



# FortiMail™ Secure Messaging Platform

Version 4.0

Log Message Reference

## **FortiMail™ Secure Messaging Platform Log Message Reference**

Version 4.0

Revision 1

17 November 2009

© Copyright 11/17/09 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

### **Trademarks**

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

### **Regulatory compliance**

FCC Class A Part 15 CSA/CUS



**CAUTION:** Risk of explosion if battery is replaced by incorrect type.  
Dispose of used batteries according to instructions.

# Contents

<b>Introduction .....</b>	<b>9</b>
<b>FortiMail documentation .....</b>	<b>9</b>
Fortinet Tools and Documentation CD .....	10
Fortinet Knowledge Base .....	10
Comments on Fortinet technical documentation .....	10
<b>Customer service and technical support.....</b>	<b>10</b>
<b>About FortiMail logs .....</b>	<b>11</b>
<b>Log types .....</b>	<b>11</b>
History logs .....	11
Event logs .....	12
Antispam logs .....	12
Antivirus logs .....	12
<b>Subtypes .....</b>	<b>13</b>
<b>Severity levels .....</b>	<b>13</b>
<b>Log message syntax.....</b>	<b>14</b>
<b>Error log messages.....</b>	<b>15</b>
<b>Log message cross search .....</b>	<b>15</b>
<b>History.....</b>	<b>17</b>
Example .....	17
<b>Event Config .....</b>	<b>19</b>
<b>FortiGuard autoupdate settings .....</b>	<b>20</b>
<b>System update setting.....</b>	<b>20</b>
<b>interface IP address .....</b>	<b>20</b>
<b>Access methods/status .....</b>	<b>21</b>
<b>Interface status.....</b>	<b>21</b>
<b>Interface status/PPPoE status .....</b>	<b>21</b>
<b>Interface status/PPPoE settings .....</b>	<b>21</b>
<b>Management IP .....</b>	<b>22</b>
<b>Interface access methods .....</b>	<b>22</b>
<b>MTU change.....</b>	<b>22</b>
<b>Interface status.....</b>	<b>22</b>
<b>Addressing mode of interface access methods .....</b>	<b>22</b>
<b>Connect option of interface access methods .....</b>	<b>23</b>
<b>DNS change.....</b>	<b>23</b>
<b>Primary DNS and secondary DNS .....</b>	<b>23</b>

Default gateway .....	23
Route entry .....	24
Route with destination IP address/netmask.....	24
Routing entry.....	24
System timezone.....	24
Daylight saving time .....	25
NTP server settings .....	25
System time .....	25
Console pageNo setting .....	25
Console mode setting.....	25
Idle timeout.....	26
Authentication timeout .....	26
System language.....	26
LCD PIN number.....	26
LCD PIN protection .....	27
GUI refresh interval.....	27
System idle and auth timeout .....	27
Admin addition .....	27
Admin change .....	28
Admin deletion .....	28
Admin password change.....	28
HA settings .....	28
SNMP status .....	28
SNMP config info .....	29
SNMP CPU threshold.....	29
SNMP memory threshold .....	29
SNMP Logdisk threshold.....	29
SNMP maildisk threshold.....	30
SNMP deferred mqueue threshold .....	30
SNMP virus detection threshold.....	30
SNMP spam detection threshold .....	30
SNMP community entry.....	30
SNMP community and host entry.....	31
FortiMail disclaimer in header for outgoing messages.....	31
FortiMail disclaimer in body for incoming messages .....	31
FortiMail disclaimer in header for incoming messages .....	31

Local domains .....	32
POP3 server port number.....	32
Relay server name .....	32
SNMP memory threshold .....	32
SMTP auth.....	33
SMTP over ssl.....	33
SMTP server port number .....	33
Status of email archiving.....	33
Email archiving account.....	33
Email archiving rotate setting.....	34
Archiving settings on local server .....	34
Archiving settings on remote server.....	34
Archiving policy .....	34
Archiving exempt.....	35
System quarantine account .....	35
System quarantine rotate setting .....	35
System quarantine quota settings .....	35
System quarantine settings .....	35
Mail server settings.....	36
FortiMail appearance information .....	36
FortiMail mail gw user group .....	36
Permission of mail .....	36
Mail server access .....	37
Local domain deletion .....	37
Local domain addition .....	37
Local user .....	37
Local domain name.....	38
User group.....	38
Mail user addition/deletion.....	38
Mail server user addition.....	38
Mail server user set with information.....	38
Mail server user added with information .....	39
Mail server user deletion .....	39
Disk quota of email archiving account .....	39
Password of email archiving account.....	39
Forwarding address for email archiving.....	40

Password of system quarantine account .....	40
Forwarding address for system quarantine .....	40
Password of mail user .....	40
Display name of mail user .....	40
User alias .....	41
POP3 auth profile .....	41
IMAP auth profile .....	41
Email banned word .....	41
Local log setting .....	42
Memory log setting .....	42
Log setting .....	42
Log setting elog .....	42
Log policy .....	42
Alertemail setting .....	43
Alertemail SMTP server .....	43
Alertemail target email addresses .....	43
Alertemail configuration .....	43
<b>Event System .....</b>	<b>45</b>
DNS servers .....	45
System restart .....	45
System shutdown .....	45
System reload .....	46
System reset .....	46
System firmware upgrade .....	46
Upgrade system firmware failed .....	46
System mode .....	47
<b>Event Update .....</b>	<b>49</b>
FortiGuard update result .....	49
<b>Event SMTP .....</b>	<b>51</b>
SMTP-related events .....	51
Starting flgrptd .....	51
Virus db loaded .....	52
FortiGuard antispam rule (FSAR) loading .....	52
FASR readme .....	52
FortiGuard antispam rule (FSAR) loaded .....	52

Mail aliases rebuilt .....	52
Antivirus database loaded .....	53
Updated daemon restarted.....	53
Antivirus database loading .....	53
Antivirus database loaded .....	53
Bayesian database training.....	54
Bayesian database training completed.....	54
<b>Event Admin .....</b>	<b>55</b>
User login.....	55
Webmail login.....	55
User login failure.....	55
WebMail GUI failure .....	56
Message retrieval failure .....	56
Message cannot be read .....	56
Attachment saving failure .....	56
LCD login .....	57
LCD login failure .....	57
<b>Event POP3.....</b>	<b>59</b>
POP3-related events .....	59
<b>Event IMAP .....</b>	<b>61</b>
IMAP-related events.....	61
<b>Event HA .....</b>	<b>63</b>
Master mode .....	63
Slave mode .....	63
Master role.....	63
<b>Event Webmail.....</b>	<b>65</b>
User login.....	65
<b>Antivirus.....</b>	<b>67</b>
Example .....	67
<b>Virus infection .....</b>	<b>67</b>
<b>Antispam.....</b>	<b>69</b>
Example .....	69
<b>Spam-related events .....</b>	<b>69</b>
<b>Deep header scanner rules reload .....</b>	<b>69</b>
<b>Index.....</b>	<b>71</b>



# 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 Installation 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.
- *FortiMail User Guides*  
Provides information that the FortiMail end users need to know in order to take advantage of the services provided by the FortiMail unit. These guides are included as chapters in the *FortiMail Administration Guide*, allowing the administrator to provide information on only the enabled features. For details, see *FortiMail Administration Guide*.

## 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](mailto: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	The History log records all email traffic going through the FortiMail unit.
Event	elog	The Event log 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	The Antispam log records spam detection events.
Antivirus	vlog	The Antivirus log records virus intrusion events.

Each of these four 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 four 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.

## 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

## 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**

<b>2006-10-10</b>	The year, month and day when the event occurred in the format, yy-mm-dd.
<b>10:19:08</b>	The hour, minute and second of when the event occurred
<b>log_id=(0114000000)</b>	An eleven-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 message ID number.
<b>type=(event)</b>	The section of the system where the event occurred. The log types are event, antivirus, antispam, and history.
<b>subtype=(imap)</b>	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.
<b>pri=(debug)</b>	The severity level, or priority, or the event. There are seven logging severity levels.
<b>user=(mail)</b>	The name of the user creating the traffic.
<b>ui=(mail)</b>	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.
<b>action=(unknown)</b>	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.
<b>status=(success)</b>	The status of the event. Status can be success, none, or failure.
<b>msg=("fortimail_debug000: user=jww@vjiang-fortinet.com, passwd=123)</b>	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.

<b>militer</b>	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.
<b>fas_militer</b>	This means FortiMail Antispam Mail filter. This covers all scanning, except antivirus. Antivirus may be included in fas_militer in future FortiMail firmware releases.
<b>sendmail</b>	Sendmail is a mail transfer agent (MTA) and is a well known project of open source, freeware and Unix communities.
<b>dbdaemon</b>	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.
<b>mysqld</b>	This is a multi-threading application which needs to start multiple separate threads to handle different but related threading tasks.
<b>Militer (fas_militer): timeout before data read</b>	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.
<b>Militer_read (fas_militer): cmd read returned 0, expecting 5</b>	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=<0e6d01c8384249785900e98c14ac@kjsad>
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=156H19fK001393
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 --"
```



# 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

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

## System update setting

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

## interface IP address

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information

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

## Access methods/status

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

## Interface status

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

## Interface status/PPPoE status

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

## Interface status/PPPoE settings

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information
<b>Message</b>	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>)}"
<b>Meaning</b>	An administrator changed PPPoE settings using the CLI or GUI.

## Management IP

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

## Interface access methods

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

## MTU change

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

## Interface status

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

## Addressing mode of interface access methods

<b>Type</b>	Event
<b>Subtype</b>	Config

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

## Connect option of interface access methods

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

## DNS change

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

## Primary DNS and secondary DNS

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

## Default gateway

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

## Route entry

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

## Route with destination IP address/netmask

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information
<b>Message</b>	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>)}"
<b>Meaning</b>	An administrator added a route with destination address/netmask using either the CLI or web-based manager.

## Routing entry

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

## System timezone

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

## Daylight saving time

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

## NTP server settings

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

## System time

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

## Console pageNo setting

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

## Console mode setting

<b>Type</b>	Event
<b>Subtype</b>	Config

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

## Idle timeout

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

## Authentication timeout

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

## System language

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information
<b>Message</b>	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>)}"
<b>Meaning</b>	An administrator changed the system language to another language using the CLI or web-based manager.

## LCD PIN number

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

## LCD PIN protection

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

## GUI refresh interval

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

## System idle and auth timeout

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

## Admin addition

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

## Admin change

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

## Admin deletion

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

## Admin password change

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

## HA settings

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

## SNMP status

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information

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

## SNMP config info

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

## SNMP CPU threshold

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

## SNMP memory threshold

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

## SNMP Logdisk threshold

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

## SNMP maildisk threshold

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

## SNMP deferred mqueue threshold

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

## SNMP virus detection threshold

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

## SNMP spam detection threshold

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

## SNMP community entry

<b>Type</b>	Event
<b>Subtype</b>	Config

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

## SNMP community and host entry

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

## FortiMail disclaimer in header for outgoing messages

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

## FortiMail disclaimer in body for incoming messages

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

## FortiMail disclaimer in header for incoming messages

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information

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

## Local domains

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

## POP3 server port number

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

## Relay server name

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

## SNMP memory threshold

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

## SMTP auth

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

## SMTP over ssl

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

## SMTP server port number

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

## Status of email archiving

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

## Email archiving account

<b>Type</b>	Event
<b>Subtype</b>	Config

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

## Email archiving rotate setting

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

## Archiving settings on local server

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

## Archiving settings on remote server

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

## Archiving policy

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

## Archiving exempt

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

## System quarantine account

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

## System quarantine rotate setting

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

## System quarantine quota settings

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

## System quarantine settings

<b>Type</b>	Event
<b>Subtype</b>	Config

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

## Mail server settings

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

## FortiMail appearance information

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

## FortiMail mail gw user group

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

## Permission of mail

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information

<b>Message</b>	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>)}"
<b>Meaning</b>	An administrator set or deleted permission of mail using the CLI or web-based manager.

## Mail server access

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

## Local domain deletion

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

## Local domain addition

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

## Local user

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

## Local domain name

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

## User group

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

## Mail user addition/deletion

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

## Mail server user addition

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

## Mail server user set with information

<b>Type</b>	Event
<b>Subtype</b>	Config

<b>Severity</b>	Information
<b>Message</b>	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>)}"
<b>Meaning</b>	An administrator sets a mail server user with information using the CLI or web-based manager.

## Mail server user added with information

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

## Mail server user deletion

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

## Disk quota of email archiving account

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

## Password of email archiving account

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

## Forwarding address for email archiving

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

## Password of system quarantine account

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

## Forwarding address for system quarantine

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

## Password of mail user

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

## Display name of mail user

<b>Type</b>	Event
<b>Subtype</b>	Config

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

## User alias

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

## POP3 auth profile

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

## IMAP auth profile

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

## Email banned word

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

## Local log setting

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

## Memory log setting

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

## Log setting

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

## Log setting elog

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

## Log policy

<b>Type</b>	Event
<b>Subtype</b>	Config

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

## Alertemail setting

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

## Alertemail SMTP server

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information
<b>Message</b>	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>)"
<b>Meaning</b>	An administrator changed the alertemail SMTP server to and a user was changed using the web-based manager.

## Alertemail target email addresses

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

## Alertemail configuration

<b>Type</b>	Event
<b>Subtype</b>	Config
<b>Severity</b>	Information
<b>Message</b>	msg="Alertemail configuration has been modified by user <user_name> via GUI(<ip_address>)"
<b>Meaning</b>	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 restart](#)

[System shutdown](#)

[System reload](#)

[System reset](#)

[System firmware upgrade](#)

[Upgrade system firmware failed](#)

[System mode](#)

## DNS servers

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

## System restart

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

## System shutdown

<b>Type</b>	Event
<b>Subtype</b>	System

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

## System reload

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

## System reset

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

## System firmware upgrade

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

## Upgrade system firmware failed

<b>Type</b>	Event
<b>Subtype</b>	System
<b>Severity</b>	Warning

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

## System mode

<b>Type</b>	Event
<b>Subtype</b>	System
<b>Severity</b>	Warning
<b>Messages</b>	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>)"
<b>Meaning</b>	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

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



# 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

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

## Starting flgrptd

<b>Type</b>	Event
<b>Subtype</b>	SMTP
<b>Severity</b>	Information
<b>Message</b>	msg= "Starting flgrptd"
<b>Meaning</b>	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

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

## FortiGuard antispam rule (FSAR) loading

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

## FASR readme

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

## FortiGuard antispam rule (FSAR) loaded

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

## Mail aliases rebuilt

<b>Type</b>	Event
<b>Subtype</b>	SMTP
<b>Severity</b>	Notification

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

## Antivirus database loaded

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

## Updated daemon restarted

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

## Antivirus database loading

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

## Antivirus database loaded

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

## Bayesian database training

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

## Bayesian database training completed

<b>Type</b>	Event
<b>Subtype</b>	SMTP
<b>Severity</b>	Information
<b>Message</b>	msg= "Bayesian Training: <integer> messages finished"
<b>Meaning</b>	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.

<a href="#">User login</a>	<a href="#">Message cannot be read</a>
<a href="#">Webmail login</a>	<a href="#">Attachment saving failure</a>
<a href="#">User login failure</a>	<a href="#">LCD login</a>
<a href="#">WebMail GUI failure</a>	<a href="#">LCD login failure</a>
<a href="#">Message retrieval failure</a>	

## User login

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

## Webmail login

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

## User login failure

<b>Type</b>	Event
<b>Subtype</b>	Admin

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

## WebMail GUI failure

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

## Message retrieval failure

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

## Message cannot be read

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

## Attachment saving failure

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

## LCD login

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

## LCD login failure

<b>Type</b>	Event
<b>Subtype</b>	Admin
<b>Severity</b>	Information
<b>Message</b>	msg="Login from LCD failed"
<b>Meaning</b>	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

<b>Log Type</b>	Event
<b>Subtype</b>	POP3
<b>Severity</b>	All severity levels
<b>Message</b>	msg="<log_message_information>"
<b>Meaning</b>	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

<b>Log type</b>	Event
<b>Subtype</b>	IMAP
<b>Severity</b>	All severity levels
<b>Message</b>	msgs="<log_message_information>"
<b>Meaning</b>	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

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

## Slave mode

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

## Master role

<b>Log type</b>	Event
<b>Subtype</b>	HA
<b>Severity</b>	Information

<b>Message</b>	msgs="monitord: ** reached retry limit, assuming MASTER role"
<b>Meaning</b>	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

<b>Log type</b>	Event
<b>Subtype</b>	Webmail
<b>Severity</b>	All severity levels
<b>Message</b>	msgs="User <user_name> from <IP address> logged in."
<b>Meaning</b>	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

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

## Deep header scanner rules reload

<b>Log Type</b>	Antispam
<b>Subtype</b>	Spam detect
<b>Severity</b>	Notification

<b>Message</b>	msg="Deep Header Scanner Rules Reload - Finished."
<b>Meaning</b>	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, 69
  - deep header scanner reload, 69
  - spam-related events, 69
- antivirus, 67
  - file name infection, 67

## D

- documentation
  - Fortinet, 9

## E

- event admin, 55
  - attachment saving failure, 56
  - LCD login, 57
  - LCD login failure, 57
  - message cannot be read, 56
  - message retrieval failure, 56
  - user login, 55
  - user login failure, 55
  - webmail GUI failure, 56
  - webmail login, 55
- event config, 19
  - access methods/status, 21
  - addressing mode of interface access methods, 22
  - admin addition, 27
  - admin change, 28
  - admin deletion, 28
  - admin password change, 28
  - alertemail configuration, 43
  - alertemail setting, 43
  - alertemail SMTP server, 43
  - alertemail target email addresses, 43
  - archiving exempt, 35
  - archiving policy, 34
  - archiving settings on local server, 34
  - archiving settings on remote server, 34
  - authentication timeout, 26
  - connect option of interface access methods, 23
  - console mode setting, 25
  - console pageNo setting, 25
  - daylight saving time, 25
  - default gateway, 23
  - disk quota of email archiving account, 39
  - display name of mail user, 40
  - DNS change, 23
  - email archiving account, 33
  - email archiving rotate setting, 34
  - email banned word, 41
  - FortiGuard autoupdate settings, 20
  - FortiMail appearance information, 36
  - FortiMail disclaimer in body for incoming messages, 31
  - FortiMail disclaimer in header for incoming messages, 31
  - FortiMail disclaimer in header for outgoing messages, 31
  - FortiMail mail gw user group, 36
  - forwarding address for email archiving, 40
  - forwarding address for system quarantine, 40
  - GUI refresh interval, 27
  - HA settings, 28
  - idle timeout, 26
  - IMAP auth profile, 41
  - interface access methods, 22
  - interface IP address, 20
  - interface status, 21, 22
  - interface status/PPPoE settings, 21
  - interface status/PPPoE status, 21
  - LCD PIN number, 26
  - LCD PIN protection, 27
  - local domain addition, 37
  - local domain deletion, 37
  - local domain name, 38
  - local domains, 32
  - local log setting, 42
  - local user, 37
  - log policy, 42
  - log setting, 42
  - log setting elog, 42
  - mail server access, 37
  - mail server settings, 36
  - mail server user added with information, 39
  - mail server user addition, 38
  - mail server user deletion, 39
  - mail server user set with information, 38
  - mail user addition/deletion, 38
  - management IP, 22
  - memory log setting, 42
  - MTU change, 22
  - NTP server settings, 25
  - password of email archiving account, 39
  - password of mail user, 40
  - password of system quarantine account, 40
  - permission of mail, 36
  - POP3 auth profile, 41
  - POP3 server port number, 32
  - primary DNS and secondary DNS, 23
  - relay server name, 32
  - route entry, 24
  - route with destination IP address/netmask, 24
  - routing entry, 24
  - SMTP auth, 33
  - SMTP over ssl, 33
  - SMTP server port number, 33
  - SNMP community and host entry, 31
  - SNMP community entry, 30
  - SNMP config info, 29
  - SNMP CPU threshold, 29
  - SNMP deferred mqueue threshold, 30
  - SNMP Logdisk threshold, 29
  - SNMP maildisk threshold, 30
  - SNMP memory threshold, 29, 32
  - SNMP spam detection threshold, 30
  - SNMP status, 28
  - SNMP virus detection threshold, 30
  - status of email archiving, 33
  - system idle and auth timeout, 27
  - system language, 26
  - system quarantine account, 35

- system quarantine quota settings, 35
  - system quarantine settings, 35
  - system time, 25
  - system timezone, 24
  - system update setting, 20
  - user alias, 41
  - user group, 38
  - event HA, 63
    - master mode, 63
    - master role, 63
    - slave mode, 63
  - event IMAP, 61
    - IMAP-related events, 61
  - event POP3, 59
    - POP3-related events, 59
  - event SMTP, 51
    - antivirus database loaded, 53
    - antivirus database loading, 53
    - bayesian database training, 54
    - bayesian database training completed, 54
    - FASR readme, 52
    - FortiGuard antispam rule (FSAR) loaded, 52
    - FortiGuard antispam rule (FSAR) loading, 52
    - mail aliases rebuilt, 52
    - SMTP-related events, 51
    - starting flgrptd, 51
    - updated daemon restarted, 53
    - virus db loaded, 52
  - event system, 45
    - FortiGuard update result, 49
    - system firmware upgrade, 46
    - system mode, 47
    - system reload, 46
    - system reset, 46
    - system restart, 45
    - system shutdown, 45
    - upgrade system firmware failed, 46
  - event update, 49
  - event webmail, 65
    - user login, 65
- ## F
- Fortinet
    - Knowledge Base, 10
    - Technical Documentation, 10
    - 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, 35

**F**ORTINET®

[www.fortinet.com](http://www.fortinet.com)

**F**ORTINET®

[www.fortinet.com](http://www.fortinet.com)