the activity or event, if applicable.
Virtual Domain (vd): `root`	The name of the VDOM, if applicable.

Priority levels

When a logging severity level is defined, the FortiManager or FortiAnalyzer unit logs all messages at and above the selected severity level. For example, if you select Error, the FortiManager or FortiAnalyzer 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 or FortiAnalyzer unit 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 and FortiAnalyzer 7.4.0 Log Messages

The following tables list the FortiManager and FortiAnalyzer 7.4.0 log messages.

APPEVENT

DISKQUOTA

Log Field Name	Description	Data Type	Length
action		string	32
adom		string	64
date		string	16
desc		string	64
devid		string	16
diskusage		int64	
eventtype		string	64
level		enum	11
logid		string	16
msg		string	4096
subtype		string	16
time		string	16
type		enum	16
tz		string	8
vd		string	64

DISKQUOTA Log Messages

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

Message ID	Message	Severity
220003	Quota_Usage_Warn	Information

INCIDENT

Log Field Name	Description	Data Type	Length
action		string	32
adom		string	64
affected_assets		string	128
attachment		string	512
attachment_type		string	64
attach_source		string	32
attach_source_id		string	64
connector_name		string	64
date		string	16
desc		string	64
devid		string	16
end_time		string	128
error		string	512
eventtype		string	64
incident_assigned_analyst		string	64
incident_id		string	64
incident_other_attrs		string	64
incident_severity		string	64
level		enum	11
logid		string	16
msg		string	4096
note		string	256
report_source		string	32
report_source_id		string	64
start_time		string	128
status		string	36
subtype		string	16
task_id		string	64
task_name		string	64

Log Field Name	Description	Data Type	Length
time		string	16
trigger_name		string	64
trigger_type		string	64
type		enum	16
tz		string	8
user		string	64
user_from		string	64
user_type		string	64
vd		string	64

INCIDENT Log Messages

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

Message ID	Message	Severity
100001	New_Incident_Create	Information
110001	New_Incident_Create_Error	Error
100002	Incident_Update	Information
110002	Incident_Update_Error	Error
100003	Incident_Delete	Information
110003	Incident_Delete_Error	Error
100004	Incident_Attachment_Update	Information
110004	Incident_Attachment_Update_Error	Error
100005	Incident_Attachment_Add	Information
110005	Incident_Attachment_Add_Error	Error
100006	Incident_Attachment_Delete	Information
110006	Incident_Attachment_Delete_Error	Error

LOGDEV

Log Field Name	Description	Data Type	Length
action		string	32

Log Field Name	Description	Data Type	Length
adom		string	64
date		string	16
desc		string	64
devid		string	16
eventtype		string	64
level		enum	11
logdev_id		string	24
logdev_last_logging		int64	
logdev_name		string	128
logdev_offline_ duration		int64	
logid		string	16
msg		string	4096
subtype		string	16
time		string	16
type		enum	16
tz		string	8
vd		string	64

LOGDEV Log Messages

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

Message ID	Message	Severity
220001	Logdev_Nolog_Alert	Information
220002	Logdev_Online_Alert	Information

PLAYBOOK

Log Field Name	Description	Data Type	Length
action		string	32
adom		string	64
affected_assets		string	128

Log Field Name	Description	Data Type	Length
connector_name		string	64
data_src		string	64
data_src_id		string	64
data_src_type		string	64
date		string	16
desc		string	64
devid		string	16
end_time		string	128
error		string	512
eventtype		string	64
event_id		string	64
job_id		string	24
level		enum	11
logid		string	16
msg		string	4096
playbook_id		string	64
playbook_name		string	128
start_time		string	128
status		string	36
subtype		string	16
task_id		string	64
task_name		string	64
time		string	16
trigger_name		string	64
trigger_type		string	64
type		enum	16
tz		string	8
user		string	64
user_from		string	64
user_type		string	64
vd		string	64

PLAYBOOK Log Messages

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

Message ID	Message	Severity
110020	Playbook_Triggered_by_User	Information
110021	Playbook_Created_by_User	Information
110022	Playbook_Updated_by_User	Information

REPORT

Log Field Name	Description	Data Type	Length
action		string	32
adom		string	64
date		string	16
desc		string	64
devid		string	16
end_time		string	128
error		string	512
eventtype		string	64
level		enum	11
logid		string	16
msg		string	4096
start_time		string	128
status		string	36
subtype		string	16
time		string	16
type		enum	16
tz		string	8
user		string	64
user_from		string	64
user_type		string	64
vd		string	64

REPORT Log Messages

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

Message ID	Message	Severity
210001	Report_Run_Failure	Information

SYSTEM

Log Field Name	Description	Data Type	Length
action		string	32
adom		string	64
changes		string	64
date		string	16
desc		string	64
devid		string	16
eventtype		string	64
level		enum	11
logid		string	16
lograte		int64	
logratelimit		int64	
msg		string	4096
operation		string	64
performed_on		string	64
subtype		string	16
time		string	16
type		enum	16
tz		string	8
vd		string	64

SYSTEM Log Messages

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

Message ID	Message	Severity
220004	Perf_Stats_Notify	Information

Event

DEVCFG

Log Field Name	Description	Data Type	Length
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	10
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
desc		string	128
device	Name of the Device	string	64
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
session_id		uint32	10
subtype	Log Subtype	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
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

DISKQUOTA

Log Field Name	Description	Data Type	Length
action		string	6
adom		string	64
changes		string	1024
date		string	10
desc		string	128
diskusage		uint32	10
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

DISKQUOTA Log Messages

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

Message ID	Message	Severity
45002	LOG_ID_alert	Alert
45005	LOG_ID_warn	Warning
45006	LOG_ID_notify	Notice
45007	LOG_ID_info	Information
45010	LOG_ID_change	Information
45011	LOG_ID_change_fail	Warning

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
changes		string	1024
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
desc		string	128
device	Name of the Device	string	64
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
operation		string	64
performed_on		string	64

Log Field Name	Description	Data Type	Length
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
session_id		uint32	10
status	Operation Result	string	4
subtype	Log Subtype	string	10
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

Message ID	Message	Severity
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

DOCKER

Log Field Name	Description	Data Type	Length
changes		string	1024
date		string	10
desc		string	128
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64

DOCKER Log Messages

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

Message ID	Message	Severity
10258	LOG_ID_emerg	Emergency
10259	LOG_ID_alert	Alert
10260	LOG_ID_critical	Critical
10261	LOG_ID_error	Error
10262	LOG_ID_warning	Warning
10263	LOG_ID_notif	Notice
10264	LOG_ID_info	Information
10265	LOG_ID_debug	Debug
10266	LOG_ID_resource	Alert

DVM

Log Field Name	Description	Data Type	Length
action	Action towards this device	string	6
adom	The name of Admin ADOM	string	64
changes		string	1024
date	Date	string	10
desc		string	128
device	Name of the Device	string	64
log_id	Log ID	uint32	10
msg	Message	string	1024
operation		string	64
performed_on		string	64
pri	Priority	string	11
session_id		uint32	10
subtype	Log Subtype	string	10
time	Time	string	8
type	Log Type	string	14

Log Field Name	Description	Data Type	Length
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
31009	LOG_ID_dvmlog_notif	Notice
31010	LOG_ID_dvmlog_info	Information
31011	LOG_ID_dvmlog_debug	Debug
31012	LOG_ID_dev_replace	Notice
31013	LOG_ID_workflow_db_reset	Information

EDISCOVERY

Log Field Name	Description	Data Type	Length
action		string	6
date		string	10
desc		string	128
log_id		uint32	10
msg		string	1024
pri		string	11
subtype		string	10
time		string	8

Log Field Name	Description	Data Type	Length
type		string	14
user		string	64
userfrom		string	64

EDISCOVERY Log Messages

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

Message ID	Message	Severity
47002	LOG_ID_create	Information
47003	LOG_ID_create_fail	Warning
47004	LOG_ID_delete	Notice
47005	LOG_ID_delete_fail	Warning

EVENTMGMT

Log Field Name	Description	Data Type	Length
action		string	6
changes		string	1024
date		string	10
desc		string	128
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14

EVENTMGMT Log Messages

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

Message ID	Message	Severity
42002	LOG_ID_new	Information
42004	LOG_ID_delete	Warning
42006	LOG_ID_update	Information
42007	LOG_ID_update_fail	Warning
42008	LOG_ID_trigger	Information

FAZHA

Log Field Name	Description	Data Type	Length
action		string	6
changes		string	1024
date		string	10
desc		string	128
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

FAZHA Log Messages

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

Message ID	Message	Severity
48002	LOG_ID_state_change	Information

Message ID	Message	Severity
48003	LOG_ID_init_sync_start	Information
48004	LOG_ID_init_sync_end	Information
48005	LOG_ID_init_sync_fail	Alert
48006	LOG_ID_configuration_error	Warning

FAZSYS

Log Field Name	Description	Data Type	Length
action		string	6
adom		string	64
app		string	32
changes		string	1024
date		string	10
desc		string	128
logdev_id		string	32
logdev_name		string	64
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
session_id		uint32	10
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

FAZSYS Log Messages

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

Message ID	Message	Severity
37002	LOG_ID_generic	Information
37003	LOG_ID_daemon_start	Information
37004	LOG_ID_daemon_exit	Information
37005	LOG_ID_daemon_suspend	Emergency
37006	LOG_ID_daemon_resume	Notice
37007	LOG_ID_daemon_suspend_info	Information
37008	LOG_ID_daemon_resume_info	Information
37012	LOG_ID_user_login	Information
37013	LOG_ID_user_login_fail	Warning
37014	LOG_ID_user_logout	Information
37016	LOG_ID_upgrade	Information
37017	LOG_ID_upgrade_fail	Warning
37018	LOG_ID_metadata_update	Information
37019	LOG_ID_metadata_update_fail	Warning
37020	LOG_ID_config_change	Information
37021	LOG_ID_config_change_fail	Warning
37022	LOG_ID_mail_send	Information
37023	LOG_ID_mail_send_fail	Warning
37024	LOG_ID_license_limit	Warning
37026	LOG_ID_data_unmask	Information
37027	LOG_ID_data_unmask_fail	Notice
37028	LOG_ID_adom_limit_exceed	Warning
37029	LOG_ID_faz_cdb_upgrade	Information
37030	LOG_ID_faz_cdb_upgrade_fail	Warning
37031	LOG_ID_time_diff_exceed	Warning
37032	LOG_ID_time_diff_sync	Notice
37033	LOG_ID_export	Information
37034	LOG_ID_export_fail	Warning

Message ID	Message	Severity
37035	LOG_ID_import	Information
37036	LOG_ID_import_fail	Warning
37037	LOG_ID_daemon_init_error	Warning
37038	LOG_ID_iocrescan	Information
37039	LOG_ID_fluentd_fail	Error
37040	LOG_ID_fluentd_info	Notice

FGD

Log Field Name	Description	Data Type	Length
changes		string	1024
constmsg	Constant Message	string	256
date	Date	string	10
dbver	The Service Database Version	string	32
desc		string	128
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_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
operation		string	64
package_desc		string	20
package_type	Identifier of Package Type	string	64
performed_on		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

Log Field Name	Description	Data Type	Length
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	10
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
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

Message ID	Message	Severity
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
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
changes		string	1024
date	Date	string	10
desc		string	128
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
operation		string	64
performed_on		string	64
pri	Priority	string	11
subtype	Log Subtype	string	10
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
11005	LOG_ID_dev_register	Alert

FIPS

Log Field Name	Description	Data Type	Length
changes		string	1024
date	Date	string	10
desc		string	128
fips_err	FIPS test error code	string	12
fips_method	FIPS self-test method	string	128
log_id	Log ID	uint32	10
operation		string	64
operstat	Operation Result	string	12
performed_on		string	64
pri	Priority	string	11
session_id		uint32	10
subtype	Log Subtype	string	10
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
changes		string	1024
constmsg	Constant Message	string	256
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
operation		string	64
performed_on		string	64
pri	Priority	string	11
remote_host	Remote Host Name or Host IP in string presentation	string	128
session_id		uint32	10
subtype	Log Subtype	string	10
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
changes		string	1024
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
operation		string	64
performed_on		string	64
pri	Priority	string	11
session_id		uint32	10
subtype	Log Subtype	string	10
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

Message ID	Message	Severity
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
desc		string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	10
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
changes		string	1024
constmsg	Constant Message	string	256

Log Field Name	Description	Data Type	Length
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
module	Identifier of the HA Sync Module	uint32	10
msg	Message	string	1024
operation		string	64
operstat	Operation Result	string	12
peer	Serial Number of HA peer	string	32
performed_on		string	64
pri	Priority	string	11
status	HA status	string	4
subtype	Log Subtype	string	10
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
24009	LOG_ID_db_hash_validation	Information
24010	LOG_ID_mode_change	Information

HCACHE

Log Field Name	Description	Data Type	Length
action		string	6
adom		string	64
changes		string	1024
date		string	10
desc		string	128
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14

HCACHE Log Messages

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

Message ID	Message	Severity
44002	LOG_ID_rebuild	Information
44003	LOG_ID_rebuild_fail	Warning
44004	LOG_ID_upgrade	Information
44005	LOG_ID_upgrade_fail	Warning
44006	LOG_ID_limit	Warning

INCIDENT

Log Field Name	Description	Data Type	Length
action		string	6
date		string	10
desc		string	128

Log Field Name	Description	Data Type	Length
log_id		uint32	10
msg		string	1024
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

INCIDENT Log Messages

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

Message ID	Message	Severity
49002	LOG_ID_attachment_deleted	Information

IOLOG

Log Field Name	Description	Data Type	Length
changes		string	1024
date	Date	string	10
desc		string	128
function	The name of the Function Call	string	128
log_id	Log ID	uint32	10
operation		string	64
performed_on		string	64
pid	Process ID	uint64	20
pri	Priority	string	11
subtype	Log Subtype	string	10
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
changes		string	1024
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
operation		string	64
performed_on		string	64
pri	Priority	string	11
session_id		uint32	10
subtype	Log Subtype	string	10
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
35004	LOG_ID_reliable_conn_stat	Warning

LOGDB

Log Field Name	Description	Data Type	Length
action		string	6
adom		string	64
adom_oid	The OID of target ADOM	uint64	20
changes		string	1024
date		string	10
desc		string	128
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

LOGDB Log Messages

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

Message ID	Message	Severity
43002	LOG_ID_sql_run	Information
43004	LOG_ID_rebuild	Notice
43005	LOG_ID_rebuild_fail	Warning
43006	LOG_ID_trim	Warning
43007	LOG_ID_trim_fail	Warning
43008	LOG_ID_remove	Warning
43009	LOG_ID_remove_fail	Warning
43010	LOG_ID_dbage_approaching	Alert
43011	LOG_ID_dbage_exceed	Critical

LOGDEV

Log Field Name	Description	Data Type	Length
action		string	6
adom		string	64
changes		string	1024
date		string	10
desc		string	128
logdev_id		string	32
logdev_last_logging		uint32	10
logdev_name		string	64
logdev_offline_ duration		uint32	10
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

LOGDEV Log Messages

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

Message ID	Message	Severity
38002	LOG_ID_device_add	Information
38003	LOG_ID_device_add_fail	Warning
38004	LOG_ID_device_delete	Warning
38005	LOG_ID_device_delete_fail	Warning
38006	LOG_ID_device_update	Information

Message ID	Message	Severity
38007	LOG_ID_device_update_fail	Warning
38008	LOG_ID_device_online	Notice
38009	LOG_ID_device_offline	Warning
38010	LOG_ID_device_idle	Notice
38012	LOG_ID_adom_add	Information
38013	LOG_ID_adom_add_fail	Warning
38014	LOG_ID_adom_delete	Warning
38015	LOG_ID_adom_delete_fail	Warning
38016	LOG_ID_adom_update	Information
38017	LOG_ID_adom_update_fail	Warning
38022	LOG_ID_devvd_add	Information
38023	LOG_ID_devvd_add_fail	Warning
38024	LOG_ID_devvd_delete	Warning
38025	LOG_ID_devvd_delete_fail	Warning
38032	LOG_ID_ha_new	Information
38033	LOG_ID_ha_new_fail	Warning
38034	LOG_ID_ha_update	Information
38035	LOG_ID_ha_update_fail	Warning
38042	LOG_ID_hamember_add	Information
38043	LOG_ID_hamember_add_fail	Warning
38052	LOG_ID_csf_import	Information
38053	LOG_ID_csf_import_fail	Warning
38054	LOG_ID_csf_delete	Information
38055	LOG_ID_csf_delete_fail	Warning
38056	LOG_ID_csf_update	Information
38057	LOG_ID_csf_update_fail	Warning

LOGFILE

Log Field Name	Description	Data Type	Length
action		string	6

Log Field Name	Description	Data Type	Length
adom		string	64
changes		string	1024
date		string	10
desc		string	128
logdev_id		string	32
logdev_name		string	64
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

LOGFILE Log Messages

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

Message ID	Message	Severity
40002	LOG_ID_new	Information
40004	LOG_ID_delete	Warning
40005	LOG_ID_delete_fail	Warning
40006	LOG_ID_upload	Notice
40007	LOG_ID_upload_fail	Warning
40008	LOG_ID_download	Information
40009	LOG_ID_download_fail	Warning
40010	LOG_ID_backup	Information
40011	LOG_ID_backup_fail	Warning
40012	LOG_ID_restore	Information

Message ID	Message	Severity
40013	LOG_ID_restore_fail	Warning
40014	LOG_ID_import	Information
40016	LOG_ID_forward	Information
40018	LOG_ID_fetch	Information
40019	LOG_ID_fetch_fail	Warning
40022	LOG_ID_aggregate	Information
40023	LOG_ID_aggregate_fail	Warning
40024	LOG_ID_merge	Information
40025	LOG_ID_merge_fail	Warning
40026	LOG_ID_roll	Information
40032	LOG_ID_archive_new	Notice
40034	LOG_ID_archive_delete	Notice
40035	LOG_ID_archive_delete_fail	Warning
40036	LOG_ID_archive_backup	Information
40037	LOG_ID_archive_backup_fail	Warning
40038	LOG_ID_archive_restore	Information
40042	LOG_ID_cloud_usage_warning	Warning
40043	LOG_ID_cloud_usage_alert	Alert
40044	LOG_ID_cloud_usage_license_alert	Alert

LOGGING

Log Field Name	Description	Data Type	Length
action		string	6
adom		string	64
changes		string	1024
date		string	10
desc		string	128
log_id		uint32	10
msg		string	1024
operation		string	64

Log Field Name	Description	Data Type	Length
performed_on		string	64
pri		string	11
subtype		string	10
time		string	8
type		string	14
user		string	64
userfrom		string	64

LOGGING Log Messages

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

Message ID	Message	Severity
39002	LOG_ID_lograte_alert	Alert
39003	LOG_ID_lograte_notify	Notice
39004	LOG_ID_diag	Information
39005	LOG_ID_resume	Notice
39012	LOG_ID_abnormal_interval_notify	Notice
39013	LOG_ID_dup_logs_detect	Warning

OBJCFG

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
changes		string	1024
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
operation		string	64
performed_on		string	64
pri	Priority	string	11

Log Field Name	Description	Data Type	Length
session_id		uint32	10
subtype	Log Subtype	string	10
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

REPORT

Log Field Name	Description	Data Type	Length
action		string	6
adom		string	64
changes		string	1024
date		string	10
desc		string	128
logdev_id		string	32
logdev_name		string	64
log_id		uint32	10
msg		string	1024
operation		string	64
performed_on		string	64
pri		string	11
runfrom		string	64
subtype		string	10
time		string	8

Log Field Name	Description	Data Type	Length
type		string	14
user		string	64
userfrom		string	64

REPORT Log Messages

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

Message ID	Message	Severity
41002	LOG_ID_run	Information
41003	LOG_ID_run_fail	Warning
41004	LOG_ID_delete	Warning
41005	LOG_ID_delete_fail	Warning
41006	LOG_ID_download	Information
41007	LOG_ID_download_fail	Warning
41008	LOG_ID_upload	Information
41009	LOG_ID_upload_fail	Warning
41010	LOG_ID_rename	Information
41011	LOG_ID_rename_fail	Warning
41012	LOG_ID_backup	Information
41013	LOG_ID_backup_fail	Warning
41014	LOG_ID_convert	Information
41015	LOG_ID_convert_fail	Warning
41016	LOG_ID_config_import	Information
41017	LOG_ID_config_import_fail	Warning
41018	LOG_ID_config_export	Information
41019	LOG_ID_config_export_fail	Warning
41020	LOG_ID_config_backup	Information
41021	LOG_ID_config_backup_fail	Warning
41022	LOG_ID_config_restore	Information
41023	LOG_ID_config_restore_fail	Warning
41024	LOG_ID_config_update	Information

Message ID	Message	Severity
41025	LOG_ID_config_update_fail	Warning
41026	LOG_ID_group_add	Information
41028	LOG_ID_group_modify	Information
41030	LOG_ID_group_delete	Information
41032	LOG_ID_language_import	Information
41033	LOG_ID_language_export	Information
41034	LOG_ID_language_delete	Warning
41035	LOG_ID_generation_failed	Warning

RTMON

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
changes		string	1024
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
operation		string	64
performed_on		string	64
pri	Priority	string	11
session_id		uint32	10
subtype	Log Subtype	string	10
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
changes		string	1024
date	Date	string	10
desc		string	128
detail	The task details	string	256
errcode		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
operation		string	64
percent	The percentage of this task being running	uint8	3
performed_on		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	10
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
17007	LOG_ID_generic_info	Information

SCRMGR

Log Field Name	Description	Data Type	Length
date	Date	string	10
desc		string	128
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
subtype	Log Subtype	string	10
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
action		string	6
address	IP address of login user	string	32
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
adom_oid		uint64	20
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
changes		string	1024
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
cpuusage		uint32	10
date	Date	string	10
date_time	String Representation of date and time in Local Timezone	string	128
desc		string	128
devlog	Name of the Device	string	64
dev_oid	The OID of Target Device	uint64	20
disk2usage		uint32	10
diskusage		uint32	10
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

Log Field Name	Description	Data Type	Length
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
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
lograte		uint32	10
logratelimit		uint32	10
logratepeak		uint32	10
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_adoms		uint16	5
max_mb	License Allowed Maximum Capacity in MB	uint32	10
memusage		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
msgrate		uint32	10
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
operation		string	64
operstat	Operation Result	string	12

Log Field Name	Description	Data Type	Length
path	CMDB Config Object Path	string	256
performed_on		string	64
pkgadom	Name of ADOM this policy package belongs to	string	64
pkgname	Name of the Policy Package which is locked/unlocked	string	128
ppkgname	Name of the Policy Package which is locked/unlocked	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
sensor_name		string	16
sensor_st		string	29
sensor_val		string	16
session_id		uint32	10
shutdown_reason	The reason for system shutdown	string	128
state	Status	string	64
status	Interface Status	string	4
subtype	Log Subtype	string	10
sw_version	Current Firmware Software Version	string	64

Log Field Name	Description	Data Type	Length
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

Message ID	Message	Severity
10005	LOG_ID_hwmon_raid_disk_error	Error
10006	LOG_ID_hwmon_raid_disk_info	Information
10007	LOG_ID_hwmon_sensor_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
10021	LOG_ID_sessionmgr	Information
10022	LOG_ID_restart_upgrade	Critical
10025	LOG_ID_upgrade_failure	Critical
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	Notice
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

Message ID	Message	Severity
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
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_high_inode_usage	Warning
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

Message ID	Message	Severity
10073	LOG_ID_raid_fw_setting	Notice
10074	LOG_ID_ssh_server_rekey	Notice
10075	LOG_ID_ssh_server_proto_error	Notice
10076	LOG_ID_ssl_cert_err	Notice
10077	LOG_ID_crl_update_info	Information
10078	LOG_ID_crl_update_error	Error
10079	LOG_ID_cloudinit_config	Notice
10080	LOG_ID_bonding_intf_status	Warning
10081	LOG_ID_sys_perf_stats_notify	Notice
10082	LOG_ID_locallog_over_quota	Warning
10083	LOG_ID_cdb_meta	Notice
10084	LOG_ID_fgc_activate_succ	Information
10085	LOG_ID_fgc_activate_fail	Warning
10086	LOG_ID_fgc_deactivate_succ	Information
10087	LOG_ID_fgc_enable_rmt	Information
10088	LOG_ID_fgc_disable_rmt	Information
10089	LOG_ID_daemon_crash	Warning
10090	LOG_ID_ssh_server_regen_hostkeys	Notice
10091	LOG_ID_license_warn	Warning
10092	LOG_ID_license_expired	Error
10093	LOG_ID_adom_perf_stats_notify	Notice
10094	LOG_ID_benchmark_io_perf	Information
10255	LOG_ID_adom_migrate_start	Notice
10256	LOG_ID_adom_migrate_end	Notice

WEBPORT

Log Field Name	Description	Data Type	Length
adom	The name of Admin ADOM	string	64
date	Date	string	10
desc		string	128

Log Field Name	Description	Data Type	Length
log_id	Log ID	uint32	10
msg	Message	string	1024
pri	Priority	string	11
session_id		uint32	10
subtype	Log Subtype	string	10
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 - 7.2.2 and 7.4.0

Refer to the *FortiManager & Analyzer Event Log Reference Guide* for a complete list of log field details related to version 7.4. This section covers changes applicable to the 7.4.0 version only. It is recommended you keep both the 7.2.2 and 7.4.0 *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 7.4.0 but exists in version 7.2.2. Similarly, the term **Added** indicates a log field was added in version 7.4.0 but does not exist in version 7.2.2.

Event

The following tables provide a list of log fields that were added or removed from the Event log subtypes in FortiManager and FortiAnalyzer version 7.4.0.

AID Log Messages

Message ID	Message	Change
49003	LOG_ID_config	Message ID removed
49004	LOG_ID_ui	Message ID removed

DVM Log Messages

Message ID	Message	Change
31013	LOG_ID_workflow_db_reset	Message ID added

FAZSYS Log Messages

Message ID	Message	Change
37039	LOG_ID_fluentd_fail	Message ID added
37040	LOG_ID_fluentd_info	Message ID added

INCIDENT Log Messages

Message ID	Message	Change
50002	LOG_ID_attachment_deleted	Message ID removed

LOGGING Log Messages

Message ID	Message	Change
39013	LOG_ID_dup_logs_detect	Message ID added

SYSTEM

Field	Change
disk2usage	Field added
diskusage	Field added
max_adoms	Field added

SYSTEM Log Messages

Message ID	Message	Change
10090	LOG_ID_ssh_server_regen_hostkeys	Message ID added
10091	LOG_ID_license_warn	Message ID added
10092	LOG_ID_license_expired	Message ID added
10093	LOG_ID_adom_perf_stats_notify	Message ID added
10094	LOG_ID_benchmark_io_perf	Message ID added

APPEVENT

The following tables provide a list of log fields that were added or removed from the Application log subtypes in FortiManager and FortiAnalyzer version 7.4.0.

DISKQUOTA

Field	Change
diskusage	Field added

DISKQUOTA Log Messages

Message ID	Message	Change
220003	Quota_Usage_Warn	Message ID added

SYSTEM

Field	Change
changes	Field added
lograte	Field added
logratelimit	Field added
operation	Field added
performed_on	Field added

SYSTEM Log Messages

Message ID	Message	Change
220004	Perf_Stats_Notify	Message ID added

www.fortinet.com