



FortiMail® Secure Messaging Platform v4.0 MR2
Log Message Reference

Revision 1



15 September 2011

Revision 1

© Copyright 2011 Fortinet, Inc. All rights reserved. Contents and terms are subject to change by Fortinet without prior notice. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.

Trademarks

ABACAS, APSecure, Dynamic Threat Prevention System (DTPS), FortiAnalyzer®, FortiASIC, FortiBIOS, FortiBridge, FortiClient®, FortiDB™, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiMail®, FortiManager®, Fortinet®, FortiOS®, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiScan, FortiShield, FortiVoIP, FortiWeb, 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.

Visit these links for more information and documentation for your Fortinet product:

Technical Documentation - <http://docs.fortinet.com>

Fortinet Knowledge Center - <http://kb.fortinet.com>

Technical Support - <http://support.fortinet.com>

Training Services - <http://training.fortinet.com>

Contents

Introduction	9
FortiMail documentation	9
Fortinet Tools and Documentation CD	9
Fortinet Knowledge Base	9
Comments on Fortinet technical documentation	9
Customer service and technical support.....	10
About FortiMail logs	11
Log types	11
History logs	11
Event logs	12
Antispam logs	12
Antivirus logs	12
Encryption logs	12
Subtypes	13
Severity levels	13
Log message syntax	14
Error log messages.....	15
Log message cross search	15
History	17
Log message dispositions and classifiers	17
Event Config	21
FortiGuard autoupdate settings	22
System update setting	22
interface IP address	22
Access methods/status	23
Interface status.....	23
Interface status/PPPoE status	23
Interface status/PPPoE settings	23
Management IP	24
Interface access methods	24
MTU change.....	24
Interface status.....	24
Addressing mode of interface access methods	24
Connect option of interface access methods	25
DNS change	25

Primary DNS and secondary DNS	25
Default gateway	25
Route entry	26
Route with destination IP address/netmask.....	26
Routing entry	26
System timezone	26
Daylight saving time	27
NTP server settings	27
System time	27
Console pageNo setting	27
Console mode setting.....	27
Idle timeout	28
Authentication timeout	28
System language.....	28
LCD PIN number.....	28
LCD PIN protection	29
GUI refresh interval.....	29
System idle and auth timeout	29
Admin addition	29
Admin change	30
Admin deletion	30
Admin password change.....	30
HA settings	30
SNMP status	30
SNMP config info	31
SNMP CPU threshold.....	31
SNMP memory threshold	31
SNMP Logdisk threshold.....	31
SNMP maildisk threshold	32
SNMP deferred mqueue threshold	32
SNMP virus detection threshold.....	32
SNMP spam detection threshold	32
SNMP community entry	32
SNMP community and host entry	33
FortiMail disclaimer in header for outgoing messages	33
FortiMail disclaimer in body for incoming messages	33

FortiMail disclaimer in header for incoming messages	33
Local domains	34
POP3 server port number	34
Relay server name	34
SNMP memory threshold	34
SMTP auth.....	35
SMTP over ssl.....	35
SMTP server port number	35
Status of email archiving.....	35
Email archiving account.....	35
Email archiving rotate setting.....	36
Archiving settings on local server	36
Archiving settings on remote server.....	36
Archiving policy	36
Archiving exempt	37
System quarantine account	37
System quarantine rotate setting	37
System quarantine quota settings	37
System quarantine settings	37
Mail server settings.....	38
FortiMail appearance information	38
FortiMail mail gw user group	38
Permission of mail	38
Mail server access	39
Local domain deletion	39
Local domain addition	39
Local user	39
Local domain name.....	40
User group.....	40
Mail user addition/deletion.....	40
Mail server user addition.....	40
Mail server user set with information.....	40
Mail server user added with information	41
Mail server user deletion	41
Disk quota of email archiving account	41
Password of email archiving account.....	41

Forwarding address for email archiving	42
Password of system quarantine account	42
Forwarding address for system quarantine	42
Password of mail user	42
Display name of mail user	42
User alias	43
POP3 auth profile	43
IMAP auth profile.....	43
Email banned word	43
Local log setting.....	44
Memory log setting	44
Log setting.....	44
Log setting elog	44
Log policy	44
Alertemail setting	45
Alertemail SMTP server	45
Alertemail target email addresses.....	45
Alertemail configuration	45
Event System.....	47
DNS servers.....	47
System restart	47
System shutdown	47
System reload.....	48
System reset.....	48
System firmware upgrade	48
Upgrade system firmware failed.....	48
System mode.....	49
Event Update	51
FortiGuard update result	51
Event SMTP	53
SMTP-related events.....	53
Starting flgrptd	53
Virus db loaded	54
FortiGuard antispam rule (FSAR) loading	54
FASR readme.....	54

FortiGuard antispam rule (FSAR) loaded	54
Mail aliases rebuilt	54
Antivirus database loaded	55
Updated daemon restarted.....	55
Antivirus database loading	55
Antivirus database loaded	55
Bayesian database training.....	56
Bayesian database training completed.....	56
Event Admin	57
User login.....	57
Webmail login.....	57
User login failure.....	57
WebMail GUI failure	58
Message retrieval failure	58
Message cannot be read	58
Attachment saving failure	58
LCD login	59
LCD login failure	59
Event POP3.....	61
POP3-related events	61
Event IMAP	63
IMAP-related events.....	63
Event HA	65
Master mode	65
Slave mode	65
Master role.....	65
Event Webmail.....	67
User login.....	67
Antivirus.....	69
Example	69
Virus infection	69
Antispam.....	71
Example	71
Spam-related events	71
Deep header scanner rules reload	71

Index..... 73

Introduction

This document introduces you to the log messages generated by the FortiMail unit. This document also includes examples of log messages that the FortiMail unit may generate.

This chapter includes the following topics:

- [FortiMail documentation](#)
- [Customer service and technical support](#)

FortiMail documentation

The most up-to-date publications and previous releases of FortiMail product documentation are available from the Fortinet Technical Documentation web site at <http://docs.fortinet.com>.

Information about the FortiMail unit is available from the following guides:

- **FortiMail QuickStart Guides**
Provides basic information about connecting and installing a FortiMail unit. A separate guide is available for each FortiMail model.
- **FortiMail Administration Guide**
Introduces the product and describes how to configure and manage a FortiMail unit, including how to create profiles and policies, configure antispam and antivirus filters, create user accounts, configure email archiving, and set up logging and reporting.
- **FortiMail Install Guide**
Describes how to set up the FortiMail unit in transparent, gateway, or server mode.
- **FortiMail online help**
Provides a searchable version of the **Administration Guide** in HTML format. You can access online help from the web-based manager as you work.
- **FortiMail Webmail online help**
Describes how to use the FortiMail web-based email client, including how to send and receive email, how to add, import, and export addresses, how to configure message display preferences, and how to manage quarantined email.

Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the [Fortinet Technical Documentation](#) web site.

Fortinet Knowledge Base

Additional Fortinet technical documentation is available from the Fortinet Knowledge Base. It contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the [Fortinet Knowledge Base](#).

Comments on Fortinet technical documentation

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

Customer service and technical support

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

Please visit the [Fortinet Technical Support](#) web site to learn about the technical support services that Fortinet provides.

About FortiMail logs

FortiMail logs can provide information on network email activity that helps identify security issues such as viruses detected within an email.

For information about configuring logging in FortiMail, see the [FortiMail Administration Guide](#).

This section provides information on the following topics:

- [Log types](#)
- [Subtypes](#)
- [Log message cross search](#)
- [Severity levels](#)
- [Log message syntax](#)
- [Error log messages](#)

Log types

FortiMail logs record per recipient, presenting log information in a very different way than most other logs do. By recording logs per recipient, log information is presented in layers, which means that one log file type contains the what and another log file type contains the why. For example, a log message in the history log contains an email message that the FortiMail unit flagged as spam (the what) and the antispam log contains why the FortiMail unit flagged the email message as spam.

FortiMail logs are divided into the following types:

Log Types	File Name	Description
History	alog	Records all email traffic going through the FortiMail unit.
Event	elog	Records management and activity events. Management activity events include changes to the system configuration as well as administrator and user log in and log outs. Activity events include system activities.
Antispam	slog	Records spam detection events.
Antivirus	vlog	Records virus intrusion events.
Encryption	nlog	Records detection of IBE-related events.

Each of these log types contains a session identification (ID) number, located in the session ID field of each log message that is recorded by the FortiMail unit. The session ID corresponds to each of the log types so that the administrator can get all the information about the event or activity that occurred on their network.

History logs

History logs are used to quickly determine the disposition of a message. History logs describe what action was taken by the FortiMail unit. Administrators use the history logs to quickly determine the status of a message for a specific recipient, then either right-click that log message and select *Cross Search*, or click the *Session ID* link. All correlating history, event, antivirus and antispam log messages appear in a new tab where you can find out why that particular action was taken.

In the following log messages, the bolded information indicates what an administrator looks for when using history logs to find out what action was taken, and the antispam log to find out why the action was taken.

(Below is an example of a history log message)

```
2008-01-07 18:19:08 log_id=04000050100 type=statistics subtype=n/a
pri=information session_id=m07NJ62T00110 from="aabb@example.com" mailer=mta
client_name="[172.16.105.99]" resolved=OK to="ccdd@example.com"
message_length=0 virus="" disposition=0x200 classifier=0x12
subject="accounting information"
```

From the disposition, 0x200, we know that the FortiMail unit deferred the delivery of the email message. We then do a session ID cross search to find it within the antispam logs, as in the following:

```
2008-01-07 18:19:08 log_id=0501080300 type=spam subtype=detected
pri=information session_id="m07NJ62T00110" client_name="[172.16.105.99]"
from="aabb@example.com" to="ccdd@example.com" subject="accounting information"
msg="Grey Listing sender"
```

In the above antispam log message, we now know why the FortiMail unit deferred the delivery because the FortiMail unit has the sender in a grey list, which is shown in the message field.

Event logs

Event logs contain log messages that concern network or system activities and events, such as firmware upgrades or password changes. This log type shows what is occurring at the protocol level, as well as the TCP level.

The event log does not have the same relationship with the history log as the antispam or antivirus log does. The event log is not necessarily used for finding the reason why an event occurred because there may not be a corresponding session ID number. Event logs are also usually self-explanatory, meaning they usually give the what and why within the log message.

Antispam logs

Antispam logs provide information pertaining to email messages that are classified as Spam or Ham messages. The antispam logs describe why they were classified, as was shown in the example in ["History logs" on page 11](#).

Antispam log messages describe spammy URI's, black/white listed IP addresses, or other techniques the FortiMail unit used to classify the message. Antispam log messages may also describe message processing errors, such as not handling email that was sent from a specific user.

Antivirus logs

Antivirus logs provide information pertaining to email messages that are classified as virus or suspicious messages. These log messages describe what virus is contained in the email message or in a file attached to the email message.

Administrators use antivirus logs to determine why an attachment was stripped from a file after someone informed them about not receiving an attachment. Administrators may also use this log type to verify why the history log detected a virus.

The session ID is not usually used when looking up an antivirus log message; the time stated in the time field of the log message is usually used as well as using the search method.

Encryption logs

Encryption logs provide information pertaining to IBE email encryption and decryption.

IBE is a type of public-key encryption. IBE uses identities (such as email addresses) to calculate encryption keys that can be used for encrypting and decrypting electronic messages. Compared with traditional public-key cryptography, IBE greatly simplifies the encryption process for both users and administrators. Another advantage is that a message recipient does not need any certificate or key pre-enrollment or specialized software to access the email.

Subtypes

FortiMail logs are grouped into categories by log type and subtype as shown in the table below:

Log Type	Subtype
event	config admin system ha update pop3 imap smtp webmail
virus	virus detect
antispam	spam detect
history	email history
encryption	ibe-encryption

Severity levels

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

Table 1: Logging severity levels in FortiMail 3.0

Levels	Description	Generated by
0-Emergency	The system has become unstable	Emergency messages
1-Alert	Immediate action is required.	NIDS attack log messages.
2-Critical	Functionality is affected.	DHCP
3-Error	An error condition exists and functionality could be affected.	Error messages
4-Warning	Functionality could be affected.	Antivirus, Web filter, email filter and system event log messages.
5-Notice	Information about normal events.	Antivirus, Web Filter, and email filter log messages.
6-Information	General information about system operation.	Antivirus, Web Filter, email filter, log messages, and other event log messages.



Note: FortiMail units log messages when the DNS server is unreachable. The severity level of the log message varies by the number of times that the DNS server could not be reached.

- Warning severity level log message: 15 failures in 5 minutes
- Alert severity level log message: 40 failures in 5 minutes

Log message syntax

All FortiMail 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. The log body contains information on where the log was recorded and what triggered the FortiMail unit to record the log.

For example, if a FortiMail-400 unit recorded an event-imap message, the following log message may be recorded:

```
2006-10-10 10:19:08 log_id=0114000000 type=event subtype=imap pri=debug
user=mail ui=mail action=unknown status=success msg="fortimail_debug000:
user=jww@vjiang-fortinet.com, passwd=123"
```

Table 2: Explanation of the event-imap log message example

2006-10-10	The year, month and day when the event occurred in the format, yy-mm-dd.
10:19:08	The hour, minute and second of when the event occurred
log_id=(0114000000)	An ten-digit number that identifies the log type. The first two digits represent the log type, and the following two digits represent the log subtype. The last six digits are the process ID that FortiMail assigns to the log message.
type=(event)	The section of the system where the event occurred. The log types are event, antivirus, antispam, and history.
subtype=(imap)	The subtype of each log message. In FortiMail 3.0, subtypes are subcategories of a log. In this example, the subtype is a subcategory of the event log, IMAP.
pri=(debug)	The severity level, or priority, or the event. There are seven logging severity levels.
user=(mail)	The name of the user creating the traffic.
ui=(mail)	The location of where the event occurred. The location can be the CLI, GUI (IP Address) or other. In this example, the location of where the event occurred is in Mail.
action=(unknown)	The action that was taken during the event. In this example, the action the user took is unknown. An action can be a user logging into an interface, resetting the FortiMail unit to factory default settings, or switching between modes. Action only appears in event-admin, event-system, event-pop3 and event-imap log messages.
status=(success)	The status of the event. Status can be success, none, or failure.
msg=("fortimail_debug000: user=jww@vjiang-fortinet.com, passwd=123)	Explains the activity or event that the FortiMail unit recorded. In this example, the log message is a debug message.



Note: For FortiMail 3.0 MR3 and up, the log header of all log messages includes the field, `log_part`, which provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

Error log messages

The FortiMail unit records error log messages, which occur in both the event log and anti-spam log. The following explains certain error messages that you may encounter in the event log. More information will be provided in future releases of the **FortiMail Log Message Reference** document.

militer	A militer is an extension of the widely used open source mail transfer agents (MTA), Sendmail and Postfix. It allows administrators to add mail filters very efficiently in the mail-processing-chain of sendmail. For example, militer filters can reject an email message during the SMTP session.
fas_militer	This means FortiMail Antispam Mail filter. This covers all scanning, except antivirus. Antivirus may be included in fas_militer in future FortiMail firmware releases.
sendmail	Sendmail is a mail transfer agent (MTA) and is a well known project of open source, freeware and Unix communities.
dbdaemon	The dbdaemon handles database persistence of some cached data. For example, greylist and sender reputation databases. Both the greylist and sender reputation databases are cached in the militer. The date is saved to the database at hourly intervals to avoid data loss after a system reboot.
mysqld	This is a multi-threading application which needs to start multiple separate threads to handle different but related threading tasks.
Militer (fas_militer): timeout before data read	This type of error message is from sendmail. The message means that sendmail didn't get the response from the militer within an expected time (4 minutes). The email message that is being processed would be temp failed (a 451 reply code would be returned to the sending MTA). A common cause of the timeout is that the DNS server is not configured properly.
Militer_read (fas_militer): cmd read returned 0, expecting 5	Sendmail didn't get the expected data from militer. The email would be temp failed. A cause of this type of error message is a militer crash, meaning the militer code is not able to handle or parse some mal-formed email. This type of error message should not happen often, because the militer in both FortiMail 2.80 and 3.0 is much more robust.

Log message cross search

Since different types of log files record different events/activities, the same SMTP session may be logged in different types of log files.

For example, if the FortiMail unit detects a virus in an email message, this event will be logged in the following types of log files:

- History log -- this is because the history log records the metadata of all the sent and undelivered email messages.
- AntiVirus log -- this is because a virus is detected. The antivirus log has more descriptions of the virus than the history log does.
- Event log -- this is because the FortiMail system's antivirus process has been started and stopped.

To find and display all the log messages triggered by the same SMTP session, you can use the cross search feature, since all the log messages share the same session ID.

Figure 1: Sample log message cross search results

Log Type	Date	Time	From	To	Subject	Message
History	2009-11-02	16:22:00	ll@kjsad	t1@feqa.com	[VIRUS FOUND]viru	
AntiVirus	2009-11-02	16:22:00	ll@kjsad	t1@feqa.com		The file eicarcom4.zip is infected with EICAR_TEST_FILE.
Event	2009-11-02	16:22:00				from=<ll@kjsad>, size=1722, class=0, nrpts=1, msgid=<0e6d01c83842449785900e98c14ac2
Event	2009-11-02	16:22:00				Start of AV process
Event	2009-11-02	16:22:00				Antivirus: cmd=data, reject=554 5.7.1 This email has been rejected. The email has been infected
Event	2009-11-02	16:22:00				End of AV process
Event	2009-11-02	16:22:00				to=<t1@feqa.com>, delay=00:00:00, pri=31722, stat=This email has been rejected. The email has

To do a cross-search of the log messages

- 1 On the FortiMail Web-based manager, go to *Monitor > Log*.
 - 2 When viewing a log message on the *History, Event, AntiVirus, or AntiSpam* tab, click the Session ID of the log message, or right-click the log message and select *Cross Search* from the popup window.
- All correlating history, event, antivirus and antispam log messages with the same session ID will appear in a new tab.

History

This chapter contains information regarding History log messages. History log has a subtype called Email History. History log messages record all mail traffic going through the FortiMail unit.

History logs are used to quickly determine the disposition of a message. History logs describe what action was taken by the FortiMail unit. Administrators use the history logs to quickly determine the status of a message for a specific recipient, then either right-click that log message and select *Cross Search*, or click the *Session ID* link. All correlating history, event, antivirus and antispam log messages appear in a new tab where you can find out why that particular action was taken.

For more information about log message cross search, see [“Log message cross search” on page 15](#).

Example

In this example, an email that was sent to `user1@example.com` contained the word `movie` that was found in a white list.

```
2008-09-24 14:50:09 log_id=0400050100 log_part=00 type=statistics
subtype=n/a pri=information session_id=156Hl9fK001393
from="user1@example.com" mailer="mta" client_name="[192.168.20.9]"
resolve=OK to="user2@example.com" direction="in" message_length=387
virus=" " disposition=0x01 classifier=0x00 subject="JUNE -- whitelist word
- movie --"
```

Log message dispositions and classifiers

History log messages, when viewed in the FortiMail web-based manager, display the classifier names and disposition names. When viewed outside the web-based manager, these classifier names and disposition names are displayed as numbers.

The numbers for classifier and disposition fields are explained in the following tables.

Table 3: Disposition numbers explained

0x0000	Undefined
0x0001	Accept (Accept the message)
0x0002	Log (Log it only, deprecated. It is not used).
0x0004	Reject (Send a reject to the SMTP client)
0x0008	Add_Header (Add a header to the message)
0x0010	Modify_Subject (Modify the subject line)
0x0020	Quarantine (Quarantine the message)
0x0040	Summary_Report
0x0080	Block (Block the message)
0x0100	Replace (Replace banned attachments)
0x0200	Delay (Delay, greylist the message)
0x0400	Forward (Forward the message to a review account)
0x0800	Disclaimer_Body (Added a disclaimer to the body)
0x1000	Disclaimer_Header (Added a disclaimer to the header)
0x2000	Defer (Defer message delivery)
0x4000	Review (Quarantine for review)
0x8000	Treat_As_Spam (Treat as spam)

Table 4: Classifier numbers explained

0x00	Undefined
0x01	User_White
0x02	User_Discard
0x03	System_White
0x04	System_Discard
0x05	RBL
0x06	SURBL
0x07	FortiGuard_Antispam
0x08	FortiGuard_Antispam_White
0x09	Bayesian
0x0A	Hueristic
0x0B	Dictionary_Scanner
0x0C	Banned_Word
0x0D	Deep_Header
0x0E	Forged_IP
0x0F	Quarantine_Control
0x10	Tagged_Virus
0x11	Attachment_Filter
0x12	Greylist
0x13	Bypass_Scan_On_Auth

Table 4: Classifier numbers explained

0x14	Disclaimer
0x15	Defer_Deliver
0x16	Session_Profile_Domain
0x17	Session_Profile_Limits
0x18	Session_Profile_White
0x19	Session_Profile_Discard
0x01A	Content_Filter
0x01B	Content_Treat_As_Spam
0x01C	Attachment_Treat_As_Spam
0x0D	Image_Spam
0x0E	Sender_Reputation
0x0F	Access_Control_List
0x020	Whitelist_Word
0x021	Domain_White
0x022	Domain_Discard
0x023	SPF
0x024	Domain_Key
0x025	DKIM
0x026	Receipient_Verification
0x027	Last

Event Config

This chapter contains information about Event Config log messages.

Event Config is a subtype log of the Event log type. Event Config logs record all configuration changes made to the system of the FortiMail unit, configuration setting, administration, including POP3, SMTP, and IMAP changes.

You can cross-search an Event Config log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the `log_part` field. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

FortiGuard autoupdate settings	Idle timeout	FortiMail disclaimer in header for incoming messages
System update setting	Authentication timeout	Local domains
interface IP address	System language	POP3 server port number
Access methods/status	LCD PIN number	Relay server name
Interface status	LCD PIN protection	SNMP memory threshold
Interface status/PPPoE status	GUI refresh interval	SMTP auth
Interface status/PPPoE settings	System idle and auth timeout	SMTP over ssl
Management IP	Admin addition	SMTP server port number
Interface access methods	Admin change	Status of email archiving
MTU change	Admin deletion	Email archiving account
Interface status	Admin password change	Email archiving rotate setting
Addressing mode of interface	HA settings	Archiving settings on local server
access methods	SNMP status	Archiving settings on remote server
Connect option of interface access methods	SNMP config info	Archiving policy
DNS change	SNMP CPU threshold	Archiving exempt
Primary DNS and secondary DNS	SNMP memory threshold	System quarantine account
Default gateway	SNMP Logdisk threshold	System quarantine rotate setting
Route entry	SNMP mailldisk threshold	System quarantine quota settings
Route with destination IP address/netmask	SNMP deferred mqueue threshold	System quarantine settings
Routing entry	SNMP virus detection threshold	Mail server settings
System timezone	SNMP spam detection threshold	FortiMail appearance information
Daylight saving time	SNMP community entry	FortiMail mail gw user group
NTP server settings	SNMP community and host entry	
System time	FortiMail disclaimer in header for outgoing messages	
Console pageNo setting	FortiMail disclaimer in body for incoming messages	
Console mode setting		

Permission of mail	Password of email archiving account	Memory log setting
Mail server access	Forwarding address for email archiving	Log setting
Local domain deletion	Password of system quarantine account	Log setting elog
Local domain addition	Forwarding address for system quarantine	Log policy
Local user	Password of mail user	Alertemail setting
Local domain name	Display name of mail user	Alertemail SMTP server
User group	User alias	Alertemail target email addresses
Mail user addition/deletion	POP3 auth profile	Alertemail configuration
Mail server user addition	IMAP auth profile	
Mail server user set with information	Email banned word	
Mail server user added with information	Local log setting	
Mail server user deletion		
Disk quota of email archiving account		

FortiGuard autoupdate settings

Type	Event
Subtype	Config
Severity	Information
Message	msg="Autoupdate settings have been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has changed the autoupdate settings using the CLI.

System update setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="System update setting has been changed by user <user_name> via GUI (<ip_address>)"
Meaning	An administrator changed a system update setting using the web-based manager.

interface IP address

Type	Event
Subtype	Config
Severity	Information

Message	msg="interface {port1 port2 ...} ip address changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed an interface IP address using the CLI.

Access methods/status

Type	Event
Subtype	Config
Severity	Information
Message	msg="Interface {port1 port2 ...} {access methods status} has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the access methods or status of an interface using the CLI.

Interface status

Type	Event
Subtype	Config
Severity	Information
Message	msg="interface {port1 port2 ...} status changed by user<user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the status of an interface using the CLI.

Interface status/PPPoE status

Type	Event
Subtype	Config
Severity	Information
Message	msg="interface {port1 port2 ...} status changed by user<user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the status of an interface using the CLI.

Interface status/PPPoE settings

Type	Event
Subtype	Config
Severity	Information
Message	user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="PPPoE settings have been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed PPPoE settings using the CLI or GUI.

Management IP

Type	Event
Subtype	Config
Severity	Information
Message	msg="Management IP has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the management IP using the CLI.

Interface access methods

Type	Event
Subtype	Config
Severity	Information
Message	msg="Interface {port1 port2 ...} access methods has been changed by user <user name> via GUI (<ip_address>)"
Meaning	An administrator changed access methods on an interface using the web-based manager.

MTU change

Type	Event
Subtype	Config
Severity	Information
Message	msg="MTU has been {enabled disabled} for interface {port1 port2 ...} by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator enabled or disabled MTU for an interface using the web-based manager.

Interface status

Type	Event
Subtype	Config
Severity	Information
Message	msg="Interface {port1 port2 ...} has been brought up by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator changed an interface to up using the web-based manager.

Addressing mode of interface access methods

Type	Event
Subtype	Config

Severity	Information
Message	msg="Addressing mode of interface {port1 port2 ...} access methods has been changed by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator changed the access methods of an interface's addressing mode using the web-based manager.

Connect option of interface access methods

Type	Event
Subtype	Config
Severity	Information
Message	msg="Connect option of interface {port1 port2 ...} access methods has been changed by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator changed the access methods of a connect option for an interface using the web-based manager.

DNS change

Type	Event
Subtype	Config
Severity	Information
Message	msg="DNS has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed DNS settings using the CLI.

Primary DNS and secondary DNS

Type	Event
Subtype	Config
Severity	Information
Message	msg="DNS has been changed to <primary_dns> and <secondary_dns> by user <user_name> via GUI (<ip_address>)"
Meaning	An administrator changed the primary DNS and secondary DNS using the web-based manager.

Default gateway

Type	Event
Subtype	Config
Severity	Information
Message	msg="default gateway has been changed to <gateway_ip_address> by user <user_name> via GUI (<ip_address>)"
Meaning	An administrator changed the default gateway IP address using the web-based manager.

Route entry

Type	Event
Subtype	Config
Severity	Information
Message	msg="Route entry <number> has been deleted by user<user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator deleted a route entry using the CLI or web-based manager.

Route with destination IP address/netmask

Type	Event
Subtype	Config
Severity	Information
Message	msg="A route to <destination_ip_address>/<destination_netmask> has been added by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator added a route with destination address/netmask using either the CLI or web-based manager.

Routing entry

Type	Event
Subtype	Config
Severity	Information
Message	msg="Routing entry <number> has been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed a routing entry using the CLI or web-based manager.

System timezone

Type	Event
Subtype	Config
Severity	Information
Message	msg="System timezone has been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed the system timezone using the CLI or web-based manager.

Daylight saving time

Type	Event
Subtype	Config
Severity	Information
Message	msg="Automatically adjust clock for Daylight Saving time has been changed by user<user_name> via GUI (<ip_address>)"
Meaning	An administrator changed the option of automatically adjusting clock for daylight saving time using the web-based manager.

NTP server settings

Type	Event
Subtype	Config
Severity	Information
Message	msg="NTP server settings have been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed NTP server settings using the CLI or web-based manager.

System time

Type	Event
Subtype	Config
Severity	Information
Message	msg="System time has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the system time using the CLI.

Console pageNo setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="Console pageNo setting has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the console page number setting using the CLI.

Console mode setting

Type	Event
Subtype	Config

Severity	Information
Message	msg="Console mode setting has been changed to {line batch} mode by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the console mode setting to line or batch mode using the CLI.

Idle timeout

Type	Event
Subtype	Config
Severity	Information
Message	msg="Idle timeout value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the idle timeout value using the CLI.

Authentication timeout

Type	Event
Subtype	Config
Severity	Information
Message	msg="Authentication timeout value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed authentication timeout value using the CLI.

System language

Type	Event
Subtype	Config
Severity	Information
Message	msg="System language has been changed to {en ja ko ch tra} by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed the system language to another language using the CLI or web-based manager.

LCD PIN number

Type	Event
Subtype	Config
Severity	Information
Message	msg="LCD PIN number has been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed the LCD PIN number using the CLI or web-based manager.

LCD PIN protection

Type	Event
Subtype	Config
Severity	Information
Message	msg="LCD PIN protection has been {enable disable} by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed LCD PIN protection enabled or disabled using the CLI or web-based manager.

GUI refresh interval

Type	Event
Subtype	Config
Severity	Information
Message	msg="GUI refresh interval set to <interval> by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed web-based manager refresh interval set to another interval using the CLI.

System idle and auth timeout

Type	Event
Subtype	Config
Severity	Information
Message	msg="{System idle and auth timeout auth timeout} has been changed by user <user_name> via GUI (<ip_address>)"
Meaning	An administrator changed both system idle and auth timeout or just auth timeout using the web-based manager.

Admin addition

Type	Event
Subtype	Config
Severity	Information
Message	msg="Admin <user_name> has been added by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator has added another administrator using the CLI or web-based manager.

Admin change

Type	Event
Subtype	Config
Severity	Information
Message	msg="Admin <user_name> has been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed another administrator using the CL or web-based manager.

Admin deletion

Type	Event
Subtype	Config
Severity	Information
Message	msg="Admin <user_name> has been deleted by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator deleted another administrator using the CLI or web-based manager.

Admin password change

Type	Event
Subtype	Config
Severity	Information
Message	msg="admin <user_name> password has been changed by user <user_name> via GUI (<ip_address>)"
Meaning	An administrator changed another administrator's password using the web-based manager.

HA settings

Type	Event
Subtype	Config
Severity	Information
Message	msg="HA settings have been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed HA settings using the CLI.

SNMP status

Type	Event
Subtype	Config
Severity	Information

Message	msg="SNMP has been {enabled disabled} by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator enabled/disabled SNMP using the CLI.

SNMP config info

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP config info changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed SNMP config information using the CLI.

SNMP CPU threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP CPU threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed SNMP CPU threshold value using the CLI.

SNMP memory threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP Memory threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the SNMP memory threshold value using the CLI.

SNMP Logdisk threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP Logdisk threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed SNMP log disk threshold value using the CLI.

SNMP maildisk threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP maildisk threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the SNMP mail disk threshold value using the CLI.

SNMP deferred mqueue threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP Deferred mqueue threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the SNMP deferred mqueue using the CLI.

SNMP virus detection threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP Virus detection threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed SNMP virus detection threshold value using the CLI.

SNMP spam detection threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP Spam detection threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed the SNMP Spam detection threshold value using the CLI.

SNMP community entry

Type	Event
Subtype	Config

Severity	Information
Message	msg="SNMP community entry <number> has been deleted by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator deleted an SNMP community entry using the CLI.

SNMP community and host entry

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP community entry <entry_number> host <host_number> has been deleted by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator deleted an SNMP community entry and host using the CLI.

FortiMail disclaimer in header for outgoing messages

Type	Event
Subtype	Config
Severity	Information
Message	msg="FortiMail disclaimer in header for outgoing messages has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has changed a FortiMail disclaimer header for outgoing messages using the CLI.

FortiMail disclaimer in body for incoming messages

Type	Event
Subtype	Config
Severity	Information
Message	msg="FortiMail disclaimer in body for incoming messages has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has changed a FortiMail disclaimer body for incoming messages using the CLI.

FortiMail disclaimer in header for incoming messages

Type	Event
Subtype	Config
Severity	Information

Message	msg="FortiMail disclaimer in header for incoming messages has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has changed a FortiMail disclaimer header for incoming messages using the CLI.

Local domains

Type	Event
Subtype	Config
Severity	Information
Message	msg="Local domains has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified local domains using the CLI.

POP3 server port number

Type	Event
Subtype	Config
Severity	Information
Message	msg="POP3 server port number has been modified to <port number> by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified a POP3 server using the CLI.

Relay server name

Type	Event
Subtype	Config
Severity	Information
Message	msg="Relay server name has been modified to <server name> by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified a relay server name using the CLI.

SNMP memory threshold

Type	Event
Subtype	Config
Severity	Information
Message	msg="SNMP Memory threshold value has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has changed SNMP Memory threshold value using the CLI.

SMTP auth

Type	Event
Subtype	Config
Severity	Information
Message	msg="smtp auth has been modified to <auth_profile_name> by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified SMTP authentication using the CLI.

SMTP over ssl

Type	Event
Subtype	Config
Severity	Information
Message	msg="smtp over ssl has been modified to {enabled disabled} by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified SMTP over SSL using the CLI.

SMTP server port number

Type	Event
Subtype	Config
Severity	Information
Message	msg="SMTP server port number has been modified to <port_number> by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified SMTP server port number using the CLI.

Status of email archiving

Type	Event
Subtype	Config
Severity	Information
Message	msg="status of email archiving has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified the status of email archiving using the CLI.

Email archiving account

Type	Event
Subtype	Config

Severity	Information
Message	msg="email archiving account has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified the status of the email archiving account using the CLI.

Email archiving rotate setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="email archiving rotate setting has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified an email archiving rotate setting using the CLI.

Archiving settings on local server

Type	Event
Subtype	Config
Severity	Information
Message	msg="Archiving settings on local server has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified archiving settings on the local server using the CLI.

Archiving settings on remote server

Type	Event
Subtype	Config
Severity	Information
Message	msg="Archiving settings on remote server has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified archiving settings on a remote server using the CLI.

Archiving policy

Type	Event
Subtype	Config
Severity	Information
Message	msg="Archiving policy has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified an archiving policy using the CLI.

Archiving exempt

Type	Event
Subtype	Config
Severity	Information
Message	msg="Archiving exempt has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified an archiving exempt setting using the CLI.

System quarantine account

Type	Event
Subtype	Config
Severity	Information
Message	msg="system quarantine account has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified the system quarantine account using the CLI.

System quarantine rotate setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="system quarantine rotate setting has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified a system quarantine rotate setting using the CLI.

System quarantine quota settings

Type	Event
Subtype	Config
Severity	Information
Message	msg="System quarantine quota settings on local server has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has modified system quarantine quota settings using the CLI.

System quarantine settings

Type	Event
Subtype	Config

Severity	Information
Message	msg="System quarantine settings have been changed by user <use_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator has changed system quarantine settings using the CLI or web-based manager.

Mail server settings

Type	Event
Subtype	Config
Severity	Information
Message	msg="Mail Server settings have been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator has changed mail server settings using the CLI or web-based manager.

FortiMail appearance information

Type	Event
Subtype	Config
Severity	Information
Message	msg="FortiMail appearance information has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has changed FortiMail appearance information using the CLI.

FortiMail mail gw user group

Type	Event
Subtype	Config
Severity	Information
Message	msg="FortiMail mail gw user group has been {changed deleted} by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator has changed or deleted a FortiMail mail gateway user group using the CLI.

Permission of mail

Type	Event
Subtype	Config
Severity	Information

Message	msg="Permission of mail from <email_address> is {set to (OK REJECT RELAY DISCARD) deleted} by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator set or deleted permission of mail using the CLI or web-based manager.

Mail server access

Type	Event
Subtype	Config
Severity	Information
Message	msg="Mail server access <string> is deleted by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator deleted mail server access using the web-based manager.

Local domain deletion

Type	Event
Subtype	Config
Severity	Information
Message	msg="local domain <domain_name> is deleted by user <user_name> via CLI (console telnet ssh)"
Message	An administrator deleted a local domain using the CLI.

Local domain addition

Type	Event
Subtype	Config
Severity	Information
Message	msg="Local domain name <domain_name> is added by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Message	An administrator added a local domain using the CLI or web-based manager.

Local user

Type	Event
Subtype	Config
Severity	Information
Message	msg="Local user <user_name> has been {added modified deleted} by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator added, modified, or deleted a local user using the CLI.

Local domain name

Type	Event
Subtype	Config
Severity	Information
Message	msg="Local domain name <domain_name> is added by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator added a local domain name using the web-based manager.

User group

Type	Event
Subtype	Config
Severity	Information
Message	msg="User group <group_name> has been {modified deleted} by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator modified or deleted a user group using the CLI or web-based manager.

Mail user addition/deletion

Type	Event
FortiMail version	3.0
Severity	Information
Message	msg="mail user <user_address> has been {added deleted} by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator added or deleted a mail user using the CLI.

Mail server user addition

Type	Event
Subtype	Config
Severity	Information
Message	msg="Mail server user <email_address> is added with information: displayname <display_name> by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator added a specified mail server user using the CLI.

Mail server user set with information

Type	Event
Subtype	Config

Severity	Information
Message	msg="Mail server user <email_address> is set with information: displayname <display_name> by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator sets a mail server user with information using the CLI or web-based manager.

Mail server user added with information

Type	Event
Subtype	Config
Severity	Information
Message	msg="Mail server user <email_address> is added with information: displayname <display_name> by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator added a mail server user with information using the web-based manager.

Mail server user deletion

Type	Event
Subtype	Config
Severity	Information
Message	msg="Mail Server User <email_address> is deleted by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator deletes a mail server user using the web-based manager.

Disk quota of email archiving account

Type	Event
Subtype	Config
Severity	Information
Message	msg="disk quota of email archiving account has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator modified the disk quota of the email archiving account using the CLI.

Password of email archiving account

Type	Event
Subtype	Config
Severity	Information
Message	msg="password of email archiving account has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator modified the email archiving account password using the CLI.

Forwarding address for email archiving

Type	Event
Subtype	Config
Severity	Information
Message	msg="forwarding address for email archiving has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator modified the forwarding address for email archiving using the CLI.

Password of system quarantine account

Type	Event
Subtype	Config
Severity	Information
Message	msg="password of system quarantine account has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator modified the system quarantine account password using the CLI.

Forwarding address for system quarantine

Type	Event
Subtype	Config
Severity	Information
Message	msg="forwarding address for system quarantine has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator modified the system quarantine forwarding address using the CLI.

Password of mail user

Type	Event
Subtype	Config
Severity	Information
Message	msg="password of mail user <user_email_address> has been modified by user <user name> via CLI (console telnet ssh)"
Meaning	An administrator modified the password of a mail user using the CLI.

Display name of mail user

Type	Event
Subtype	Config

Severity	Information
Message	msg="display name of mail user <user_address> has been modified by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator modified the display name of a specific mail user using the CLI.

User alias

Type	Event
Subtype	Config
Severity	Information
Message	msg="User alias <alias_name> has been {added modified deleted} by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator added, modified, or deleted a user alias using the web-based manager.

POP3 auth profile

Type	Event
Subtype	Config
Severity	Information
Message	msg="POP3 auth profile <profile_name> has been {added renamed modified deleted} by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator added, renamed, modified, or deleted a POP3 auth profile using the CLI.

IMAP auth profile

Type	Event
Subtype	Config
Severity	Information
Message	msg="IMAP auth profile <profile_name> has been {added modified deleted} by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator added, modified, or deleted an IMAP auth profile using the CLI.

Email banned word

Type	Event
Subtype	Config
Severity	Information
Message	msg="email banned word was removed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator removed an email banned word using the CLI.

Local log setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="Local log setting has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed a local log setting using the CLI.

Memory log setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="Memory logsetting has been changed by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator changed memory log setting using the CLI.

Log setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="Log setting has been changed by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator changed a log setting using the CLI or web-based manager.

Log setting elog

Type	Event
Subtype	Config
Severity	Information
Message	msg="Log setting elog has been cleared by user <user_name> via CLI (console telnet ssh)"
Meaning	An administrator cleared elog using the CLI.

Log policy

Type	Event
Subtype	Config

Severity	Information
Message	msg="Log Policy has been modified by user admin via GUI(<ip_address>)"
Meaning	An administrator has edited a log policy using the web-based manager.

Alertemail setting

Type	Event
Subtype	Config
Severity	Information
Message	msg="Alertemail setting has been changed by user admin via CLI (console telnet ssh)"
Meaning	An administrator changed the alert email setting using the CLI.

Alertemail SMTP server

Type	Event
Subtype	Config
Severity	Information
Message	msg="Alertemail SMTP server has been changed to <server_name> and user has been changed to <user_name> by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator changed the alertemail SMTP server to and a user was changed using the web-based manager.

Alertemail target email addresses

Type	Event
Subtype	Config
Severity	Information
Message	msg="Alertemail target email addresses have been changed by user <user_name> via GUI (<ip_address>)"
Meaning	An administrator changed alert email target email addresses using the web-based manager.

Alertemail configuration

Type	Event
Subtype	Config
Severity	Information
Message	msg="Alertemail configuration has been modified by user <user_name> via GUI(<ip_address>)"
Meaning	An administrator modified alert email configuration using the web-based manager.

Event System

This chapter contains information regarding Event System log messages.

Event System is a subtype log of the Event log type. Event System log messages inform you of system changes made to your FortiMail unit. For example, the log message may record a user that shuts down the system from the console, or a user that restarts the FortiMail unit from a system reboot from the console.

You can cross-search an Event System log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

[DNS servers](#)

[System reload](#)

[Upgrade system firmware failed](#)

[System restart](#)

[System reset](#)

[System mode](#)

[System shutdown](#)

[System firmware upgrade](#)

DNS servers

Type	Event
Subtype	System
Severity	Warning
Message	msg= “DNS: Connection timed out. No servers could be reached.”
Meaning	An administrator could not reach any DNS servers before a time out occurred.

System restart

Type	Event
Subtype	System
Severity	Warning
Message	msg=“System has been restarted by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}”
Meaning	An administrator restarted the system using the CLI or web-based manager.

System shutdown

Type	Event
Subtype	System

Severity	Warning
Message	msg="System has been shutdown by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)"
Meaning	An administrator shut down the system using the CLI or web-based manager.

System reload

Type	Event
Subtype	System
Severity	Warning
Message	msg="System has been reloaded by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)"
Meaning	An administrator reloaded the system using the CLI or web-based manager.

System reset

Type	Event
Subtype	System
Severity	Warning
Messages	msg="System has been reset to factory default by user <user_name> via {console SSH (<ip_address>) telnet(<ip_address>) GUI(<ip_address>) LCD}"
Meaning	An administrator reset the system to factory default using the CLI, web-based manager, or LCD.

System firmware upgrade

Type	Event
Subtype	System
Severity	Warning
Messages	msg="System firmware has been {upgraded downgraded} by user <user_name> via {console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator upgraded/downgraded system firmware using the CLI or web-based manager.

Upgrade system firmware failed

Type	Event
Subtype	System
Severity	Warning

Message	msg="Upgrade system firmware failed by user <user_name> via {console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)}"
Meaning	An administrator upgraded system firmware unsuccessfully using the CLI, console, telnet, or web-based manager.

System mode

Type	Event
Subtype	System
Severity	Warning
Messages	msg="System has been changed to {gateway server transparent} mode by {user <user_name> user LCD} via console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)"
Meaning	An administrator or LCD user changed the mode to gateway, server, or transparent mode using the CLI, web-based manager or LCD.

Event Update

This chapter contains information regarding Event Update log messages.

Event Update log is a subtype log of the Event log type. Event Update log messages contain information about the success or failure of an update of FortiGuard services, such as updating the virus database.

You can cross-search an Event Update log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

[FortiGuard update result](#)

FortiGuard update result

Type	Event
Subtype	Update
Severity	Warning
Message	msg="Update result: virusdb:<yes no>, avengine:<yes no>, spamdb:<yes no>, asengine:<yes no>
Meaning	The FortiMail unit updated the following FortiGuard services: <ul style="list-style-type: none"> • Antivirus engine • Virus database • Spam database • AntiSpam engine

Event SMTP

This chapter contains information regarding Event-SMTP log messages.

Event SMTP log is a subtype log of the Event log type. Event SMTP log messages inform you of any SMTP-related events that occur.

You can cross-search an Event SMTP log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

SMTP-related events	FortiGuard antispam rule (FSAR) loaded	Antivirus database loaded
Starting flgrptd	Mail aliases rebuilt	Bayesian database training
Virus db loaded	FortiGuard antispam rule (FSAR) loading	Bayesian database training completed
	Updated daemon restarted	
FASR readme	Antivirus database loading	

SMTP-related events

Type	Event
Subtype	SMTP
Severity	All severity levels
Message	msg="<log_message_information>"
Meaning	Any SMTP-related events.

Starting flgrptd

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Starting flgrptd"
Meaning	The reporting daemon is starting. The reporting daemon generates the reports that are available in the web-based manager, Log & Report > Reports. The reporting daemon generates the reports by parsing the various log files.

Virus db loaded

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Successfully loaded virus db: /var/spool/etc/vir"
Meaning	The antivirus database is successfully loaded.

FortiGuard antispam rule (FSAR) loading

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Initializing FASR /var/spool/etc/antispam..."
Meaning	The FortiGuard Antispam Rule (FSAR) database is loading.

FASR readme

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Parsing FASR Readme /var/spool/etc/antispam/README..."
Meaning	Parsing the accompanying README file which includes version information about the database.

FortiGuard antispam rule (FSAR) loaded

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Initializing FASR /var/spool/etc/antispam done!"
Meaning	The parsing of the rule set is finished.

Mail aliases rebuilt

Type	Event
Subtype	SMTP
Severity	Notification

Message	user=mail ui=mail action=unknown status=success msg="*@*: alias database /var/spool/etc/mail/aliases has been rebuilt"
Meaning	Mail aliases have been rebuilt.

Antivirus database loaded

Type	Event
Subtype	SMTP
Severity	Information
Message	msg="Successfully loaded virus db: /var/spool/etc/virus"
Meaning	The antivirus database is loaded successfully.

Updated daemon restarted

Type	Event
Subtype	SMTP
Severity	Warning
Message	msg="Restart the updated daemon to re-load default avengine and virusdb..."
Meaning	Updated daemon is restarted to reload default antivirus engine and database.

Antivirus database loading

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Loading virusdb: /var/spool/etc/vir..."
Meaning	The user is loading the antivirus database.

Antivirus database loaded

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Successfully loaded virus db: /var/spool/etc/vir"
Meaning	The user successfully uploaded the antivirus database.

Bayesian database training

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Bayesian Training user global bayesian"
Meaning	The FortiMail unit is training a specific bayesian database.

Bayesian database training completed

Type	Event
Subtype	SMTP
Severity	Information
Message	msg= "Bayesian Training: <integer> messages finished"
Meaning	A specific number of messages have completed the bayesian training.

Event Admin

This chapter contains information regarding Event Admin log messages.

Event Admin log is a subtype log of the Event log type. Event Admin log messages inform you of administration changes made to your FortiMail unit.

You can cross-search an Event Admin log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

User login	Message cannot be read
Webmail login	Attachment saving failure
User login failure	LCD login
WebMail GUI failure	LCD login failure
Message retrieval failure	

User login

Type	Event
Subtype	Admin
Severity	Information
Message	msg="User <user_name> login successfully from {GUI(<ip_address> console SSH(<ip_address>) telnet(<ip_address>)}"
Meaning	An administrator successfully logged in using the web-based manager or CLI.

Webmail login

Type	Event
Subtype	Admin
Severity	Information
Message	msg="User <user_name> from <ip_address> logged in"
Meaning	An administrator from a specified IP address logged into the WebMail.

User login failure

Type	Event
Subtype	Admin

Severity	Information
Message	msg="User <user_name> login failed from {console SSH(<ip_address>) telnet(<ip_address>)}"
Meaning	An administrator failed to log in using the console, SSH, or telnet.

WebMail GUI failure

Type	Event
Subtype	Admin
Severity	Information
Message	msg="mailbox_get_header: failed"
Meaning	The WebMail GUI cannot display the email message, or the quarantined message in the web-based manager.

Message retrieval failure

Type	Event
Subtype	Admin
Severity	Information
Message	msg="mailbox_get_num_parts: failed"
Meaning	Specific information in a message cannot be retrieved.

Message cannot be read

Type	Event
Subtype	Admin
Severity	Information
Message	msg="Could not get message part"
Meaning	The message cannot be read from the mailbox.

Attachment saving failure

Type	Event
Subtype	Admin
Severity	Information
Message	msg="Could not save attachment"
Meaning	An unknown failure occurred when trying to prepare the attachment for a user to download.

LCD login

Type	Event
Subtype	Admin
Severity	Information
Message	msg="Login from LCD successfully"
Meaning	An administrator successfully logged in using the LCD.

LCD login failure

Type	Event
Subtype	Admin
Severity	Information
Message	msg="Login from LCD failed"
Meaning	An administrator failed to log in using the LCD.

Event POP3

This chapter contains information regarding Event POP3 log messages.

Event POP3 log is a subtype log of the Event log type. Event POP3 log messages inform you of any POP3-related events that occur.

You can cross-search an Event POP3 log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

[POP3-related events](#)

POP3-related events

Log Type	Event
Subtype	POP3
Severity	All severity levels
Message	msg="<log_message_information>"
Meaning	Any POP3-related events.

Event IMAP

This chapter contains information regarding Event IMAP log messages.

Event IMAP log is a subtype log of the Event log type. Event IMAP log messages inform you of any IMAP-related messages.

You can cross-search an Event IMAP log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

[IMAP-related events](#)

IMAP-related events

Log type	Event
Subtype	IMAP
Severity	All severity levels
Message	msgs="<log_message_information>"
Meaning	Any IMAP-related events.

Event HA

This chapter contains information regarding Event HA (high availability) log messages.

Event HA log is a subtype log of the Event log type. Event HA log messages inform you of any high availability problems that may occur within a high availability cluster.

You can cross-search an Event HA log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

Master mode

Slave mode

Master role

Master mode

Log type	Event
Subtype	HA
Severity	Information
Message	msgs="monitord: main loop starting, entering MASTER mode"
Meaning	The FortiMail unit is entering primary mode.

Slave mode

Log type	Event
Subtype	HA
Severity	Information
Message	msgs="configd: main loop starting, entering slave mode"
Meaning	The FortiMail unit is entering subordinate mode.

Master role

Log type	Event
Subtype	HA
Severity	Information

Message	msgs="monitord: ** reached retry limit, assuming MASTER role"
Meaning	The FortiMail unit is assuming the primary unit role because the retry limit was reached for connecting to the original primary unit.

Event Webmail

This chapter contains information regarding Event Webmail log messages.

Event Webmail log is a subtype log of the Event log type. Event Webmail log messages inform you of any webmail-related events that occur.

You can cross-search an Event Webmail log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

[User login](#)

User login

Log type	Event
Subtype	Webmail
Severity	All severity levels
Message	msgs="User <user_name> from <IP address> logged in."
Meaning	A user logged into the FortiMail webmail.

Antivirus

This chapter contains information regarding antivirus log messages, including an example of an antivirus log message.

Antivirus log messages have a subtype called virus detect. Antivirus log messages inform you of viruses detected by your FortiMail unit.

Anti-virus uses a dynamic error reporting scheme. This scheme is unable to create a definitive list of log messages that you may encounter. Errors are logged in a format similar to the following example.

You can cross-search an antivirus log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).

Example

In this example, an email from `user1@example.com` has an infected file within the email.

```
2008-09-28 16:30:18 log_id=0200060101 log_part=00 type=virus
subtype=infected pri=information session_id=n/a from=user1@example.com
to=<user3@example.com> src_ip=172.20.130.26 msg="The file wqdf.zip is
infected with HGBYN_TEST_FILE."
```



Note: Log headers in FortiMail 3.0 MR3 and up include the field, `log_part`. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

Virus infection

Virus infection

Log Type	Antivirus
Subtype	Viruses detect
Severity	All severity levels.
Message	msg="The file name is infected with <virus_name>"
Meaning	The file contains the specified virus.

Antispam

This chapter contains information regarding Antispam log messages, including an example of a Antispam log message.

Antispam log messages have a subtype called spam detect. Antispam log messages notify you of any spammed email.

The FortiMail Antispam uses a dynamic error reporting scheme. This scheme is unable to create a definitive list of log messages that you may encounter. Errors are logged in a format similar to the following example.

You can cross-search an antispam log message to get more information about it. For more information about log message cross search, see [“Log message cross search” on page 15](#).

Example

In this example, a FortiMail unit detected a spam in an email sent from user 1 to user 3. The email was rejected by a banned word check.

```
2008-09-21 10:06:45 log_id=051080300 log_part=00 type=spam
subtype=detected pri=information session_id=k8PFfe5K4002115
from=user1@example.com to=user3@example.com client_name=152.20.120.99
msg=Rejected by BannedWord check
```



Note: Log headers in FortiMail 3.0 MR3 and up include the field, log_part. This field provides identification when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length decreased to 1 kilobyte.

[Spam-related events](#)

[Deep header scanner rules reload](#)

Spam-related events

Log Type	Antispam
Subtype	Spam detect
Severity	Information
Message	msg="<log_message_information>"
Meaning	Any spam-related events.

Deep header scanner rules reload

Log Type	Antispam
Subtype	Spam detect
Severity	Notification

Message	msg="Deep Header Scanner Rules Reload - Finished."
Meaning	Rule loading has been completed.

FortiMail units may sometimes write log messages similar to the following:

```
2008-01-10 15:07:54 log_id=0501080300 type=spam subtype=detected > pri=information session_id=""  
from="" to="" msg="SocketSmtplib receive banner > from 1.1.73.66 failed SocketException( 115 ) ,  
Socket.cpp:573, "Operation now in progress"
```

This socket exception occurred during recipient verification with the protected email server through SMTP. The recipient verification process didn't finish. This is most likely caused by the sudden session termination by the protected email server. When this exception occurs, the recipient verification process would not finish, and therefore message delivery would temporarily fail. The sending mail transfer agent (MTA) will retry to deliver the email.

Index

A

- antispam, 71
 - deep header scanner reload, 71
 - spam-related events, 71
- antivirus, 69
 - file name infection, 69

D

- documentation
 - Fortinet, 9

E

- event admin, 57
 - attachment saving failure, 58
 - LCD login, 59
 - LCD login failure, 59
 - message cannot be read, 58
 - message retrieval failure, 58
 - user login, 57
 - user login failure, 57
 - webmail GUI failure, 58
 - webmail login, 57
- event config, 21
 - access methods/status, 23
 - addressing mode of interface access methods, 24
 - admin addition, 29
 - admin change, 30
 - admin deletion, 30
 - admin password change, 30
 - alertemail configuration, 45
 - alertemail setting, 45
 - alertemail SMTP server, 45
 - alertemail target email addresses, 45
 - archiving exempt, 37
 - archiving policy, 36
 - archiving settings on local server, 36
 - archiving settings on remote server, 36
 - authentication timeout, 28
 - connect option of interface access methods, 25
 - console mode setting, 27
 - console pageNo setting, 27
 - daylight saving time, 27
 - default gateway, 25
 - disk quota of email archiving account, 41
 - display name of mail user, 42
 - DNS change, 25
 - email archiving account, 35
 - email archiving rotate setting, 36
 - email banned word, 43
 - FortiGuard autoupdate settings, 22
 - FortiMail appearance information, 38
 - FortiMail disclaimer in body for incoming messages, 33
 - FortiMail disclaimer in header for incoming messages, 33
 - FortiMail disclaimer in header for outgoing messages, 33
 - FortiMail mail gw user group, 38
 - forwarding address for email archiving, 42
 - forwarding address for system quarantine, 42
 - GUI refresh interval, 29
 - HA settings, 30
 - idle timeout, 28
 - IMAP auth profile, 43
 - interface access methods, 24
 - interface IP address, 22
 - interface status, 23, 24
 - interface status/PPPoE settings, 23
 - interface status/PPPoE status, 23
 - LCD PIN number, 28
 - LCD PIN protection, 29
 - local domain addition, 39
 - local domain deletion, 39
 - local domain name, 40
 - local domains, 34
 - local log setting, 44
 - local user, 39
 - log policy, 44
 - log setting, 44
 - log setting elog, 44
 - mail server access, 39
 - mail server settings, 38
 - mail server user added with information, 41
 - mail server user addition, 40
 - mail server user deletion, 41
 - mail server user set with information, 40
 - mail user addition/deletion, 40
 - management IP, 24
 - memory log setting, 44
 - MTU change, 24
 - NTP server settings, 27
 - password of email archiving account, 41
 - password of mail user, 42
 - password of system quarantine account, 42
 - permission of mail, 38
 - POP3 auth profile, 43
 - POP3 server port number, 34
 - primary DNS and secondary DNS, 25
 - relay server name, 34
 - route entry, 26
 - route with destination IP address/netmask, 26
 - routing entry, 26
 - SMTP auth, 35
 - SMTP over ssl, 35
 - SMTP server port number, 35
 - SNMP community and host entry, 33
 - SNMP community entry, 32
 - SNMP config info, 31
 - SNMP CPU threshold, 31
 - SNMP deferred mqueue threshold, 32
 - SNMP Logdisk threshold, 31
 - SNMP maildisk threshold, 32
 - SNMP memory threshold, 31, 34
 - SNMP spam detection threshold, 32
 - SNMP status, 30
 - SNMP virus detection threshold, 32
 - status of email archiving, 35
 - system idle and auth timeout, 29
 - system language, 28
 - system quarantine account, 37

- system quarantine quota settings, 37
- system quarantine settings, 37
- system time, 27
- system timezone, 26
- system update setting, 22
- user alias, 43
- user group, 40
- event HA, 65
 - master mode, 65
 - master role, 65
 - slave mode, 65
- event IMAP, 63
 - IMAP-related events, 63
- event POP3, 61
 - POP3-related events, 61
- event SMTP, 53
 - antivirus database loaded, 55
 - antivirus database loading, 55
 - bayesian database training, 56
 - bayesian database training completed, 56
 - FASR readme, 54
 - FortiGuard antispam rule (FSAR) loaded, 54
 - FortiGuard antispam rule (FSAR) loading, 54
 - mail aliases rebuilt, 54
 - SMTP-related events, 53
 - starting flgrptd, 53
 - updated daemon restarted, 55
 - virus db loaded, 54
- event system, 47
 - FortiGuard update result, 51
 - system firmware upgrade, 48
 - system mode, 49
 - system reload, 48
 - system reset, 48

- system restart, 47
- system shutdown, 47
- upgrade system firmware failed, 48
- event update, 51
- event webmail, 67
 - user login, 67

F

- Fortinet
 - Knowledge Base, 9
 - Technical Documentation, 9
 - Technical Support, 10
- Fortinet documentation, 9

I

- introduction
 - Fortinet documentation, 9

L

- log
 - cross search, 15
 - error messages, 15
 - messages, 14
 - severity levels, 13
 - subtypes, 13
 - types, 11
- log type
 - history, 17

S

- system quarantine rotate setting, 37

FORTINET®

