FortiManager Log Message Reference™

Version 4.0 MR1

Reference

The FortiManager Log Message Reference is published periodically and, therefore, contains only information that was gathered at the date of publication. Make sure to visit the Fortinet Technical Documentation web site on a regular basis to verify that you have the current, up-to-date version of the FortManager Log Message Reference.

F:::RTINET®

UNIFIED THREAT MANAGEMENT SOLUTIONS

FortiManager Log Message Reference

Version 4.0 MR1

31 August 2009

02-410-82628-20090831

Trademarks

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

Contents

Introduction

This reference provides detailed information about FortiManager log messages. This reference is intended for administrators that enabled and configured local logging on their FortiManager unit and need to know what the log messages mean.

Log messages provide valuable information about what is occurring on your network and on the FortiManager unit itself.

This chapter includes the following topics:

- Before you begin
- Document conventions
- Registering your Fortinet product
- Fortinet products End User License Agreement
- Customer service and technical support
- Training
- Fortinet documentation

Before you begin

Before you begin using this reference, take a moment to note the following:

- The information in this reference applies to all FortiManager units and models that are currently running 4.0 and higher.
- You have enabled logging of FortiManager events. If you have not enabled logging, see the *FortiManager Administration Guide*.
- Each log message is written as it would appear in the RAW format on the web-based manager.
- The log message tables in this reference indicate the firmware maintenance release each log message is recorded in, whenever applicable. The firmware maintenance release informs readers which firmware maintenance release records each log message. If no firmware maintenance release is applicable, the firmware version is used (as in the initial release of this document) and indicates the log message carries forward through all FortiManager 4.0 maintenance releases.

  Log messages generated in one firmware maintenance release (or firmware version) to another may not contain the exact information because of changes to existing features or new features.

- This reference is published periodically, and therefore, contains only information gathered at the date of publication. This information includes only log messages from log types that are supported. For a list of the log types that are supported, see "Log types and subtypes" on page 10.

How this reference is organized

This document contains all known log messages for the current release. This document also contains information about FortiManager log types and subtypes, including a detailed explanation of an example log message.

This document contains the following chapters:

FortiManager 4.0 logs and updates provides general information about the event log type and its subtypes, as well as updates about what's new or changed for log messages. This chapter also includes a detailed example of a FortiManager log message.

The following chapters are grouped by the event log's subtypes, for example, event-fortiguard-fortimanager protocol. The event log type is the only log type recorded by the FortiManager unit.

- System
- FortiGuard-FortiManager protocol
- Policy console
- VPN console
- Deployment manager
- Real-time monitor
- High Availability
- FortiGuard service
- FortiClient Manager

Document conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

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

Cautions, Notes and Tips

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

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

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

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

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From *Minimum log level*, select *Notification*.
CLI input	```config system dns set primary <address_ipv4> end```
CLI output	```FGT-602803030703 # get system settings comments : (null) opmode : nat```
Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.
File content	```<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>```
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com.
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to *VPN > IPSEC > Auto Key (IKE)*.
Publication	For details, see the *FortiGate Administration Guide*.
	Note: Links typically go to the most recent version. To access earlier releases, go to http://docs.fortinet.com/. This link appears at the bottom of each page of this document.

Registering your Fortinet product

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

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

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Fortinet products End User License Agreement

See the *Fortinet products End User License Agreement*.

Customer service and technical support

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

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

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

Training

Fortinet Training Services provides a variety of training programs to serve the needs of our customers and partners world-wide. Visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

Fortinet documentation

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

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

Tools and Documentation CD

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

Fortinet Knowledge Base

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

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

FortiManager 4.0 logs and updates

FortiManager logs provide historical information as well as current analysis of FortiManager system activity. For more information about configuring logging in FortiManager 4.0, see the *FortiManager Administration Guide*.

This section describes:

- FortiManager log message updates
- FortiManager logs
- FortiManager log messages

FortiManager log message updates

There have been significant changes in log messages since FortiManager 3.0, along with several new log subtypes and log messages. The following information explains these changes and any new log subtypes that were introduced. This topic also includes, whenever applicable, updates for all 4.0 maintenance releases.

FortiManager 4.0 log message updates

In FortiManager 4.0, many log messages have been removed or merged into other log message types. There are log types in *System Settings > Event Log* that are not supported but are still in the list. This document contains only the log messages from the log types that are supported.

Table 2: Explanation of what log types are supported and not supported in FortiManager 4.0

Log types not supported	Log types supported (* indicates that the log type is new)
Policy Device	*FortiGuard-FortiManager protocol
VPN	*VPN console
Update Manager	*Policy console
Log & Report Manager	*Deployment Manager
Firewall objects	*FortiGuard service (previously Update Manager
Script Manager	*FortiClient Manager
Update Manager	High Availability (HA)
Deployment	System
	Real-time Monitor

There were also changes to the Real-time Monitor log identification number. The Real-time Monitor log ID number was previously 22001 and is now 46001.

FortiManager logs

Log messages display in *System Settings > Local Log > Log Access*. The Log Access page displays the event log file. The event log file is the only log file recorded by the FortiManager unit. There are 9 sub-categories under the event log file, which are shown in Table 3. Event-System contains all log messages that the FortiManager unit generates and is the only log file generated.

Log types and subtypes

FortiManager logs have only one log type and 9 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, an Event-Policy console log message contains the numbers `31001`.

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

Table 3: Subtype numbers for the Event-System

Event-System subtype categories	Sub-type category number
System	00
FortiGuard-FortiManager protocol	01
Policy console	07
VPN console	08
Deployment Manager	11
Real-time Monitor	12
High Availability	14
FortiGuard service	16
FortiClient Manager	17

Log severity 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.

Table 4: Logging severity levels in FortiManager

Levels	Description
0-Emergency	The system has become unstable
1-Alert	Immediate action is required.
2-Critical	Functionality is affected.
3-Error	An error condition exists and functionality could be affected.
4-Warning	Functionality could be affected.
5-Notice	Information about normal events.
6-Information	General information about system operation.

The Debug log severity level is rarely used, although you can select it in the Event Log list in System *Settings > Local Log > Event Log*. 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.

FortiManager log messages

All 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.

For example, if a FortiManager-3000 unit recorded an Event-FortiGuard message, the following log message may be recorded:

```
2009-04-15 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"
```

Table 5: Explanation of the Event-System log message example

date=(2009-04-15)	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 are the message ID number.
type=(event)	The section of the system where the event occurred. The log types are event, antivirus, antispam, and history.
subtype=(fgd)	The subtype of each log message. In this example, a FortiGuard service update has occurred.
pri=(information)	The severity level, or priority, or the event. There are six logging severity levels.
user=(user_2)	The name of the user creating the traffic.
msg=["Receive an update package from FDS, type=OBLT00000, version=00000.00000-090571930"]	Explains the activity or event that the FortiManager unit recorded. In this example, the log message states that an update package was received from the FDS, indicating the type of package that was received and its version number.

System

Event-system log messages are recorded when a user changes an interface setting or upgrades the firmware on the FortiManager unit. Event-system log messages are identified by three numbers, `10001`, `10100` and `10200`.

Note: Event-system activity log messages do not record events happening on the individual FortiGate units.

10001
10100
10200

10001

- A user failed to log in from an SSH client.
- A user failed to log in from the console.
- A user failed to log in from a java console.
- A user failed to log in from a Telnet client.
- A user logged in from the web-based manager.
- A user who logged in was accepted.
- A user successfully logged out.
- The administrator user was created or updated.
- The administrator was deleted.
- The administrator profile was deleted.
- A new administrator was created.
- The administrator was updated.
- The administrator's password was changed.
- An interface IP address was changed.
- An interface status changed.
- The system time changed.
- The system restarted.
- The system has been shut down.
- A scheduled back up of all settings was successful.
- A schedule back up of all settings failed.
- The host name has changed.
- A user session is killed.
- A firmware upgrade from one firmware version to another. The field <build_type> indicates what type of build the firmware version is, such as a patch build or regular release of a maintenance build.
- The FortiManager unit's system was restarted with the specified firmware running on the unit.
- Failed to do the firmware upgrade because of the invalid image file.
- Failed to do the firmware upgrade because of the invalid FortiManager image type.
- Failed to do the firmware upgrade.
- Failed to upgrade the firmware from FTP.
- An invalid image file.
- System configuration was restored.
- All settings are restored.
- The database is restored.
- Failed to restore all settings because of the invalid backup file.
- Failed to restore database.
- Failed to restore all settings.
- Failed to back up all settings from the TFTP server.
- Failed to restore all settings from TFTP server.
- Invalid backup file.

- Decrypt backup file failed.
- Fail to back up all-settings from the TFTP server.
- A FortiAnalyzer package could not be installed because there was a TFTP transmission error.
- There was a system error.
- The maximum number of FortiGate devices and/or VDOMs has been exceeded.
- Nearing the maximum number of FortiGate devices and/or VDOMs.

Message ID	10001
Log Type	Event-System
Severity	Alert
FortiManager version	4.0
Message	user=*<user_name>* msg=*"user <user_name> login failed from ssh(<ip_address>)"*
Meaning	A user failed to log in from an SSH client.

Message ID	10001
Log Type	Event-System
Severity	Alert
FortiManager version	4.0
Message	user=*<user_name>* msg=*"user <user_name> login failed from console"*
Meaning	A user failed to log in from the console.

Message ID	10001
Log Type	Event-System
Severity	Alert
FortiManager version	4.0
Message	user=*<user_name>* msg=*"user <user_name> login failed from javaconsole"*
Meaning	A user failed to log in from a java console.

Message ID	10001
Log Type	Event-System
Severity	Alert
FortiManager version	4.0
Message	user=*<user_name>* msg=*"user <user_name> login failed from telnet"*
Meaning	A user failed to log in from a Telnet client.

Message ID	10001
Log Type	Event-Deployment
Severity	Information
FortiManager version	4.0

Message ID	10001
Message	user=*<user_name>* msg=*"user <user_name> login login accepted from GUI (<ip_address>)"*
Meaning	A user logged in from the web-based manager.

Message ID	10001
Log Type	Event-System
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"user <user_name> login accepted from {GUI	CLI	console}"*
Meaning	A user who logged in was accepted.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<administrator_name>* msg=*"user <administrator_name> logout accepted from <string>"*
Meaning	A user successfully logged out.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=*<administrator_name>* msg=*"the admin user <administrator_name> was deleted"*
Meaning	The administrator user was created or updated.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=*<administrator_name>* msg=*"the admin user <administrator_name> was deleted"*
Meaning	The administrator was deleted.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=*<user_name>* msg=*"the admin profile <profile_name> was deleted"*
Meaning	The administrator profile was deleted.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=***<administrator_name>*** msg=***"new admin user <administrator_name> was created"***
Meaning	A new administrator was created.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=***<administrator_name>*** msg=***"the admin user <administrator_name> was updated"***
Meaning	The administrator was updated.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=***<administrator_name>*** msg=***"the admin user <administrator_name> password was changed"***
Meaning	The administrator's password was changed.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"interface <interface_name> ip changed <old_ip_address> --> <new_ip_address>"***
Meaning	An interface IP address was changed.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"interface <interface_name> status changed: <string> --> <string>"***
Meaning	An interface status changed.

Message ID	10001
Log Type	Event-System
Severity	Notification

Message ID	10001
FortiManager version	4.0
Message	user=*<user_name>* msg=*"system time changed: <seconds> --> <seconds>"*
Meaning	The system time changed.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"System restart"*
Meaning	The system restarted.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"System shutdown"*
Meaning	The system has been shut down.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Schedule Backup all settings to <string>:<string> Success"*
Meaning	A scheduled back up of all settings was successful.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Schedule Backup all settings to <string>:<string> Failure"*
Meaning	A schedule back up of all settings failed.

Message ID	10001
Log Type	Event-System
Severity	Notification
FortiManager version	4.0
Message	user=*<user_name>* msg=*"hostname changed: <string> --> <string>"*
Meaning	The host name has changed.

Message ID	10001
Log Type	Event-System
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"The session of the user <user_name> from <string> is killed"***
Meaning	A user session is killed.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Firmware upgrade from <version_number>-<build_number>, <date_of_build> (<build_type>) to <version_number>-<build_number>."***
Meaning	A firmware upgrade from one firmware version to another. The field <build_type> indicates what type of build the firmware version is, such as a patch build or regular release of a maintenance build.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"System restart <version_number>-<build_number>, <date_of_build> (<build_type>)"***
Meaning	The FortiManager unit's system was restarted with the specified firmware running on the unit.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Failed to do the firmware upgrade because of the invalid image file"***
Meaning	Failed to do the firmware upgrade because of the invalid image file.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Failed to do the firmware upgrade because of the invalid FortiManager image type"***
Meaning	Failed to do the firmware upgrade because of the invalid FortiManager image type.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"Failed to do the firmware upgrade"*
Meaning	Failed to do the firmware upgrade.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"Failed to do the firmware upgrade because of the FTP transmission error"*
Meaning	Failed to upgrade the firmware from FTP.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"Failed to do firmware upgrade because of the invalid image file"*
Meaning	An invalid image file.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"Restore system configuration"*
Meaning	System configuration was restored.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"Restore all settings"*
Meaning	All settings are restored.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0

Message ID	10001
Message	user=*<user_name>* msg=*"Restore database"*
Meaning	The database is restored.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Failed to restore all settings because of the invalid backup file"*
Meaning	Failed to restore all settings because of the invalid backup file.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Failed to restore database"*
Meaning	Failed to restore database.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Failed to restore all settings"*
Meaning	Failed to restore all settings.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Failed to restore database because of the TFTP transmission error"*
Meaning	Failed to back up all settings from the TFTP server.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Failed to restore all settings because of the TFTP tranmission error."*
Meaning	Failed to restore all settings from TFTP server.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=**<user_name>** msg=**"Failed to restore all settings because of the invalid backup file"**
Meaning	Invalid backup file.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=**<user_name>** msg=**"Failed to restore all settings because decrypt backup file failed"**
Meaning	Decrypt backup file failed.

Message ID	10001
Log Type	Event-System
Severity	Critical
FortiManager version	4.0
Message	user=**<user_name>** msg=**"Failed to restore system configuration because of the TFTP transmission error"**
Meaning	Fail to back up all-settings from the TFTP server.

Message ID	10001
Log Type	Event-System
Severity	Variable
FortiManager version	4.0
Message	user=**<user_name>** msg=**"Failed to install FortiAnalyzer Package because of the TFTP transmission error."**
Meaning	A FortiAnalyzer package could not be installed because there was a TFTP transmission error.

Message ID	10001
Log Type	Event-System
Severity	Variable
FortiManager version	4.0
Message	user=**<user_name>** msg=**"Failed to restart the DeviceManager process to install new fortianalyzer package"**
Meaning	There was a system error.

Message ID	10001
Log Type	Event-System
Severity	Variable

Message ID	10001
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"<log_message_information>"***
Meaning	The maximum number of FortiGate devices and/or VDOMs has been exceeded.

Message ID	10001
Log Type	Event-System
Severity	Variable
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"<log_message_information>"***
Meaning	Nearing the maximum number of FortiGate devices and/or VDOMs.

10100

Message ID	10100
Log Type	Event-System
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=***\"Memory <string> log: 75%%% full\"***
Meaning	Logs stored in system memory is 75 percent full.

Message ID	10100
Log Type	Event-System
Severity	Warning
FortiManager version	4.0
Message	user=***<user_name>*** msg=***\"Memory <string> log: 90%%% full"***
Meaning	Logs stored in system memory is 90 percent full.

Message ID	10100
Log Type	Event-System
Severity	Warning
FortiManager version	4.0
Message	user=***<user_name>*** msg=***\"Memory <string> log: 95%%% full"***
Meaning	Logs stored in system memory is 95 percent full.

10200

Message ID	10200
Log Type	Event-System
Severity	Emergency
FortiManager version	4.0
Message	user=***<user_name>*** msg=***\"Disk has rolled the max number of times. It will not roll logs again until deleting some of the old rolled logs.\"***
Meaning	Log rolling has reached the maximum number.

Message ID	10200
Log Type	Event-System
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=***\"Log has been rolled and are uploading as file <file_name>, size=<value> bytes(<percent>2fMB)\"***
Meaning	A rolled log file is being updated.

FortiGuard-FortiManager protocol

Event-FortiGuard-FortiManager protocol log messages are recorded when this protocol is used. Event-FortiGuard-FortiManager protocol log messages are identified by the numbers `13001`.

13001

Message ID	13001
Log Type	Event-FortiGuard-FortiManager protocol
Severity	Information
FortiManager version	4.0(MR1 and higher)
Message	user=fgfm msg=*"fgfm protocol start, offline mode is disable"*
Meaning	The FortiGuard-FortiManager protocol was started.

Policy console

Event-policy console log messages are recorded when events or activities are occuring within the Security Console menu. Event-policy console log messages are identified by the numbers `31001`.

31001

Message ID	31001
Log Type	Event-Policy console
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Policy installed on adom=<adom_name> device=<device_name>"***
Meaning	A policy was installed from within the specified ADOM by a specified device.

VPN console

Event-VPN console log messages are recorded recorded when events or activities are occuring within the Security Console menu. Event-policy console log messages are identified by the numbers `31001`.

31001

Message ID	31001
Log Type	Event-VPN
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"VPN installed on adom=<adom_name> device=<device_name>"***
Meaning	The specified user installed a VPN tunnel within the specified ADOM.

Deployment manager

Event-deployment manager log messages are recorded when a user configures settings in the Device Manager menu, as well as script installation events. Event-deployment log messages are identified by the number, 43001.

43001

- An automatic back up occurred for a specified device.
- An automatic retrieval of a back up occurred for a specified device.
- A user successfully installed a script on a specified device at a specified date and time.
- A managed device was removed from the FortiManager database.
- The user installed a revision for a specified device and may have succeed or failed. If failed, a specific reason is given, for example, failed (verify installation failed).
- The specified user deleted a revision.
- The specified user edited a revision within the Revision History tab of the specified device.
- The installation of a specified script file on the global database failed.
- The user successfully saved a revision to the specified device.
- The user successfully retrieved a revision from the specified device.
- The user successfully imported a configuration to the specified device.
- The user successfully reverted to the specified configuration for the specified device.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*auto_backup* msg=*"Load revision(<sequential_number>) from <device_hostname>(<device_serial number>)*
Meaning	An automatic back up occurred for a specified device.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*auto_backup* msg= *"Retrieve revision(<sequential_number>) from <device_hostname>(<device_serial number>)*
Meaning	An automatic retrieval of a back up occurred for a specified device.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg= *"script <script_name> install on device '(<device_name>)' (id=<number>) at time <day> <month> <date> <hh:mm:ss> <year> succeed"*
Meaning	A user successfully installed a script on a specified device at a specified date and time.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Delete device <host_name> (<device_serial_number>)"*
Meaning	A managed device was removed from the FortiManager database.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg= *"Install revision (<revision_number>) for <device_name>(<device_serial_number>) {successfully| failed (unknown error)| failed (parse error)| failed (network error)| failed (connection timeout)| failed (invalid host)| failed (connection error)| failed (internal error)| failed (login failed)| failed (web service failed)| failed (device serial number has changed)| failed (secure copy failed)| failed (verify installation failed)}"*
Meaning	The user installed a revision for a specified device and may have succeed or failed. If failed, a specific reason is given, for example, *failed (verify installation failed)*.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"DEPMGR (del revision): usr=<user_name> date=<date> device=<device_name> rev=<rev_number>"*
Meaning	The specified user deleted a revision.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Edit revision(<sequential_number>) for <device_name> (<device_serial_number>) to set revision comment."*
	user=*<user_name>* msg=*"Edit revision(<sequential_number>) for <device_name> (<device_serial_number>) to set tag revision"*
Meaning	The specified user edited a revision within the Revision History tab of the specified device.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Install of CLI script '<script_file_name>' on global db at <day_of_week> <month> <date> <hh:mm:ss> <year> failed."*
Meaning	The installation of a specified script file on the global database failed.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Save revision (<sequential_number>) to <device_name>(device_serial_number)"*
Meaning	The user successfully saved a revision to the specified device.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Retrieve revision (<sequential_number>) from <device_name>(<device_serial_number>)"*
Meaning	The user successfully retrieved a revision from the specified device.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Import revision (<sequential_number>) to <device_name>(<device_serial_number>)"*
Meaning	The user successfully imported a configuration to the specified device.

Message ID	43001
Log Type	Event-Deployment manager
Severity	Information
FortiManager version	4.0
Message	user=**<user_name>** msg=**"Revert to revision (<sequential_number>) for <device_name>(<device_serial_number>)"**
Meaning	The user successfully reverted to the specified configuration for the specified device.

Real-time monitor

Event-real-time monitor log messages are recorded when events or activities occur within Real-time monitor. Event-real-time monitor log messages are identified by the numbers `46001`.

46001

Message ID	46001
Log Type	Event-Real-time monitor
Severity	Notification
FortiManager version	4.0
Message	user=***<user_name>*** devNetAddr=***<device_ip_address>*** devName=***<device_name>*** devSerialNo=***<device_serial_number>*** OID=***<fortiguard_identification_number>*** msg=***"fnFmTrapConfChange (<trap_serial_number>) received from <device_ip_address>"***
Meaning	There was an SNMP trap change that was received from the specified device.

Message ID	46001
Log Type	Event-Real-time monitor
Severity	Notification
FortiManager version	4.0
Message	user=***<user_name>*** user=***<user_name>*** devNetAddr=***<device_ip_address>*** devName=***<device_name>*** devSerialNo=***<device_serial_number>*** OID=***<fortiguard_identification_number>*** msg=***"coldstart (<trap_serial_number>) received from <device_ip_address>"***
Meaning	The specified device received the coldstart SNMP MIB.

High Availability

Event-high availability, or HA, log messages are recorded when there is a cluster of FortiGate units in high availability mode. Event-HA log messages are identified by the number `52001`.

52001

- Groups have the same priority, HA cannot be intitialized.
- Group or Group Password doesn't match, HA cannot be initialized.
- GroupId or Password does not match, HA cannot be setup.
- The HA Slave joined the cluster, Protection is up!
- Backup System is out of sync with primary.
- Switch Over occurs between Peer System is rebooted.
- Switch Over occurs because Monitor Port in Peer System is down.
- The HA Slave is lost, the protection is down.
- The HA switchover happened, because the peer side is down.
- HA status changed at a specified time.
- One of the Monitor port is down.
- The FortiManager version or build does not match. HA cannot be initialized.
- HA status changed at a specified time.
- HA cannot be set up because the subordinate unit cannot fully restore the primary unit's configuration.
- The subordinate unit reconnected as the primary unit in the HA cluster; however, HA protection will be down and it may be possible that the subordinate unit cannot receive heartbeat for a period of time.
- Another FortiManager unit has connected as the primary unit in the HA cluster and HA will re-elect the original primary unit.
- The sequence number received by the subordinate unit does not match the expected sequence number and HA is going down.
- The subordinate unit's synchronization process timed out.
- The subordinate unit's synchronization process lost one heartbeat.
- The HA status changed to UP at the specified time stated.
- The HA status changed to DOWN at the specified time stated.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Groups have the same priority, HA cannot be intitialized."***
Meaning	Groups have the same priority, HA cannot be intitialized.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Group or Group Password doesn't match, HA cannot be initialized."*
Meaning	Group or Group Password doesn't match, HA cannot be initialized.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"GroupId or Password does not match, HA cannot be setup."*
Meaning	GroupId or Password does not match, HA cannot be setup.

Message ID	52001
Log Type	Event-HA
Severity	Alert
FortiManager version	4.0
Message	user=*<user_name>* msg=*"The HA Slave joined the cluster, Protection is up!"*
Meaning	The HA Slave joined the cluster, Protection is up!

Message ID	52001
Log Type	Event-HA
Severity	Error
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Backup System is out of sync with primary"*
Meaning	Backup System is out of sync with primary.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Switch Over occurs between Peer System is rebooted"*
Meaning	Switch Over occurs between Peer System is rebooted.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Switch Over occurs because Monitor Port in Peer System is down."***
Meaning	Switch Over occurs because Monitor Port in Peer System is down.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"The HA Slave is lost, the protection is down."***
Meaning	The HA Slave is lost, the protection is down.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"The HA switchover happened, because the peer side is down."***
Meaning	The HA switchover happened, because the peer side is down.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"HA role changed: <status --> status>"***
Meaning	HA status changed at a specified time.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"One of the Monitor Port is down, switchover is in process."***
Meaning	One of the Monitor port is down.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FMG Version or build doesn't match, HA cannot be initialized."*
Meaning	The FortiManager version or build does not match. HA cannot be initialized.

Message ID	52001
Log Type	Event-HA
Severity	Error
FortiManager version	4.0
Message	user=*<user_name>* msg=*"HA cannot be setup because Slave cannot fully restore the master's configuration."*
Meaning	HA cannot be set up because the subordinate unit cannot fully restore the primary unit's configuration.

Message ID	52001
Log Type	Event-HA
Severity	Alert
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Slave reconnected as master, HA protection will go down, reason: Possible slave cannot receive heartbeat for a while!!"*
Meaning	The subordinate unit reconnected as the primary unit in the HA cluster; however, HA protection will be down and it may be possible that the subordinate unit cannot receive heartbeat for a period of time.

Message ID	52001
Log Type	Event-HA
Severity	Alert
FortiManager version	4.0
Message	user=*<user_name>* msg=*"Another FMG connected as master role, HA will re-elect master!!"*
Meaning	Another FortiManager unit has connected as the primary unit in the HA cluster and HA will re-elect the original primary unit.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"SeqNo received by Slave is not matched expected SeqNo, HA is going down"***
Meaning	The sequence number received by the subordinate unit does not match the expected sequence number and HA is going down.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Slave Sync Time out."***
Meaning	The subordinate unit's synchronization process timed out.

Message ID	52001
Log Type	Event-HA
Severity	Critical
FortiManager version	4.0
Message	user=***<user_name>*** msg=***"Slave Sync lost one HeartBeat."***
Meaning	The subordinate unit's synchronization process lost one heartbeat.

Message ID	52001
Log Type	Event-HA
Severity	Information
FortiManager version	4.0(MR1 and higher)
Message	user=***<user_name>*** msg=***"HA status change: Status=UP, time=<dayofweek_month_date_hh:mm:ss_year>"***
Meaning	The HA status changed to UP at the specified time stated.

Message ID	52001
Log Type	Event-HA
Severity	Information
FortiManager version	4.0(MR1 and higher)
Message	user=***<user_name>*** msg=***"HA status change: Status=DOWN, time=<dayofweek_month_date_hh:mm:ss_year>"***
Meaning	The HA status changed to DOWN at the specified time stated.

Message ID	52001
Log Type	Event-HA
Severity	Information
FortiManager version	4.0(MR1 and higher)
Message	user=***<user_name>*** msg=***"HA app sync error: time=<dayofweek_month_date_hh:mm:ss_year> module=<module_name>"***
Meaning	There was a HA application synchronization error at the specified time.

FortiGuard service

Event-FortiGuard service are recorded when a connection to the FDS server occurs, or any other related service request, such as from a managed device or an update package. Event-FortiGuard service log messages are identified by the number `58001`.

58001

- The FortiManager failed to connect to the FDS.
- The FortiManager unit received an update package, such as antivirus engine, from the FDS for a specific FortiGuard service which includes its version number.
- The FortiManager unit received an update package from the FDS for a specific FortiGuard service, which includes its version number.
- The FortiManager unit received an update request from the specified managed device.
- The FortiManager unit failed to receive a response from the FDS server. The host name of the server and port number is included.

Message ID	58001
Log Type	Event-FortiGuard service
Severity	Errof
FortiManager version	4.0(MR1 and higher)
Message	user=***\<user_name\>*** msg=***"Failed to connect fds server. host:\<ip_address or fqdn\> port:\<port_number\>"***
Meaning	The FortiManager failed to connect to the FDS.

Message ID	58001
Log Type	Event-FortiGuard service
Severity	Information
FortiManager version	4.0(MR1 and higher)
Message	user=***\<user_name\>*** msg=***"Receive an update package from FDS, type=\<FortiGuard service type_number_identification\> version=\<version_number\>"***
Meaning	The FortiManager unit received an update package, such as antivirus engine, from the FDS for a specific FortiGuard service which includes its version number.

Message ID	58001
Log Type	Event-FortiGuard service
Severity	Information
FortiManager version	4.0(MR1 and higher)
Message	user=***<user_name>*** msg=***"Sending UDP announcement to <ip_address>:<port_number>"***
Meaning	The FortiManager unit received an update package from the FDS for a specific FortiGuard service, which includes its version number.

Message ID	58001
Log Type	Event-FortiGuard service
Severity	Information
FortiManager version	4.0(MR1 and higher)
Message	user=***<user_name>*** msg=***"Receive device update request, SN=<device_serial_number>, Address=<device_internal_Ipaddress>"***
Meaning	The FortiManager unit received an update request from the specified managed device.

Message ID	58001
Log Type	Event-FortiGuard service
Severity	Error
FortiManager version	4.0(MR1 and higher)
Message	user=***<user_name>*** msg=***"Failed to recv response from fds server. host:<ip_address or fqdn> port:<port_number>"***
Meaning	The FortiManager unit failed to receive a response from the FDS server. The host name of the server and port number is included.

FortiClient Manager

Event-FortiClient manager log messages are recorded when an event occurred with regards to FortiClient Manager. Event-FortiClient manager log messages are identified by the number `61001`. If you have selected *Debug I/O log event* in the *Event Log* list, the Event-FortiClient manager log messages contain the log identification number `67001`.

61001

- A new client group was added.
- A new enterprise client license was added.
- An enterprise client license was removed.
- A specified FortiClient is registered as a managed client.
- A specified FortiClient was locked down.
- The specified FortiClients are receiving a configuration file.
- A specified FortiClient received the configuration file.
- Configurations were retrieved from the specified FortiClients.
- A client group was changed.
- A client group was removed.
- A FortiClient was removed.
- A new FortiClient license key was added.
- A FortiClient license key was removed.
- A new firmware release is available for FortiClient on the Fortinet Distribution Server (FDS).

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Add new client group (<sequential_number>)"*
Meaning	A new client group was added.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Add new enterprise client license (<license_number>)"*
Meaning	A new enterprise client license was added.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Remove the enterprise client license (<license_number>)"*
Meaning	An enterprise client license was removed.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: FortiClient (<name>, ip=<ip_address>) uid=<identification_number> registered as managed client"*
Meaning	A specified FortiClient is registered as a managed client.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Done send lockdown to client (<client_name>, ip=<ip_address>)"*
Meaning	A specified FortiClient was locked down.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Deploy configuration to client(s): (<client_name1>, <client_name2>, <client_name3> …)"*
Meaning	The specified FortiClients are receiving a configuration file.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Done deploy configuration to client (<client_name1>, <client_name2>, <client_name3> …)"*
Meaning	A specified FortiClient received the configuration file.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Retrieve configurations from client(s): (<client_name1>, <client_name2>, <client_name3> …)"*
Meaning	Configurations were retrieved from the specified FortiClients.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Edit client group (sequential_number)"*
Meaning	A client group was changed.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Refresh dynamic grouping"*
Meaning	

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Remove client group (<sequential_number>)"*
Meaning	A client group was removed.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=*<user_name>* msg=*"FCM: Remove client (<client_name>, ip=<ip_address>) uid=<identification_number>"*
Meaning	A FortiClient was removed.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"FCM: Added a new FortiClient license key (<license _number>)"*
Meaning	A new FortiClient license key was added.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"FCM: Removed FortiClient license key (<license_number>)"*
Meaning	A FortiClient license key was removed.

Message ID	61001
Log Type	Event-FortiClient Manager
Severity	Information
FortiManager version	4.0
Message	user=***<user_name>*** msg=*"FCM: New official release upgrade package (<firmware_version><package_name>) is available on FDS"*
Meaning	A new firmware release is available for FortiClient on the Fortinet Distribution Server (FDS).

www.fortinet.com

FÜRTINET®

www.fortinet.com