FortiManager v5.0 Patch Release 1
Log Message Reference

FortiManager v5.0 Patch Release 1 Log Message Reference

February 01, 2013

02-501-181036-20130201

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2012-11-21	Initial release.
2012-02-01	Updated for FortiManager v5.0 Patch Release 1.

Introduction

This reference provides detailed information about FortiManager log messages. This reference is intended for administrators that have 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.

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 v5.0 Patch Release 1 and higher.
- You have enabled logging of FortiManager events. If you have not enabled logging, see the *FortiManager v5.0 Patch Release 1 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 v5.0 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 "FortiManager v5.0.1 Logs and Updates" on page 7.

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 v5.0.1 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, eventfortiguard-fortimanager protocol. The event log type is the only log type recorded by the FortiManager unit.

- Event-System
- Event-FortiGuard-FortiManager protocol
- Event-Script Manager
- Event-Web Portal
- Event-Policy Console
- Event-Deployment Manager
- Event-Real-Time Monitor
- Event-High Availability (HA)
- Event-FortiGuard service
- Event-Object Change
- Event-Device Manager

FortiManager v5.0.1 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 v5.0 Patch Release 1, see the *FortiManager v5.0 Patch Release 1 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 v4.0, 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 v5.0 maintenance releases.

FortiManager v5.0 Patch Release 1 log message updates

In FortiManager v5.0 Patch Release 1, many log messages have been removed or merged into other log message types. There are log types in *System Settings > General > Log Access > 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 1: Supported and unsupported log types in FortiManager v5.0.1

Supported Log Types	Unsupported Log Types
Device Manager	Endpoint Manager
Deployment Manager	Firewall Objects
FortiGuard service	FortiMail Manager
FortiGuard-FortiManager protocol	Log & Report Manager
High Availability (HA)	Revision History
Object Change	VPN Console
Policy Console	
Real-Time Monitor	
Script Manager	
System	
Web Portal	

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 > General > 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 nine sub-categories under the event log file, which are shown in Table 2. Event-System contains all log messages that the FortiManager unit generates and is the only log file generated.

Figure 1: Log access page
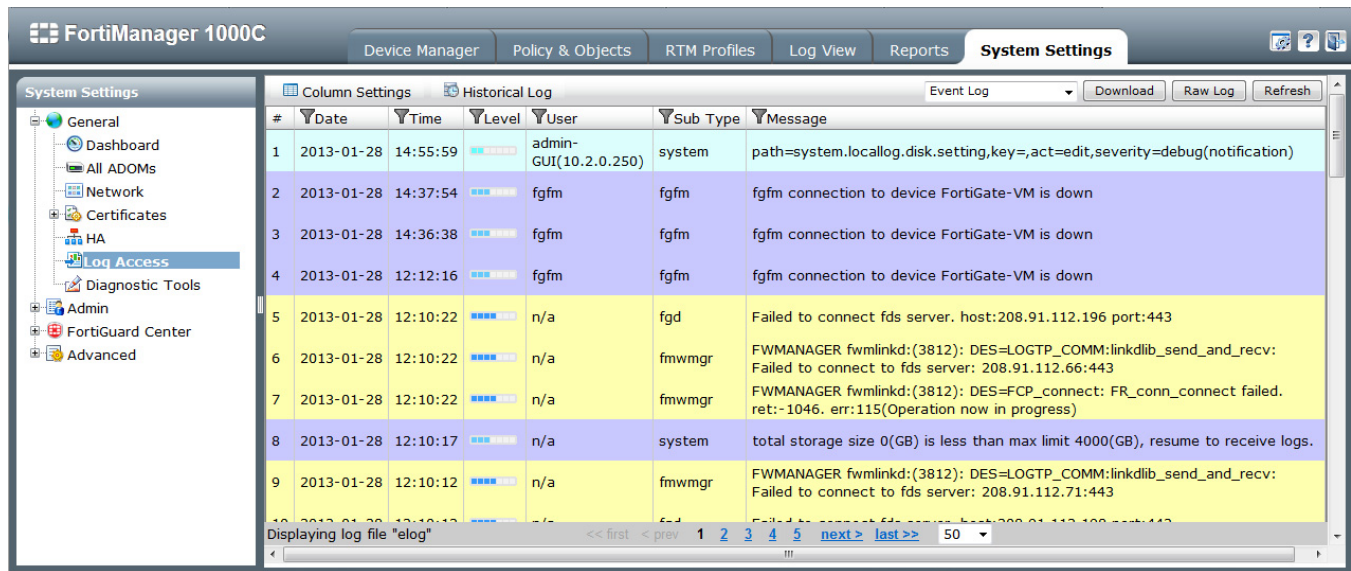
Log types and subtypes

FortiManager logs have only one log type and nine subtypes. The type and subtype numbers are combined in the *log_id* field. There are ten numbers; the first two identify the type of log, and the second two numbers identify the subtype. The last five numbers identify the log. For example, 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 2: Subtype categories and numbers for Event log type

Event Subtype Categories	Subtype Category Number
System	00
FortiGuard-FortiManager protocol	01
Script Manager	04
Web Portal	05
Policy Console	07
Deployment Manager	11

Table 2: Subtype categories and numbers for Event log type (continued)

Event Subtype Categories	Subtype Category Number
Real-Time Monitor	12
High Availability (HA)	14
FortiGuard service	16
Object Change	20
Device Manager	21

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.

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

Table 3: Logging severity levels

Level	Description
0 - Emergency	The system has become unusable.
1 - Alert	Immediate action is required.
2 - Critical	Functionality is affected.
3 - Error	An erroneous condition exists, and functionality is probably affected.
4 - Warning	Functionality could be affected.
5 - Notification	Information about normal events.
6 - Information	General information about system operation.
7 - Debug	Detailed information useful for debugging purposes.

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 3000C 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 4: Explanation of the Event-System log message example

Log Field	Description
date = 2009-04-05	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=OBLT0000, 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 the version number.

Event-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 the message ID 10001.

10001 Event-System

1.	
Severity	Critical
Message	user=<user_name> msg="System restart"
Description	The system restarted

2a.	
Severity	Critical
Message	msg="Power <number> goes to online"
Description	A power supply has been switched on.

2b.	
Severity	Critical
Message	msg="Power <number> goes to offline"
Description	A power supply has been switched off.

3.	
Severity	Critical
Message	msg="System shutdown (Power Button)"
Description	The system has been shutdown via the power button.

5.	
Severity	Error/Information
Message	msg="raid disk <disk number> status changed from <disk_status> to <disk_status>"
Description	The specified RAID disk status has been changed The possible status values are: • None - No RAID detected or status is unknown. • OK - Everything is OK. • Degraded - At least one failed disk, but RAID is still functioning. • Fail - RAID does not work anymore, the RAID has to be deleted, and re-created. • Initializing - A one time check ran after RAID was created. • Verifying - Verifying RAID status. • Rebuilding - Rebuilding a failed disk.

6.	
Severity	Error/Information
Message	msg="raid status changed from <status> to <status>"
Description	The RAID status changed. The possible status values are: • None - No RAID detected or status is unknown. • OK - Everything is OK. • Degraded - At least one failed disk, but RAID is still functioning. • Fail - RAID does not work anymore, the RAID has to be deleted, and re-created. • Initializing - A one time check ran after RAID was created. • Verifying - Verifying RAID status. • Rebuilding - Rebuilding a failed disk.

8.	
Severity	Warning
Message	user= "" msg= "Log upload failed caused by too many miglogd children running"
Description	Too many FTP/SFTP/SCP child processes are running, causing log upload to fail.

9.	
Severity	Warning
Message	user= "" msg= "Log upload failed caused by invalid FortiAnalyzer setting"
Description	Invalid FortiAnalyzer setting caused log upload to fail. Could be caused by inability to retrieve FortiLog, FortiAnalyzer is disabled, or there is no IP address in the settings.

10.	
Severity	Information
Message	user= "" msg= "Log <log_path> is compressed to <gz_upload_path> successfully"
Description	Log compressed successfully. Reason this message may not appear is if there is not enough disk space to compress or gzip returns an error while compressing.

11.	
Severity	Warning
Message	user= "" msg= "Pid <pid>: Unable to access compressed log: <gz_upload_path>"
Description	Cannot access compressed log.

12.	
Severity	Information
Message	user= "" msg= "Pid <pid>: Log <link_name> uploaded to <location> successfully"
Description	Log was uploaded successfully.

13.	
Severity	Warning
Message	user= "" msg= "Pid <pid>: Log <link_name> uploaded to <location> failed"
Description	Failed to upload log. There can be many reasons why this occurred and an error is shown to the user. Possible reasons are: internal error, system call error, buffer overflow, invalid option, socket buffer full, connection closed, packet too large, invalid packet length, timeout, invalid packet version, ssl connection error.

15.	
Severity	Information
Message	user= "" msg= "Device log <link_name> uploaded to <address> successfully"
Description	Device log uploaded successfully.
	Note: This is displayed incorrect in the code, says failed even though success src/daemon/miglogd/miglog_disk.c.

16.	
Severity	Warning
Message	user= "" msg= "Device log <link_name> uploaded to <address> failed"
Description	Failed to upload device log.

17.	
Severity	Warning
Message	user= "" msg= "Clean-up uploaded file: <upload_path>"
Description	File was cleaned up upload directory.

18.	
Severity	Critical
Message	user= "" msg= "System lost power at <year>-<month>-<day> <hour>:<minute>"
Description	System lost power at the specified time.

19.	
Severity	Notification
Message	user=<administrator_name> msg= "Backup all settings succeed"
Description	All settings were backed up successfully.

20.	
Severity	Warning
Message	user=<administrator_name> msg= "Backup all settings failed"
Description	Failed to back up all settings.
	Prior to seeing this message in the logs, there should be reason(s) why back up failed. (ie. "SFTP Timeout: Network is unreachable" or "FTP error: FTP service is unavailable") Look up descriptions for those log messages for further explanation.

21.	
Severity	Alert
Message	user=<user_name> msg= "user '<user_name>' login failed from ssh(<remote ip_address>)"
Description	A user failed to log in from an SSH client.
	Reasons for failure include: user name does not exist in the CMDB, login remote IP is invalid, or the IP is blocked.

22.	
Severity	Notification
Message	user=<administrator_name> msg= "metafield added: <object_type>: name=<name>, length=<length>, importance=<importance>, status=<status>"
Description	A metafield was added.

23.	
Severity	Notification
Message	user=<administrator_name> msg= "metafield changed: <object_type>: name=<name>, length=<length>, importance=<importance>, status=<status>"
Description	A metafield was changed.

24.	
Severity	Notification
Message	user=<administrator_name> msg= "metafield deleted: <object_type>: name=<name>, length=<length>, importance=<importance>, status=<status>"
Description	A metafield was deleted.

25.	
Severity	Notification
Message	user=<user_name> msg= "Device profile <original_profile_name> is <unable to rename | renamed> as <new_profile_name>"
Description	The specified device profile was either renamed or unable to be renamed as the specified new profile name.

26.	
Severity	Notification
Message	user=<user_name> msg= "Device <device ID> added to profile '<profile_name>' <failed | successfully>"
Description	The specified device was added to the specified profile either succeeded or failed.

27.	
Severity	Notification
Message	user=<user_name> msg= "Device <device ID> removed from profile '<profile_name>' <failed | successfully>"
Description	The specified device was removed from the specified profile either succeeded or failed.

28.	
Severity	Notification
Message	user=<user_name> msg= "Device association for profile '<profile_name>' is <unable to change | changed>"
Description	The specified device association for the specified profile was changed or unable to be changed.

29.	
Severity	Notification
Message	user=<user_name> msg= "Configuration copied from profile '<profile_name>' to device <device_id> <failed | successfully>"
Description	Copy all configurations from the specified profile to the specified device failed or were successfully copied. This process includes specified attributes, removing the original device settings, and filtering out disabled and unsupported categories.

30.	
Severity	Notification
Message	user=<administrator_name> msg= "A new policy <type> <name> is <creation_status>
Description	Created or unable to create a new policy package or folder.

31.	
Severity	Notification
Message	user=<administrator_name> msg= "A policy <type> <name> is <deletion status>"
Description	Deleted or unable to delete a policy package or folder.

32.	
Severity	Notification
Message	user=<administrator_name> msg= "A policy <type> <name> is <rename status> as <new_name>"
Description	Renamed or unable to rename a policy package or folder.

33.	
Severity	Notification
Message	user=<administrator_name> msg= "A policy package installation target <name> is <change status>"
Description	Changed or unable to change a policy package.

34.	
Severity	Notification
Message	user=<user_name> msg= "A new device profile <profile_name> is <created	unable to create>"
Description	The specified new device profile is created or was unable to be created. Failure to create new profile can be caused by duplicate name entry.

35.	
Severity	Notification
Message	user=<user_name> msg= "Device profile <profile_name> is <unable to delete	deleted>"
Description	The specified device profile was deleted or could not be deleted.

36.	
Severity	Notification
Message	user=<user_name> msg= "Device <device_id> add to device profile failed"
Description	Failed to add the specified device to the device profile, most likely because it failed to find the profile object.

37.	
Severity	Information
Message	user=<user_name> msg= "user '<user_name>' logout from FortiConsole(<CLI_address>)"
Description	A user logged out from FortiConsole. Note: FortiConsole is not supported in v5.0.0 or later.

38.	
Severity	Notification
Message	user=<administrator_name> msg= "deleted checkpoint"
Description	A system checkpoint was deleted.

39.	
Severity	Notification
Message	user=<administrator_name> msg= "create system checkpoint failed"
Description	Failed to create system checkpoint. May be caused by failure to back up global data, failure to back up device configuration, or wrap system checkpoint failed.

40.	
Severity	Notification
Message	user=<administrator_name> msg= "create system checkpoint succeeded"
Description	System checkpoint was created successfully.

41.	
Severity	Notification
Message	user=<administrator_name> msg= "revert system checkpoint failed"
Description	Failed to revert system checkpoint. Possible causes are: invalid system checkpoint ID, check system checkpoint revision failed, unwrap system checkpoint failure, failed to restore global data, or failure to restore device revision.

42.	
Severity	Notification
Message	user=<administrator_name> msg= "revert system checkpoint succeeded"
Description	System checkpoint revert succeeded.

43.	
Severity	Information
Message	user=<user_name> msg= "user '<login_user>' with profile '<admin_profile>' timed out from <user_from>"
Description	A user timed out.

44.	
Severity	Notification
Message	user=<user_name> msg= "path=<path>,key=<config_object>,act=<act>,<config_attribute>"
Description	Log message configuration with path, key, and other information.

45.	
Severity	Information
Message	user=<login_user> msg= "user '<login_user>' with profile '<admin_prof>' login accepted from <user_from>"
Description	User login information.

46.	
Severity	Information
Message	user=<login_user> msg= "user '<login_user>' with profile '<admin_prof>' <exit status> from <user_from>"
Description	User logout/timeout information.

47.	
Severity	Notification
Message	user=<administrator_name> msg= "FIPS mode enable Success | Failure"
Description	FIPS mode is enabled successfully or failed.

48.	
Severity	Alert
Message	user=<user_name> msg= "user '<user_name>' with profile '<admin_prof>' login failed from <user_from> because of declined disclaimer"
Description	User failed to login because of declined disclaimer.

50.	
Severity	Critical
Message	user=<user_name> msg= "Failed to restore all settings because of the TFTP transmission error."
Description	Failed to restore all settings because of TFTP transmission error.

51.	
Severity	Critical
Message	user=<user_name> msg= "Failed to restore all settings because of the invalid backup file."
Description	Failed to restore all settings because of invalid backup file.

52.	
Severity	Critical
Message	user=<user_name> msg= "Failed to restore all settings because decrypt backup file failed."
Description	Failed to restore all settings because decrypt backup file failed.

53.	
Severity	Critical
Message	user=<user_name> msg= "Failed to restore all settings."
Description	Failed to restore all settings for reasons other than 51. and 52.

54.	
Severity	Critical
Message	user=<user_name> msg= "Restore all settings"
Description	All settings restored.

56.	
Severity	Critical
Message	user=<user_name> msg= "Failed to restore all settings because of the SCP transmission error."
Description	Failed to restore all settings from SCP server.

62.	
Severity	Critical
Message	user=<user_name> msg= "Failed to install FortiAnalyzer Package because of the TFTP transmission error."
Description	Failed to install FortiAnalyzer package because of the TFTP transmission error.

63.	
Severity	Critical
Message	user=<user_name> msg= "Failed to restart the lrmd process to install new FortiAnalyzer package"
Description	Failed to restart the lrmd process to install new FortiAnalyzer package.

64.	
Severity	Notification
Message	user=<administrator_name> msg= "Administrator <administrator_name> initiates all self-tests from <user_from>"
Description	Administrator initiated all self-tests.

65.	
Severity	Critical
Message	user=<user_name> msg= "Firmware <upgrade/downgrade> from v<Major_number>.0-build<build number> <build date> (Interim) to <version>-build<build number><branch><patch>"
Description	Firmware is being upgraded or downgraded.

66.	
Severity	Critical
Message	user=<user_name> msg= "Failed to do the firmware upgrade because of the TFTP transmission error."
Description	Failed to do the firmware upgrade because of the TFTP transmission error.

67.	
Severity	Critical
Message	user=<user_name> msg= "Failed to do the firmware upgrade because of the invalid image file."
Description	Failed to do the firmware upgrade because of the invalid image file.

68.	
Severity	Critical
Message	user=<user_name> msg= "Failed to do the firmware upgrade."
Description	Failed to do the firmware upgrade.

69.	
Severity	Critical
Message	user=<user_name> msg= "Failed to do the firmware upgrade because of the FTP transition error."
Description	Failed to do the firmware upgrade because of the FTP transition error.

72.	
Severity	Critical
Message	user=<user_name> msg= "System restart v<Major_number>.0-build<build number> <build date> (Interim)"
Description	System restart with software version information after adding VM license.

74.	
Severity	Critical
Message	user=<administrator_name> msg= "System shutdown (CLI)"
Description	System shutting down via the CLI.

75.	
Severity	Information
Message	user=<administrator_name> msg= "Privileged system access granted to user '<administrator_name>'"
Description	Privileged system access granted to administrator.

76.	
Severity	Information
Message	user=<administrator_name> msg= "User '<administrator_name>' exited from the privileged system"
Description	Administrator exited from privileged system.

77.	
Severity	Notification
Message	user=<administrator_name> msg= "system time changed: <original_time> ---> <new_time>"
Description	System time was changed.

79.	
Severity	Notification
Message	user=<administrator_name> msg= "hostname changed: <old_hostname> --> <new_hostname>"
Description	Hostname was changed.

88.	
Severity	Information
Message	user=<administrator_name> msg= "System prepare upgrade from version[<major version>], build[<buid_number>],branchpt[<branch>] to version[<major version>], build[<buid_number>],branchpt[<branch>]"
Description	System is preparing for software version upgrade.

89.	
Severity	Critical
Message	user=<user_name> msg= "System v<Major_number>.0-build<build number> <build date> (Interim) restart to upgrade"
Description	System restart to upgrade FortiManager version.

90.	
Severity	Emergency
Message	user=n/a msg= "Entering FIPS error mode due to '<error string>'"
Description	Entering FIPS error mode due to error described by error string.

91.	
Severity	Alert
Message	user=n/a msg= "EVP encryption failed"
Description	EVP encryption failed.

92.	
Severity	Alert
Message	user=n/a msg= "EVP Decryption failed"
Description	EVP decryption failed.

93.	
Severity	Warning
Message	msg= "SFTP Timeout: Network is unreachable"
Description	SFTP timeout, network is unreachable.

94.	
Severity	Warning
Message	msg= "SFTP session error: <error number>(<error message>)"
Description	SFTP session error with information including error number and message.

96.	
Severity	Warning
Message	msg= "SFTP session is closed"
Description	SFTP session is closed.

97.	
Severity	Warning
Message	msg= "SFTP session read error: <error number>(<error message>)"
Description	SFTP session read error with error information including error number and message.

98.	
Severity	Warning
Message	msg= "SFTP error: Cannot connect to server"
Description	Cannot connect to server

99.	
Severity	Warning
Message	msg= "SFTP error: Error password or invalid directory permission"
Description	SFTP error, error password or invalid directory permission.

100.	
Severity	Warning
Message	msg= "SFTP error: Failed to change the directory"
Description	SFTP error, failed to change the directory.

101.	
Severity	Warning
Message	msg= "SFTP error: Invalid directory"
Description	SFTP error, invalid directory, directory cannot be found.

102.	
Severity	Warning
Message	msg= "SFTP error: File transfer error"
Description	SFTP error, file transfer error.

103.	
Severity	Warning
Message	msg= "SFTP error: rename file error"
Description	SFTP error, rename file error.

104.	
Severity	Warning
Message	msg= "SFTP error: The file cannot be found"
Description	SFTP error, file cannot be found.

105.	
Severity	Warning
Message	msg= "SFTP error: No permission to upload"
Description	SFTP error, no permission to upload.

106.	
Severity	Warning
Message	msg= "SCP Timeout: data transmission is aborted"
Description	SCP timeout, data transmission is aborted.

107.	
Severity	Warning
Message	msg= "SCP session error: <error number>:(<error message>)"
Description	SCP session error with error information such as error number and message.

108.	
Severity	Warning
Message	msg= "SCP Timeout: Network is unreachable"
Description	SCP timeout, network is unreachable.

109.	
Severity	Warning
Message	msg= "SCP session is closed"
Description	SCP session is closed.

110.	
Severity	Warning
Message	msg= "SCP session read error: <error number>:(<error message>)"
Description	SCP session read error with error information including error number and message.

111.	
Severity	Warning
Message	msg= "SCP error: Cannot connect to server <server ip>"
Description	SCP error, cannot connect to server.

112.	
Severity	Warning
Message	msg= "SCP error: Invalid password or directory permission denied"
Description	SCP error, invalid password or directory permission denied.

113.	
Severity	Warning
Message	msg= "SCP error: No such file or directory"
Description	SCP error, no such file or directory.

120.	
Severity	Warning
Message	msg= "SCP error: Invalid certificate or directory permission denied"
Description	Error certificate or permission denied.

122.	
Severity	Warning
Message	msg= "FTP error: Network is unreachable"
Description	FTP error, network is unreachable.

125.	
Severity	Warning
Message	msg= "FTP error: FTP service is unavailable"
Description	Connect to FTP service failed.

126.	
Severity	Warning
Message	msg= "FTP error: Login failed"
Description	FTP error, login failed.

127.	
Severity	Warning
Message	msg= "FTP error: Wrong password"
Description	FTP error, wrong password.

128.	
Severity	Warning
Message	msg= "FTP error: Change binary mode error"
Description	FTP error, change binary mode error.

129.	
Severity	Warning
Message	msg= "FTP error: Change directory error"
Description	FTP error, change directory error.

130.	
Severity	Warning
Message	msg= "FTP error: The remote directory or file cannot be found"
Description	FTP error, the remote directory or file cannot be found.

131.	
Severity	Warning
Message	msg= "FTP error: File transfer error"
Description	FTP error, file transfer error.

132.	
Severity	Warning
Message	msg= "FTP error: Permission denied"
Description	FTP error, permission denied.

133.	
Severity	Warning
Message	msg= "FTP error: The file cannot be found"
Description	FTP error, the file cannot be found.

134.	
Severity	Alert
Message	user=<user_name> msg= "user '<user_name>' login failed from <console/telnet>(<opt_host | n/a>) cause system lockout"
Description	User login failed from telnet/console caused system lockout.

135.	
Severity	Alert
Message	user=<user_name> msg= "user '<user_name>' login failed from console"
Description	User login failed from console.

136.	
Severity	Alert
Message	user=<user_name> msg= "user '<user_name>' login failed from telnet(<opt_host>)"
Description	User login failed from telnet.

137.	
Severity	Information
Message	user=<user_name> msg= "user '<user_name>' with profile '<profile_id>' login accepted from GUI(<client_ip_address>)"
Description	User with a specific profile login accepted from Web-based Manager.

138.	
Severity	Alert
Message	user=<user_name> msg= "user '<user_name>' login failed from GUI(<client_ip_address>)"
Description	A user login failed from Web-based Manager.

139.	
Severity	Information
Message	user=<user_name> msg= "from address '<client_ip_address>' do firmware upgrade. firmware version:<fm_version> fm_release:<fm_release>"
Description	User with given address is trying to do an official firmware upgrade from Web-based Manager.

140.	
Severity	Information
Message	user=<user_name> msg= "from address '<client_ip_address>' do firmware upgrade. firmware version:<fm_version> build number:<build_num>"
Description	User with given address is trying to do a special firmware upgrade from Web-based Manager.

143.	
Severity	Information
Message	user=<user_name> msg= "user '<user_name>' with profile '<profile_id><profile_name>' logout from GUI(<client_ip_address>)"
Description	A user logged out from Web-based Manager.

145.	
Severity	Information
Message	user=<administrator_name> msg= "The session of the user '<user_name>' from <user_from> is killed"
Description	A user session is killed.

146.	
Severity	Notification
Message	user=<administrator_name> msg= "<keyname> license key changed"
Description	License key changed.

147.	
Severity	Warning
Message	user=<administrator_name> msg= "Invalid <keyname> license key"
Description	Invalid license key.

151.	
Severity	Notification
Message	user=<administrator_name> msg= "<CA/local> certificate exported: <cert>"
Description	CA or local certificate is exported.

154.	
Severity	Notification
Message	user=<user_name> msg= "Event log has been cleared by user '<user_name>'"
Description	Event log has been cleared by user.

158.	
Severity	Information
Message	user=<administrator_name> msg= "The Policy Package <package_name>(<policy_description>) is being installed"
Description	A policy package with the given name and description is being installed.

Event-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 message ID 13001.

13001 Event-FortiGuard-FortiManager protocol

2.	
Severity	Alert
Message	user=fgfm msg= "fgfm protocol start, offline mode is <enable | disable>"
Description	FortiGuard-FortiManager protocol is being started and the status of offline mode is displayed.

3.	
Severity	Warning
Message	user=fgfm msg= "fgfm connection to device <device_name> is down"
Description	FortiGuard-FortiManager connection to the device with the given device name is down.

4.	
Severity	Information
Message	user=fgfm msg= "fgfm connection to device <device_name> is up"
Description	FortiGuard-FortiManager connection to the device with the given name is up.

Event-Script Manager

Event-Script Manager log messages are recorded when there are changes to scripts (creation, deletion, or modification). Event-Script Manager log messages are identified by the message ID 22001.

22001 Event-Script Manager

2.	
Severity	Information
Message	msg= "create script <script_name> ok"
Description	A script with the given name is created successfully.

3.	
Severity	Information
Message	msg= "delete script <script_id> ok"
Description	A script with the given script ID is deleted successfully.

4.	
Severity	Information
Message	msg= "modify script <script_name> ok
Description	A script with the given script name is modified successfully.

Event-Web Portal

Event-Web Portal log messages are identified by the message ID 25001.

25001 Event-Web Portal

1.	
Severity	Variable
Message	user=<administrator_name> msg= "Refresh remote FMG devices succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to refresh remote FortiManager devices.

2.	
Severity	Variable
Message	user=<administrator_name> msg= "Configure profile <id> succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to configure profile with given ID.

3.	
Severity	Variable
Message	user=<administrator_name> msg= "Add <content> <id> (<enabled | disabled>) succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to add specific content with given ID.

4.	
Severity	Variable
Message	user=<administrator_name> msg= "Change <content> <id> (<enabled | disabled>) succeeded widget=<widget_name> action=<action>"
Description	Succeeded or failed to change specific content with given ID.

5.	
Severity	Variable
Message	user=<administrator_name> msg= "Delete <content> <id> succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to delete specific content with given ID.

6.	
Severity	Variable
Message	user=<administrator_name> msg= "Select logo <id> on profile <profile_name> succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to save selected logo with given ID on the profile with specific name.

7.	
Severity	Variable
Message	user=<administrator_name> msg= "Reset logo to default on profile <profile_name> succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to reset logo to the default image on the specified profile.

8.	
Severity	Variable
Message	user=<administrator_name> msg= "Delete logo <id> on profile <profile_name>succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to delete logo with given ID on the specific profile.

9.	
Severity	Variable
Message	user=<administrator_name> msg= "Add module <id> on profile <profile_name> succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to add a module with given ID on the specified profile.

10.	
Severity	Variable
Message	user=<administrator_name> msg= "Save layout on profile <profile_name> succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to save the layout of the specified profile.

11.	
Severity	Variable
Message	user=<administrator_name> msg= "Upload new logo on profile <profile_name> succeeded | failed widget=<widget_name> action=<action>"
Description	Succeeded or failed to upload a new logo onto the specified profile.

12.	
Severity	Variable
Message	user=<administrator_name> msg= "<error message>"
Description	Daemon error described by error message.

13.	
Severity	Variable
Message	user=<administrator_name> msg= "Session <data> loaded in ptmgr"
Description	Session with the given data is loaded into Portal Manager.

14.	
Severity	Variable
Message	user=<administrator_name> msg= "Processed job using <data> handler"
Description	Processed job using specified handler.

15.	
Severity	Variable
Message	user=<administrator_name> msg= "User <id> login from <ip_address> succeeded | failed"
Description	User with specified ID logged in from given IP address succeeded or failed.

16.	
Severity	Variable
Message	user=<administrator_name> msg= "User <id> logout"
Description	User with specified ID logged out.

17.	
Severity	Variable
Message	user=<administrator_name> msg= "Session <session_id> timed out"
Description	Specified session with given ID timed out.

Event-Policy Console

Event-Policy Console log messages are recorded when events or activities are occurring within the Security Console menu. Event-policy console log messages are identified by the message ID 31001.

31001 Event-Policy Console

4.	
Severity	Information
Message	user=<user_name> msg= "Policy installed on adom=<adom_oid> device=<device_id>"
Description	A policy was installed within the specified ADOM by the specified device.

5.	
Severity	Error
Message	user=<user_name> msg= "Device <device_id> is not locked., <task title>"
Description	Specified device is not locked and the title of the task trying to do the install is displayed.

5.	
Severity	Error
Message	user=<user_name> msg= "Get devinfo fail or device in backup mode. dev:<device_id>, <task title>"
Description	Failed to get device information or the device backup mode. The device ID is showed as well as the title of the task.

5.	
Severity	Error
Message	user=<user_name> msg= "Connect to device failed. dev:<device_id>, <task_title>"
Description	Failed to connect to the specified device as well as the title of the task.

5.	
Severity	Error
Message	user=<user_name> msg= "version mismatched, adom:<adom_mr>,dev:<device_mr>, <task_title>"
Description	The version on the ADOM and the device do not match.

5.	
Severity	Error
Message	user=<user_name> msg= "Set mm ops failed, adom:<adom_oid>, dev:<device_name>, <task_title>"
Description	Failed to set mm ops on the specified ADOM and device name.

5.	
Severity	Error
Message	user=<user_name> msg= "Start transaction failed, adom:<adom_oid>, dev:<device_name>, <task_title>"
Description	Failed to start transaction on the specified ADOM and device name.

5.	
Severity	Error
Message	user=<user_name> msg= "Preparing device failed, adom:<adom_oid>, dev:<device_name>, <task_title>"
Description	Failed while preparing the device with ADOM and device name information.

6.	
Severity	Error
Message	user=<user_name> msg= "Device vdom(<vdom_name>) is a slave mirror vdom, <task_title>"
Description	The specified device VDOM is a slave mirror VDOM.

6.	
Severity	Error
Message	user=<user_name> msg= "Device vdom(<vdom_name>) was unlocked, <task_title>"
Description	The specified device VDOM was not locked.

6.	
Severity	Error
Message	user=<user_name> msg= "Validation failed, cancelled by user, <task_title>"
Description	Validation failed because it was cancelled by the user.

6.	
Severity	Error
Message	user=<user_name> msg= "Copy rollbacked, due to error, <task_title>"
Description	Copy was rolled back due to an error.

6.	
Severity	Error
Message	user=<user_name> msg= "Copy rollbacked, cancelled by user, <task_title>"
Description	Copy rolled back because the action was cancelled by the user.

7.	
Severity	Error
Message	user=<user_name> msg= "Failed to commit policies to devdb, <task_title>"
Description	Failed to commit policies to device database.

7.	
Severity	Error
Message	user=<user_name> msg= "Aborted due to previous error, <task_title>"
Description	Process aborted due to previous error.

7.	
Severity	Error
Message	user=<user_name> msg= "Install failed(dev-related info was changed, install it first), <task_title>"
Description	Policy installation failed because device related information was changed, install device related information first.

7.	
Severity	Error
Message	user=<user_name> msg= "Initiate install to real device failed, <task_title>"
Description	Failed to initiate installation to real device.

11.	
Severity	Error
Message	user=<user_name> msg= "Create policy context failed, <task_title>"
Description	While compiling policy, create policy context failed.

11.	
Severity	Error
Message	user=<user_name> msg= "Malloc memory failed, <task_title>"
Description	While compiling policy, malloc memory failed.

11.	
Severity	Error
Message	user=<user_name> msg= "Init fetch context failed, <task_title>"
Description	While compiling policy, initiate fetch context failed.

11.	
Severity	Error
Message	user=<user_name> msg= "create task lines failed, <task_title>"
Description	While compiling policy, create task lines failed.

11.	
Severity	Error
Message	user=<user_name> msg= "Calloc memory failed, <task_title>"
Description	While compiling policy, calloc memory failed.

11.	
Severity	Error
Message	user=<user_name> msg= "fork error, <task_title>"
Description	While compiling policy, fork process error.

12.	
Severity	Error
Message	user=<user_name> msg= "Error create policy ctx, <task_title>"
Description	Error creating policy context.

12.	
Severity	Error
Message	user=<user_name> msg= "Loading device error, <task_title>"
Description	Loading device error.

12.	
Severity	Error
Message	user=<user_name> msg= "No installing devices, <task_title>"
Description	Error installing devices.

12.	
Severity	Error
Message	user=<user_name> msg= "Load_gms_policies error, <task_title>"
Description	Function used to load GMS policies returned an error.

12.	
Severity	Error
Message	user=<user_name> msg= "Load_gms_central_nat error, <task_title>"
Description	Loading GMS central NAT returned an error.

12.	
Severity	Error
Message	user=<user_name> msg= "Load_profile_group error, <task_title>"
Description	Error loading profile group.

12.	
Severity	Error
Message	user=<user_name> msg= "Load pkg setting error, <task_title>"
Description	Error loading package settings.

13.	
Severity	Information
Message	user=<user_name> msg= "Assigning global policy package '<package_name>' to adom=<adom_name> successful"
Description	Successfully assigned global policy package with specified name to given ADOM.

14.	
Severity	Information
Message	user=<user_name> msg= "Assigning global policy package '<package_name>' to adom=<adom_name> failed"
Description	Failed to assign global policy package with specified name to given ADOM.

Event-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 message ID 43001.

43001 Event-Deployment Manager

2.	
Severity	Notification
Message	user=<user_name> msg= "device <device_name> <action> failed"
Description	Specified device import/reload failed.

3.	
Severity	Notification
Message	user=<user_name> msg= "device <device_name> <action> succeeded"
Description	Specified device import/reload succeeded.

4.	
Severity	Information
Message	user=<user_name> msg= "device <device_name> add <succeeded	failed>"
Description	Adding specified device succeeded or failed.

5.	
Severity	Information
Message	user=<user_name> msg= "device <device_name> delete <succeeded	failed>"
Description	Delete specified device succeeded or failed.

6.	
Severity	Information
Message	user=fgfm msg= "device <device_name> configuration is synchronized"
Description	Specified device configuration is synchronized.

7.	
Severity	Information
Message	user=fgfm msg= "device <device_name> configuration is out-of-sync"
Description	Specified device's configuration is out-of-sync.

8a.	
Severity	Information
Message	user=<administrator_name> msg= "Install of <script_type> script '<script_name>' on policy package <package_name> at <time> succeed"
Description	Successfully installed TCL or CLI script of given name on specified policy package at the given time.

8a.	
Severity	Information
Message	user=<administrator_name> msg= "Install of <script_type> script '<script_name>' on device '<device_name>' (devid=<device_id>) at <time> succeed"
Description	Successfully installed TCL or CLI script of given name on specified device at given time.

8b.	
Severity	Information
Message	user=<administrator_name> msg= "Script install <script_name> on policy package <package_name> cancelled"
Description	Specified script install to policy package was cancelled.

8b.	
Severity	Information
Message	user=<administrator_name> msg= "Script install <script_name> on policy package <package_name> failed"
Description	Failed to install specified script to policy package.

8b.	
Severity	Information
Message	user=<administrator_name> msg= "Script install <script_name> on <device_name> cancelled"
Description	Specified script install to device was cancelled.

8b.	
Severity	Information
Message	user=<administrator_name> msg= "Script install <script_name> on <device_name> failed"
Description	Failed to install specified script to device.

9a.	
Severity	Information
Message	user=<user_name> msg= "Security Console revision ID <revision_num>, saved by install operation, by operator <user_name>"
Description	Security console revision ID saved by install operation.

9b.	
Severity	Information
Message	user=<user_name> msg= "Security Console revision ID <revision_num>, manually saved by operator <user_name>"
Description	Security console revision ID manually saved by operator.

9c.	
Severity	Information
Message	user=<user_name> msg= "Security Console revision ID(<revision_num>), revert successfully"
Description	Successfully revert security console revision ID.

9d.	
Severity	Information
Message	user=<user_name> msg= "Security Console revision ID(<revision_num>), manually deleted by operator (<user_name>)"
Description	Security console revision ID manually deleted by user.

10.	
Severity	Information
Message	user=<user_name> msg= "Security Console revision ID(<revision_num>), revert fail"
Description	Failed to revert security console revision ID.

11.	
Severity	Information
Message	user=<user_name> msg= "Save revision <revision_num> to <device_hostname>(<device_serialnumber>)"
Description	Save revision to specified device.

12.	
Severity	Information
Message	user=<user_name> msg= "Retrieve revision <revision_num> from <device_hostname>(<device_serialnumber>)"
Description	Retrieve revision from specified device.

13.	
Severity	Information
Message	user=<user_name> msg= "Import revision <revision_num> to <device_hostname>(<device_serialnumber>)"
Description	Import revision from specified device.

14.	
Severity	Information
Message	user=<user_name> msg= "Load revision <revision_number> from <device_hostname>(<device_serialnumber>)"
Description	Load revision from specified device.

15.	
Severity	Information
Message	user=<user_name> msg= "Edit revision(<revision_number>) for <device_hostname>(<device_serialnumber>): Updated revision comment"
Description	Edit revision comment from specified device.

15.	
Severity	Information
Message	user=<user_name> msg= "Edit revision(<revision_number>) for <device_hostname>(<device_serialnumber>): Updated tag name from "<old tag_name>" to "<new tag name>""
Description	Updated tag name for revision for specified device.

16.	
Severity	Information
Message	user=<user_name> msg= "Revert to revision (<revision number>) for <device_hostname>(<device_serialnumber>) <result>"
Description	Success/fail to revert to specified revision for specified device.

17.	
Severity	Information
Message	user=<user_name> msg= "Install revision(<revision number>) to <device_hostname>(<device_serialnumber>) successfully"
Description	Successfully installed specified revision to device.

17.	
Severity	Information
Message	user=<user_name> msg= "Install revision(<revision number>) to <device_hostname>(<device_serialnumber>) failed(<reason>)"
Description	Failed to install specified revision to device and the reason.

18.	
Severity	Information
Message	user=<user_name> msg= "Delete revision(<revision number>) for <device_hostname>(<device_serialnumber>)"
Description	Specified revision was deleted from device.

19.	
Severity	Information
Message	user=<user_name> msg= "Downloaded configuration revision(<revision number>) for <device_hostname>(<device_serialnumber>)"
Description	Downloaded configuration of specified revision from device.

20.	
Severity	Information
Message	user=<admin> msg= "Cancel scheduled global installation succeed for adom(<adom_id>)"
Description	Successfully cancelled the scheduled global installation for specific ADOM.

21.	
Severity	Information
Message	user=<admin> msg= "Cancel scheduled global installation fail for adom(<adom_id>)"
Description	Failed to cancel scheduled global installation for specified ADOM.

22.	
Severity	Information
Message	user=<user_name> msg= "Schedule install succeed for device(<device_id>)"
Description	Scheduled installation succeeded for specified device.

23.	
Severity	Information
Message	user=<user_name> msg= "Schedule install fail for device(<device_id>)"
Description	Scheduled installation failed for specified device.

24.	
Severity	Information
Message	user=<admin> msg= "Cancel scheduled installation succeed for device(<device_id>)"
Description	Successfully cancelled scheduled installation for specified device.

25	
Severity	Information
Message	user=<admin> msg= "Cancel scheduled installation fail for device(<device_id>)"
Description	Failed to cancel scheduled installation for specified device.

26.	
Severity	Information
Message	user=<user_name> msg= "Import revision failed"
Description	Failed to import revision.

27.	
Severity	Information
Message	user=<user_name> msg= "Import revision successful"
Description	Import revision succeeded.

Event-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 message ID 46001.

46001 Event-Real-Time Monitor

2.	
Severity	Notification
Message	devNetAddr=<device_ip_address> devName=<device_name> devSerialNo=<device_serial_number> OID=<oid> msg= "<trap_name> (<trap_serial_number>) received from <device_ip_address>"
Description	Specified trap was received from given device.

3.	
Severity	Alert
Message	type=<alert_type> id=<ID> events=<number of incidents> msg= "<alert_type> <id> triggered alert"
Description	Monitor/trap/console/reachable ID triggered the alert.

Event-High Availability (HA)

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 message ID 52001.

52001 Event-High Availability (HA)

2a.	
Severity	Information
Message	msg= "HA sync: attempting to connect to slaves"
Description	Attempting to connect to slaves.

2b.	
Severity	Information
Message	msg= "HA sync: attempting to connect to master"
Description	Attempting to connect to master.

2c.	
Severity	Information
Message	msg= "HA sync: successful sync with <{slave	master}> <peer_ip>"
Description	Successfully synchronized with slave or master with given IP.

2e.	
Severity	Information
Message	msg= "HA sync: all slaves connected, start full sync"
Description	All slaves are connected, can start full synchronization.

2f.	
Severity	Information
Message	msg= "HA sync: negotiating with <peer_ip>"
Description	Negotiating with IP.

2g.	
Severity	Information
Message	msg= "HA sync: negotiating with master"
Description	Negotiating with master.

3.	
Severity	Information/Alert
Message	msg= "HA status change: status=<up | down>"
Description	HA status change.

4.	
Severity	Information
Message	msg= "peer <peer_serial_number> is locally disabled"
Description	Specified peer is locally disabled.

5.	
Severity	Information
Message	msg= "sending image to <device_serial_number>"
Description	Image is currently being sent to specified device.

6.	
Severity	Information
Message	msg= "sending image to <device_serial_number> <failed | ok>"
Description	Succeeded or failed to send image to specified device.

Event-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 message ID 58001.

58001 Event-FortiGuard Service

2.	
Severity	Error
Message	msg= "FDS fmupdate tftp import update manage package failed. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate TFTP import update manage package failed.

3.	
Severity	Information
Message	msg= "FDS fmupdate tftp import update manage package success. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate TFTP import update manage package success.

4.	
Severity	Error
Message	msg= "FDS fmupdate ftp import update manage package failed. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate FTP import update manage package failed.

5.	
Severity	Information
Message	msg= "FDS fmupdate ftp import update manage package success. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate FTP import update manage package success.

6.	
Severity	Error
Message	msg= "FDS fmupdate scp import update manage package failed. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate SCP import update manage package failed.

7.	
Severity	Information
Message	msg= "FDS fmupdate scp import update manage package success. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate SCP import update manage package success.

8.	
Severity	Error
Message	msg= "FDS fmupdate tftp export update manage package failed. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate TFTP export update manage package failed.

9.	
Severity	Information
Message	msg= "FDS fmupdate tftp export update manage package success. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate TFTP export update manage package success.

10.	
Severity	Error
Message	msg= "FDS fmupdate ftp export update manage package failed. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate FTP export update manage package failed.

11.	
Severity	Information
Message	msg= "FDS fmupdate ftp export update manage package success. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate FTP export update manage package success.

12.	
Severity	Error
Message	msg= "FDS fmupdate scp export update manage package failed. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate SCP export update manage package failed.

13.	
Severity	Information
Message	msg= "FDS fmupdate scp export update manage package success. package type:<package_type> file:<file_name> Server:<server_ip>"
Description	FDS fmupdate SCP export update manage package success.

14.	
Severity	Information
Message	msg= "Virus statistical notification to FDS network Changed: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	The virus statistical notification to FDS network has been changed from disabled/enabled to enabled/disabled.

15.	
Severity	Information
Message	msg= "FGD DB Changed: <old URL DB> --> <new URL DB>"
Description	FortiGuard database changed from old URL database to new URL database.

16.	
Severity	Information
Message	msg= "FGT Support Version. <old supported versions> --> <new supported versions>"
Description	List of the new FortiGate supported versions.

17.	
Severity	Information
Message	msg= "FCT Support Version. <old supported versions> --> <new supported versions>"
Description	List of the new FortiClient supported versions.

18.	
Severity	Information
Message	msg= "FML Support Version. <old supported versions> --> <new supported versions>"
Description	List of the new FortiMail supported versions.

19.	
Severity	Information
Message	msg= "FAZ Support Version. <old supported versions> --> <new supported versions>"
Description	List of the new FortiAnalyzer supported versions.

20.	
Severity	Information
Message	msg= "FSW Support Version. <old supported versions> --> <new supported versions>"
Description	List of the new FortiSwitch supported versions.

21.	
Severity	Information
Message	msg= "{fmupdate.av-ips	fmupdate.web-spam	fmupdate.av-ips.fgt	fmupdate.av-ips.fct} Status: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	Status change of the specified service from disabled/enabled to enabled/disabled.

22.	
Severity	Information
Message	msg= "{fmupdate.av-ips	fmupdate.web-spam	fmupdate.av-ips.fgt	fmupdate.av-ips.fct} New Override Server List(<sequential number>): IP:<ip_address>, TimeZone: <port>"
Description	New override server list with IP address and port information given.

23.	
Severity	Information
Message	msg= "Push override <service_type> port Changed: <old port> --> <new port>"
Description	FDS service changed, push override of specified service type port changed from old port to the specified new port.

24.	
Severity	Information
Message	msg= "Push override <service_type> ip Changed: <old ip_address> --> <new ip_adress>"
Description	FDS service changed, push override of specified service type IP changed from old IP to the specified new IP address.

25.	
Severity	Information
Message	msg= "Announce IP List Status: {Disabled | Enabled} --> {Disabled | Enabled}"
Description	Status of announce IP has been changed.

26.	
Severity	Information
Message	msg= "Announce IP List: IP:<ip_address>, Port: <port>"
Description	Announce IP list with IP address and port number.

27.	
Severity	Information
Message	msg= "Server Poll Frequency <service_type> Changed: <old poll frequency> --> <new poll frequency>"
Description	The server poll frequency of the specified service type is changed from the old poll frequency to the new specified one.

28.	
Severity	Information
Message	msg= "UM proxy <service_type> Status Changed: {Disabled | Enabled} --> {Disabled | Enabled}"
Description	UM proxy of the specific service type is changed from previous status to the new status.

29.	
Severity	Information
Message	msg= "UM proxy <service_type> Mode Changed: <Proxy | Tunnel> --> <Proxy | Tunnel>"
Description	UM proxy of the specific service type has mode changed from proxy or tunnel to proxy or tunnel.

30.	
Severity	Information
Message	msg= "UM proxy <service_type> port Changed: <old port> --> <new port>"
Description	UM proxy of the specific service type port changed from previous port to new port number.

31.	
Severity	Information
Message	msg= "UM proxy <service_type> ip Changed: <old ip_address> --> <new ip_address>"
Description	UM proxy of the specific service type IP changed from previous IP to the new IP address.

32.	
Severity	Information
Message	msg= "FCT Service status changed: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	FortiClient service status changed.

33.	
Severity	Information
Message	msg= "FCT Service port Changed: <old port> --> <new port>"
Description	FortiClient service port changed to the new port number.

34.	
Severity	Information
Message	msg= "Log Update From FDS: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	Log update from FDS is changed.

35.	
Severity	Information
Message	msg= "Log FGT Update History: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	Log for FortiGate update history is changed.

36.	
Severity	Information
Message	msg= "FDS Update Schedule Status: {Disabled | Enabled} --> {Disabled | Enabled}"
Description	Status for FDS update schedule is changed.

37.	
Severity	Information
Message	msg= "FDS Update Schedule Frequency: <old frequency> --> <new frequency>"
Description	FDS update schedule frequency changed to the new frequency.

38.	
Severity	Information
Message	msg= "FDS Update Schedule Time(D H:M)<day> <hour>:<minute> --> <day> <hour>:<minute>"
Description	FDS update schedule time is changed.

39.	
Severity	Information
Message	msg= "Private Server Settings. Allow FGT access public server: {Disabled | Enabled} --> {Disabled | Enabled}"
Description	Private server settings for allowing FortiGate to access public server is changed.

40.	
Severity	Information
Message	msg= "Private Server Settings. Serverlist for AVIPS: {Disabled | Enabled} --> {Disabled | Enabled}"
Description	Private server settings. Server list for antivirus/IPS is changed.

41.	
Severity	Information
Message	msg= "Private Server Settings. Serverlist for WebSpam: {Disabled | Enabled} --> {Disabled | Enabled}"
Description	Server list for Web Spam is changed.

42.	
Severity	Information
Message	msg= "New Private Server List(<sequential number>): IP:<ip_address>, TimeZone: <time_zone>"
Description	List of private servers with their IP and time zone information.

43.	
Severity	Information
Message	msg= "FDS WebSpam Query Log Status : {Disabled	Enabled} --> {Disabled	Enabled}"
Description	FDS Web Spam query log status is changed.

44.	
Severity	Information
Message	msg= "FDS WebSpam Query URL Log: {URL Log disable	Log Rating Misses	Log ALL URL lookups} --> {URL Log disable	Log Rating Misses	Log ALL URL lookups}"
Description	FDS Web Spam Query URL Log changed.

45.	
Severity	Information
Message	msg= "FDS WebSpam Query Spam Log: {Spam Log disable	Log Non-spam events	Log all Spam lookups}"
Description	FDS Web Spam Query Spam Log is changed.

46.	
Severity	Information
Message	msg= "FDS Service AVIPS: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	FDS service antivirus/IPS status is changed.

47.	
Severity	Information
Message	msg= "FDS Service WebSpam: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	FDS service Web Spam status is changed.

48.	
Severity	Information
Message	msg= "Use certificate: {FortiGuard	BIOS} --> {FortiGuard	BIOS}"
Description	Certificate being used is changed.

49.	
Severity	Information
Message	msg= "FDS Service Connect public network: {Disabled	Enabled} --> {Disabled	Enabled}"
Description	Connect to public network status is changed.

50.	
Severity	Information
Message	msg= "FDS Server Override Mode: {Loose	Strict} --> {Loose	Strict}"
Description	FDS server override mode status is changed.

51.	
Severity	Warning
Message	msg= "Receive a URL rating request, result=miss, ip=<ip_address>, SN=<device_id> URL=[<URL>]"
Description	Received a URL rating request but the result is a miss. Details of the request are then displayed. (ie. IP address, device ID and the URL).

52.	
Severity	Information
Message	msg= "Receive a URL rating request, result=hit, ip=<ip_address>, SN=<device_id> URL=[<URL>]"
Description	Received a URL rating request but the result is a hit. Details of the request are then displayed. (ie. IP address, device ID and the URL).

54.	
Severity	Warning
Message	msg= "Receive a Spam rating request, result=Spam, ip=<ip_address>, SN=<device_id>"
Description	This query is deemed a spam, coming from the device with given IP address and device ID.

55.	
Severity	Information
Message	msg= "Receive a Spam rating request, result=Non-spam, ip=<ip_address>, SN=<device_id>"
Description	Received a spam rating request and this query is not deemed as spam, coming from device with given IP address and device ID.

60.	
Severity	Information
Message	msg= "Web-filter/Anti-spam service rate to FortiGuard:<requests/minute> requests/minute"
Description	Amount of Web Filter and Antispam service requests per minute.

61.	
Severity	Information
Message	msg= "Receive a new device request, SN=<serial number>, Address=<ip_address>"
Description	A new device is added with the given serial number and IP address.

62.	
Severity	Information
Message	msg= "Receive a new device request, SN=<serial number>"
Description	A new device is added with only the given serial number as information.

63.	
Severity	Information
Message	msg= "Manual Deployment to serial:[<serial_number>]"
Description	Manually deploying configuration to device with given serial number.

64.	
Severity	Error
Message	msg= "Failed to connect fds server. host:<server host> port:<server port>"
Description	Failed to connect to FDS server with the given server host and port information.

65.	
Severity	Error
Message	msg= "Failed to send request to fds server. host:<server host> port:<server port>"
Description	Failed to send request to FDS server with given server host and port information.

66.	
Severity	Error
Message	msg= "Failed to receive response from fds server. host:<server host> port:<server port>"
Description	Failed to receive response from FDS server with given host and port information.

67.	
Severity	Information
Message	msg= "Sending UDP announcement to <ip_address>:<port>"
Description	Sending UDP announcement to specified IP address and port number.

68.	
Severity	Information
Message	msg= "Receive an update package from FDS, type=<type>, version=<version>"
Description	Received an update package from FDS with specified type and version.

69.	
Severity	Information
Message	msg= "Received a device update request, SN=<serial_number> UID=<user_id>"
Description	Received a device update request from device with given serial number and the UID of whom sent the request.

70	
Severity	Information
Message	msg= "Received a device update request, SN=<serial_number>, Address=<peer ip_address>"
Description	Received a device update request from device with given serial number and the peer IP address.

71.	
Severity	Information
Message	msg= "Received a device update request, SN=<serial_number>, object: <obj_path>, pre_version: <full_version>, new_version: <new full_version>"
Description	Received a FortiClient update request with the given information, IP address is not logged when it is FortiClient information.

72.	
Severity	Information
Message	msg= "Received a device update request, SN=<serial_number>, Address=<ip_address>, object: <obj_path>, pre_version: <full_version>, new_version: <new full_version>"
Description	Received a device update request from device with given serial number. The change in version number is also displayed as well.

76.	
Severity	Information
Message	msg= "Receive an update package from FDS, firmware=<firmware>, type=<type>, version=<version>"
Description	Received an update package from FDS with the given firmware number, type, and version number.

80.	
Severity	Critical
Message	msg= "FortiGuard Service: Disk usage has exceeded disk quota!"
Description	FortiGuard service disk quota has been exceeded.

81.	
Severity	Warning
Message	msg= "FortiGuard Service: Disk usage is near disk quota! Over <percentage used>% used!"
Description	FortiGuard service disk usage is as the specified percentage of quota.

82.	
Severity	Error
Message	msg= "This is proxy error, no need retry"
Description	There is a proxy error so there is no reason to retry because it will always fail.

83.	
Severity	Error
Message	msg= "Polling failed. give up."
Description	Polling failed, do not retry.

84.	
Severity	Error
Message	msg= "Polling failed. service disabled"
Description	Polling failed because the service was disabled

85.	
Severity	Error
Message	msg= "Generate whitelist[<index>]: Can not get sublist_shm"

Description	Generating whitelist but cannot get shared memory sublist
	
	Whitelist is composed of every device which has:
	
	   (1) valid license and registered (in devices.txt or redistuid.txt), or
	
	   (2) valid license and non-registered but UM_ACCEPT_UNREGDEV_ENABLE_SERVICE is set.

86.	
Severity	Error
Message	msg= "<function name>: Can not attach shared memory. err:<error number>(<error message>)"
Description	Could not attach to shared memory and the function where this error occurred with the given error number and a specific error message.

87.	
Severity	Error
Message	msg= "<function name>: Failed to detach sublist shared memory, err:<error number>(<error message>)"
Description	Failed to detach sublist shared memory and the function where this error occurred along with the error number and a specific error message.

88	
Severity	Error
Message	msg= "Can not switch to new shared memory new_shmid:<shmid>"
Description	Cannot switch to the specified new shared memory.

89.	
Severity	Error
Message	msg= "sub_check_contract: shm_handler is NULL"
Description	Handler is NULL meaning there is most likely no such user.

90.	
Severity	Error
Message	msg= "sub_check_contract: sublist is NULL"
Description	There are no sublist entries.

91.	
Severity	Warning
Message	msg= "[<service name>] subscriber update: shmid=<shmid> handler_id=<handler_id> return=<return value> whitelist_size=[<wf_size>,<as_size>]"
Description	Whitelist did not update because shared memory switch was not successful. The shared memory ID, handler ID and other information are given.

93.	
Severity	Warning
Message	user=fgdsvr msg= "Fail to attach share memory(id=FGD) for 10 seconds"
Description	Failed to attach shared memory after 10 seconds.

95.	
Severity	Information
Message	user=fgdsvr msg= "<service_name>: --STAT-- [query=<query_counter>, rated=<rater_query_counter>, db-query=<db_query_counter>] in <duration> minutes"
Description	Display the query counters for all query, rated query, and database query and how much time was used.

96.	
Severity	Warning
Message	user=fgdsvr msg= "<svc_name>: INIT request(unauthorized): ip=<requester ip_address>, sn=<device id>, license_type=<license_type>, expiration=<expiration date>, setup=<need_setup>"
Description	FortiGuard has invalid license. Information regarding the device, (ie. IP, device ID, license type, expiration and the setup) is shown.

97.	
Severity	Warning
Message	user=fgdsvr msg= "<svc_name>: SPAM query(unauthorized): ip=<requester ip_address> sn=<device_id>"
Description	FortiGuard has invalid license. IP address and device ID of the requester is given.

107.	
Severity	Warning
Message	user=fgdsvr msg= "<svc_name>: upddb was broken, drop it!"
Description	Error caused by an issue with the update database. Either because there was an issue with accessing the database information, or checking database validation for the db_path failed.

108.	
Severity	Warning
Message	user=fgdsrv msg= "<svc_name>: Update rundb, upddb_ver=<uppdb_version> rundb_ver<rundb_version>
Description	Database needs an update, and the database currently being used will now be updated from the specified version to the version of the update database.

113.	
Severity	Warning
Message	user=fgdsvr msg= "<svc_name>: URL query(unauthorized): ip=<requester ip_address>, sn=<device_id>"
Description	FortiGuard has invalid license. IP address and device ID of the requester is given.

118.	
Severity	Warning
Message	user=fgdupd msg= "Make tmp_db failed."
Description	Failed to make temporary database.

119.	
Severity	Warning
Message	user=fgdupd msg= "<svc_name> db was broken"
Description	The specified database failed database check validation.

Event-Object Change

Event-Object Change log messages are recorded when an event occurred with regards to copying objects to the global level. These log messages are identified by the message ID 70001.

70001 Event-Object Change

2.	
Severity	Information
Message	user=<user_name> msg= "copy objects to global fail"
Description	Failed to copy objects to global level.

2.	
Severity	Information
Message	user=<user_name> msg= "copy objects to global succeed"
Description	Objects were copied to global level successfully.

Event-Device Manager

Event-Device Manager log messages are recorded when an event occurred with regards to a change with the device configuration. Event-Device Manager log messages are identified by the message ID 73001.

73001 Event-Device Manager

1-1.	
Severity	Notification
Message	user=<user_name> msg= "Updated device <device_name> (device_serial_number)"
Description	The device was updated without error.

1-2.	
Severity	Notification
Message	user=<user_name> msg= "Retrieved device <device_name> (<device_serial_number>) config"
Description	Successfully retrieved configuration from the device.

1-3.	
Severity	Notification
Message	user=<user_name> msg= "Added device <device_name> (<device_serial_number>)"
Description	Successfully added the specified device.

1-4.	
Severity	Notification
Message	user=<user_name> msg= "Deleted device <device_name> (<device_serial_number>)"
Description	Successfully deleted the specified device.

1-5.	
Severity	Information
Message	user=<user_name> msg= "Chassis '<device_name>' <object_type> #<index>: <sensor_name> is <sensor_state> (current: <sensor_value>)"
Description	Log of the sensor state and some information regarding the sensor. Object type can be voltage sensor, current sensor, temperature sensor, power-entry module, fan, shelf manager, power module, shelf alarm panel, extension card, link, slot, EEPROM, or unknown. The sensor state can be unknown, ok, blow lower non-critical, below lower-critical, blow lower non-recoverable, above upper non-critical, above upper critical, above upper non-recoverable, or error.

1-6.	
Severity	Warning
Message	user=<user_name> msg= "Chassis '<device_name>' <object_type> #<index>: <sensor_name> is <sensor_state> (threshold: <threshold_value>, current: <sensor_value>)"
Description	Sensor value is nearing the threshold value generating this warning log.

1-7.	
Severity	Notification
Message	user=<user_name> msg= "Added chassis <chassis_name>"
Description	Added a new chassis.

1-8.	
Severity	Notification
Message	user=<user_name> msg= "Deleted chassis <chassis_name>"
Description	Delete the specific chassis.

1-9.	
Severity	Notification
Message	user=<user_name> msg= "Restored partially-deleted device <device_name> (<device_serial_number>)"
Description	Restored a partially deleted device.

1-10.	
Severity	Notification
Message	user=<user_name> msg= "Created group <group_name>"
Description	Created a group.

1-11.	
Severity	Notification
Message	user=<user_name> msg= "Deleted group <group_name>"
Description	Delete the specific group.

1-16.	
Severity	Notification
Message	user=taskdb-upgrade msg= "Imported <tasks_copied>/<old_tasks> tasks, <lines_copied>/<old_lines> lines, <history_copied>/<old_history> history"
Description	Details on the data that were imported from old database.

1-17.	
Severity	Notification
Message	user=taskdb-upgrade msg= "Repairing task database"
Description	Trying to re-import/repair task database.

1-18.	
Severity	Notification
Message	user=taskdb-upgrade msg= "Error during task database repair: old data may be partially or completely lost"
Description	Could not repair and the old data may be partially or completely lost.

1-23.	
Severity	Information
Message	user=check-intergrity msg= "Fixed task database counts"
Description	The counter keeping track of the task numbers is fixed

1-24.	
Severity	Notification
Message	user=check-intergrity msg= "DVM integrity check made <number_changes> changes with <number_error> errors"
Description	The numbers of changes made and the number of errors that resulted while performing DVM integrity check.

1-25.	
Severity	Notification
Message	user=<user_name> msg= "Switched ADOM mode to advanced"
Description	Enabling this option will result in a reduced operation mode and more complicated management scenarios. It is recommended only for advanced users.

1-26.	
Severity	Notification
Message	user=<user_name> msg= "Switch ADOM mode to normal"
Description	The ADOM mode has been switch to normal.

1-27.	
Severity	Information
Message	user=<user_name> msg= "Switched to adom <adom_id> from adom <adom_id>"
Description	Switched RAID ADOM.

1-28.	
Severity	Notification
Message	user=<user_name> msg= "Initiated update of chassis <chassis_name> slot <slot_index>"
Description	Initiated update for the specified slot in the chassis.

1-29.	
Severity	Notification
Message	user=<user_name> msg= "Initiated update of chassis <chassis_name>"
Description	Initiated update for the specified chassis.

1-30.	
Severity	Notification
Message	user=<user_name> msg= "Activated chassis <chassis_name> slot <slot_index>"
Description	Rebooting slots, the specific slot from that chassis is activated.

1-31.	
Severity	Notification
Message	user=<user_name> msg= "Deactivated chassis <chassis_name> slot <slot_index>"
Description	Rebooting slots, the specific slot from that chassis is deactivated

1-32.	
Severity	Notification
Message	user=<user_name> msg= "Changed sensor thresholds on chassis <chassis_name>"
Description	The sensor threshold is changed for this chassis.

1-34.	
Severity	Notification
Message	user=<user_name> msg= "Edited group <group_name>"
Description	The specified group is edited.

1-35.	
Severity	Notification
Message	user=<user_name> msg= "Edited device <device_name> (<device_serial_number>)"
Description	The specified device was edited.

1-36.	
Severity	Notification
Message	user=<user_name> msg= "Deleted task <task_id>"
Description	The task was deleted

1-37.	
Severity	Notification
Message	user=<user_name> msg= "Cancelled task <task_id>"
Description	The task was cancelled.

1-38.	
Severity	Notification
Message	user=<user_name> msg= "Disabled adom <adom_id>"
Description	The ADOM was disabled.

1-39.	
Severity	Notification
Message	user=<user_name> msg= "Enabled adom <adom_id>"
Description	The ADOM was enabled.

1-40.	
Severity	Notification
Message	user=<user_name> msg= "Deleted adom <adom_id>"
Description	The ADOM was deleted.

1-44.	
Severity	Notification
Message	user=<user_name> msg= "Moved <number_objects> objects into adom <adom_name> [<object>]"
Description	Moved a certain number of objects into the specified ADOM.

1-46.	
Severity	Notification
Message	user=<user_name> msg= "Edited adom <adom_name>"
Description	The ADOM was edited.

1-47.	
Severity	Notification
Message	user=<user_name> msg= "Created adom <adom_name>"
Description	The ADOM was created.

1-53.	
Severity	Notification
Message	user=<user_name> msg= "Exported <number_adoms> adoms, <number_groups> groups, <number_devices> devices"
Description	The number of ADOMs, groups, and devices exported is listed.

1-54.	
Severity	Notification
Message	user=<user_name> msg= "Initiated import of <number_adoms> adoms, <number_groups> groups, <number_devices> devices"
Description	The number of ADOMs, groups, and devices that were imported is listed.

2.	
Severity	Information
Message	user=<administrator_name> msg= "device <device_name> change succeeded"
Description	Device with the specified name was changed successfully.