



FortiMail Log Message Version 3.0

This document is published periodically and contains only log messages acquired at the date of publication.

FORTINET™

www.fortinet.com

FortiMail Log Message Reference

Version 3.0

January 28, 2009

06-30004-88959-20090128

© Copyright 2009 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.

Contents

| | |
|---|-----------|
| Introduction | 7 |
| About this document..... | 7 |
| FortiMail documentation | 7 |
| Comments on FortiMail technical documentation | 8 |
| Customer service and technical support | 8 |
| Register your Fortinet product..... | 9 |
| FortiMail log message overview | 11 |
| FortiMail log categories | 11 |
| History logs | 11 |
| Event logs | 12 |
| Antispam logs..... | 12 |
| Antivirus logs..... | 12 |
| Log types and subtypes..... | 13 |
| Logging severity levels | 13 |
| FortiMail log messages | 14 |
| FortiMail error log messages..... | 15 |
| What's new | 17 |
| What's new in v3.0 MR4 | 17 |
| What's new in v3.0 MR3 | 18 |
| What's new in v3.0 MR2 | 21 |
| What's new in v3.0 MR1 | 21 |
| What's new in v3.0 GA | 21 |

| | |
|--------------------------------|-----------|
| History logs | 23 |
| Event-Config logs | 27 |
| Event-System logs | 63 |
| Event-Update logs | 69 |
| Event-Admin logs | 71 |
| Event-SMTP logs..... | 75 |
| Event-POP3 logs..... | 79 |
| Event-IMAP logs..... | 81 |
| Event-HA logs | 83 |
| Anti-virus logs..... | 87 |
| Anti-spam logs | 89 |

Introduction

This document introduces you to the log messages generated by the FortiMail unit in FortiMail v3.0. This document also includes examples of log messages that the FortiMail unit may generate.

This chapter includes the following topics:

- [About this document](#)
- [FortiMail documentation](#)
- [Customer service and technical support](#)
- [Register your Fortinet product](#)

About this document

This document explains all log messages generated by the FortiMail unit in FortiMail v3.0, along with examples of log messages. This document contains the following chapters:

- [FortiMail log message overview](#)
- [What's new](#)
- [History logs](#)
- [Event-Config logs](#)
- [Event-System logs](#)
- [Event-Update logs](#)
- [Event-Admin logs](#)
- [Event-SMTP logs](#)
- [Event-POP3 logs](#)
- [Event-IMAP logs](#)
- [Event-HA logs](#)
- [Anti-spam logs](#)
- [Anti-virus logs](#)

FortiMail documentation

You can find FortiMail documentation from the following resources:

Online Help

- [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. You can access online help when using the webmail.

Fortinet Documentation CD

All Fortinet documentation is available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. The CD contains the following documents:

- *FortiMail QuickStart Guides*

Provides basic information about connecting and installing a FortiMail unit. A separate guide is available for each FortiMail model.

- *FortiMail Install Guide*

Describes how to set up the FortiMail unit in transparent, gateway, or server mode.

- *FortiMail Administration Guide*

This document. 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 CLI Reference*

Describes how to use the FortiMail CLI and contains a reference of all FortiMail CLI commands.

Fortinet Documentation Web Site

Go to <http://docs.forticare.com> to get the up-to-date FortiMail documentation.

Fortinet Knowledge Center

Go to <http://kc.forticare.com> to find more FortiMail related documents:

- *FortiMail Log Message Reference*

Describes the structure of FortiMail log messages and provides information about the log messages that are generated by FortiMail units.

- Other troubleshooting and how-to articles, FAQs, technical notes, and more.

Comments on FortiMail technical documentation

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

Customer service and technical support

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

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services Fortinet provides.

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

Register your Fortinet product

Register your Fortinet product to receive Fortinet customer services such as product updates and technical support. You must also register your product for FortiGuard services such as FortiGuard Antivirus and Intrusion Prevention updates and for FortiGuard Web Filtering and AntiSpam.

Register your product by visiting <http://support.fortinet.com> and selecting Product Registration.

To register, enter your contact information and the serial numbers of the Fortinet products that you or your organization have purchased. You can register multiple Fortinet products in a single session without re-entering your contact information.

FortiMail log message overview

FortiMail logs provide historical information as well as current analysis of network email activities that help identify security issues such as viruses within emails.

For more information about configuring logging in FortiMail v3.0, see the *FortiMail Administration Guide*.

This section contains the following topics:

- [FortiMail log categories](#)
- [Log types and subtypes](#)
- [Logging severity levels](#)
- [FortiMail log messages](#)
- [FortiMail error log messages](#)

FortiMail log categories

FortiMail logs record information per recipient. By recording logs per recipient, log information is presented in layers, which means that one log file category contains the “what” and another log file category 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 categories:

| Log Types | File Name | Description |
|-----------|-----------|--|
| Event | elog | The Event log records management and activity events. Management events include changes to the system configuration as well as administrator and user logins and logouts. Activity events include system activities. |
| Antispam | slog | The Antispam log records spam detection events. |
| Antivirus | vlog | The Antivirus log records virus intrusion events. |
| History | alog | The History log records all email traffic going through the FortiMail unit. |

Each of these four log categories contains a session identification (ID) number, located in the session ID field of each log message. 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, and then go to other logs with that session ID to 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 take the session ID number and match 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 shown in the example in ["History logs" on page 11](#).

Antispam log messages describe spam URIs, 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.

Log types and subtypes

FortiMail logs are grouped into categories by log type and subtype with corresponding log message identification numbers. For example, event logs are identified by the numbers 01, with the subcategory config identified by the numbers 00. The event-config log is identified by the numbers 0100.

| Log Type | Category Number | Subtype | Sub-type Number |
|----------|-----------------|---------------|-----------------|
| event | 01 | config | 00 |
| | | admin | 04 |
| | | system | 06 |
| | | ha | 07 |
| | | update | 10 |
| | | pop3 | 11 |
| | | imap | 12 |
| | | smtp | 13 |
| virus | 02 | virus detect | 00 |
| history | 04 | email history | 00 |
| antispam | 05 | spam detect | 01 |

Logging 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. |

FortiMail log messages

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) | A ten-digit number that identifies the log type. The first two digits represent the log type, and the following two digits represent the log subtype. The last six digits are the message ID number. |
| type=(event) | The section of the system where the event occurred. The log types are event, antivirus, antispam, and history. |
| subtype=(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.

FortiMail 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. |

What's new

When Fortinet releases a new maintenance release, log messages and changes to existing log messages usually occurs. These changes and new log messages occur because of changes to existing features or new features included in the maintenance release. This section explains these changes to existing log messages and if any new log messages will be recorded in the new maintenance release.

If you require additional information about a specific log message your FortiMail unit records that is not included or fully explained in this document, contact techdocs@fortinet.com for this information and include the following:

- firmware version
- build number
- line number (found in the # column when viewing log messages)

For example, an error message displays in the Event log type tab; the current firmware version is FortiMail 3.0 MR2 build-199 and the line number is 5.

The following topics are included in this section:

- [What's new in v3.0 MR4](#)
- [What's new in v3.0 MR3](#)
- [What's new in v3.0 MR2](#)
- [What's new in v3.0 MR1](#)
- [What's new in v3.0 GA](#)



Note: The following information includes only changes to existing log messages and new log messages.

What's new in v3.0 MR4

In FortiMail v3.0 MR4 release, two new log message subtypes were created. They are Event-HA (identified by the numbers 0107) and Event-Update (identified by the numbers 0110).

History logs include a new field called **direction**, within the log file. This new field indicates whether the email message is destined for a managed or protected domain or if the email message's destination is unknown. The following is an example of a history log, with the new field in bold, recorded in FortiMail 3.0 MR4.

```
2008-10-06 14:38:41 log_id=0400016394 log_part=00 type=statistics
subtype=n/a pri=information session_id=m96IbaBW001359
from="user1@example.com" mailer="mta" client_name="[172.16.122.14]"
direction="out" message_length=55 virus="" disposition=0x01
classifier=0x00 subject="June sales inventory"
```

What's new in v3.0 MR3

In FortiMail v3.0 MR3 release, many changes occurred with log messages, as well as how to view or search log messages. The Anti-spam log chapter, as well as the History and Event-SMTP log chapters, all include one new log message. The History log chapter also contains updated information about classifier and disposition numbers.

All log messages now contain the field, log_part, and is found in the log header. The log_part field contains the number associated with a log message that has split. Log message length is now 1 kilobyte. The log_part field information is in numbers, usually containing the numbers 00, but if the log message is split, the numbers will be 01, 02, and so on depending on how many times the log message was split. The numbers help administrators to identify the split log message along with the session ID number.

You can now view log messages in Raw format by moving your mouse over a number in the # column, as shown in Figure 1. You can also highlight a log message by selecting the row that the log message is in, which is also shown in Figure 1.

Accessing log messages has also changed, and rolled log files were renamed as well. Log files now contain a start time and an end time, in the Logging menu. The start time and end times are links, including the Current link, and when you select one of the links you are redirected to those log messages that were recorded in that time period. Rolled logs and the current log file are shown in Figure 2.

Figure 1: Viewing log messages

| # | Date | Time | Type | Log Id | Message |
|----|------------|----------|-------|------------|---|
| 1 | 2008-01-15 | 09:36:30 | event | 0115000000 | starting daemon: SMTP+persistent-queueing@00:00:01 |
| 2 | 2008-01-15 | 09:36:30 | event | 0115000000 | 0 aliases, longest 0 bytes, 0 bytes total |
| 3 | 2008-01-15 | 09:36:30 | event | 0115000000 | alias database /var/spool/etc/mail/aliases has been rebuilt |
| 4 | 2008-01-15 | 09:36:30 | event | 0115000000 | Initializing FASR /var/spool/etc/antispam done! |
| 5 | 2008-01-15 | 09:36:30 | event | 0115000000 | Parsing FASR Readme /var/spool/etc/antispam/README ... |
| 6 | 2008-01-15 | 09:36:30 | event | 0115000000 | Initializing FASR /var/spool/etc/antispam ... |
| 7 | 2008-01-15 | 09:36:30 | event | 0115000000 | Successfully loaded virus db: /var/spool/etc/vir |
| 8 | 2008-01-15 | 09:36:30 | event | 0115000000 | Starting flgrptd |
| 9 | 2008-01-15 | 09:36:30 | event | 0115000000 | Loading virusdb: /var/spool/etc/vir ... |
| 10 | 2007-12-17 | 14:47:02 | event | 0115000000 | starting daemon: SMTP+persistent-queueing@00:00:01 |
| 11 | 2007-12-17 | 14:47:02 | event | 0115000000 | 0 aliases, longest 0 bytes, 0 bytes total |
| 12 | 2007-12-17 | 14:47:02 | event | 0115000000 | alias database /var/spool/etc/mail/aliases has been rebuilt |
| 13 | 2007-12-17 | 14:47:01 | event | 0115000000 | Initializing FASR /var/spool/etc/antispam done! |
| 14 | 2007-12-17 | 14:47:01 | event | 0115000000 | Parsing FASR Readme /var/spool/etc/antispam/README ... |
| 15 | 2007-12-17 | 14:47:01 | event | 0115000000 | Initializing FASR /var/spool/etc/antispam ... |
| 16 | 2007-12-17 | 14:47:01 | event | 0115000000 | Successfully loaded virus db: /var/spool/etc/vir |
| 17 | 2007-12-17 | 14:47:00 | event | 0115000000 | Loading virusdb: /var/spool/etc/vir ... |
| 18 | 2007-12-17 | 14:47:00 | event | 0115000000 | Starting flgrptd |
| 19 | 2007-12-17 | 14:32:51 | event | 0115000000 | starting daemon: SMTP+persistent-queueing@00:00:01 |
| 20 | 2007-12-17 | 14:32:51 | event | 0115000000 | 0 aliases, longest 0 bytes, 0 bytes total |
| 21 | 2007-12-17 | 14:32:51 | event | 0115000000 | alias database /var/spool/etc/mail/aliases has been rebuilt |
| 22 | 2007-12-17 | 14:32:51 | event | 0115000000 | Initializing FASR /var/spool/etc/antispam done! |
| 23 | 2007-12-17 | 14:32:51 | event | 0115000000 | Parsing FASR Readme /var/spool/etc/antispam/README ... |
| 24 | 2007-12-17 | 14:32:51 | event | 0115000000 | Initializing FASR /var/spool/etc/antispam ... |
| 25 | 2007-12-17 | 14:32:50 | event | 0115000000 | Successfully loaded virus db: /var/spool/etc/vir |

Figure 2: Accessing log files in the Logging menu

| # | Start time | End time | Size | Action |
|----|-------------------------|-------------------------|----------|-------------------------------|
| 1 | 2008-01-15 09:13:16 Tue | Current | 20268 | [Download] [Refresh] [Delete] |
| 2 | 2008-01-09 16:33:38 Wed | 2008-01-15 09:13:16 Tue | 6144 | [Download] [Refresh] [Delete] |
| 3 | 2007-11-16 09:19:19 Fri | 2008-01-09 16:31:39 Wed | 714240 | [Download] [Refresh] [Delete] |
| 4 | 2007-10-15 17:43:39 Mon | 2007-11-16 09:17:34 Fri | 829440 | [Download] [Refresh] [Delete] |
| 5 | 2007-10-02 10:13:19 Tue | 2007-10-15 16:42:14 Mon | 26624 | [Download] [Refresh] [Delete] |
| 6 | 2007-08-10 09:34:33 Fri | 2007-10-02 09:12:58 Tue | 1158656 | [Download] [Refresh] [Delete] |
| 7 | 2007-08-10 08:02:16 Fri | 2007-08-10 08:34:14 Fri | 251392 | [Download] [Refresh] [Delete] |
| 8 | 2007-08-07 15:30:45 Tue | 2007-08-10 07:02:04 Fri | 10485760 | [Download] [Refresh] [Delete] |
| 9 | 2007-08-04 22:59:05 Sat | 2007-08-07 14:30:34 Tue | 10485760 | [Download] [Refresh] [Delete] |
| 10 | 2007-08-02 06:30:38 Thu | 2007-08-04 21:58:53 Sat | 10485760 | [Download] [Refresh] [Delete] |
| 11 | 2007-07-30 14:04:24 Mon | 2007-08-02 05:30:25 Thu | 10485760 | [Download] [Refresh] [Delete] |
| 12 | 2007-07-27 21:46:50 Fri | 2007-07-30 13:04:14 Mon | 10485760 | [Download] [Refresh] [Delete] |
| 13 | 2007-07-25 05:33:06 Wed | 2007-07-27 20:46:39 Fri | 10485760 | [Download] [Refresh] [Delete] |
| 14 | 2007-07-20 17:26:41 Fri | 2007-07-25 04:32:55 Wed | 10485760 | [Download] [Refresh] [Delete] |
| 15 | 2007-07-15 16:31:57 Sun | 2007-07-20 16:26:20 Fri | 10485760 | [Download] [Refresh] [Delete] |
| 16 | 2007-07-10 16:24:18 Tue | 2007-07-15 15:31:37 Sun | 10485760 | [Download] [Refresh] [Delete] |

When downloading logs, the naming scheme has changed to a date and time format. For example, the antivirus log, using the new naming scheme, is 2007-12-13-09-34-06_2008-02-27-11-13-39.vlog.log. The following table explains each part of the new naming scheme.

- 2007-12-13** The start date of the log file in the format, yyyy-mm-dd.
- 09-34-06** The start time of the log file in the format hh:mm:ss.
- 2008-02-27** The end date of the log file.
- 11-13-39** The end time of the log file in the format hh:mm:ss.
- vlog.log** The name of the log file, for example, the event log is elog.log.

Searching log messages now contains several additional options, including From, To, Session ID, and Time Within. You can search event log messages by selecting the search icon, or use the subtype drop-down list. The following are tables that explain search options for searching event logs by subtype, or using the search icon.

Table 3: Available options when using the Search icon for searching log messages.

| | | |
|---------------------------------------|---|---|
| Keyword | Enter the word or words to search for within the log file. | |
| Subject (History Log only) | If you are searching for emails, enter the subject line of the email contained in the email. | |
| From | If you are searching for emails, enter the sender's email address. | |
| To | If you are searching for emails, enter the receiver's email address. | |
| Session Id | Enter the session identification of the log message you are searching for. | |
| Log Id | Enter the log identification number of the log message you are searching for. | |
| Client Name (History Log only) | Enter the client name of the log messages you are searching for. The client name is usually an IP address, for example, 10.30.15.1. | |
| Time within | Enter the time period of when the log message occurred. Use the following options. | |
| | [0 day] | In the first line, select from the drop-down list, one of the following: <ul style="list-style-type: none"> • 0 day – default • One day – day of specified date and time • One week – week starting before specified date and time • Two weeks – two week period starting before specified date and time • One month – month time period starting before specified date and time |
| | [12] hour(s) | Select the number of hours from the drop-down list. The list provides numbers in the 24 hour format, 0-23. The default is 12. |
| | [current day of the current month] | Select the date for the search. The default is the current day of the current month. For example, 26 displays because it is February 26, 2008. |
| | [current month] | Select the month for the search. The default is the current month. For example, February displays because it is the current month. |
| | [current year] | Select the year for the search. The default is the current year. For example, 2008, because 2008 is the current year. |
| [current time] | Select the time for the search. The default is the current time. The format is hour only and is in the 24 hour format. For example, the time that displays is 10 because it is 10 am. | |

Table 4: Subtype drop-down list options

| | |
|-----------------------|--|
| ALL | Displays no filtering on the subtype column. |
| Configuration | Displays log messages containing only configuration in the subtype field. |
| Admin User | Displays log messages containing only admin user in the subtype field. |
| Web Mail | Displays log messages containing only webmail in the subtype field. |
| System | Displays log messages containing only system in the subtype field. |
| HA | Displays log messages containing only HA in the subtype field. |
| Update Failure | Displays log messages containing only Update Failure in the subtype field. |
| Update Success | Displays log messages containing only Update Success in the subtype field. |

Table 4: Subtype drop-down list options

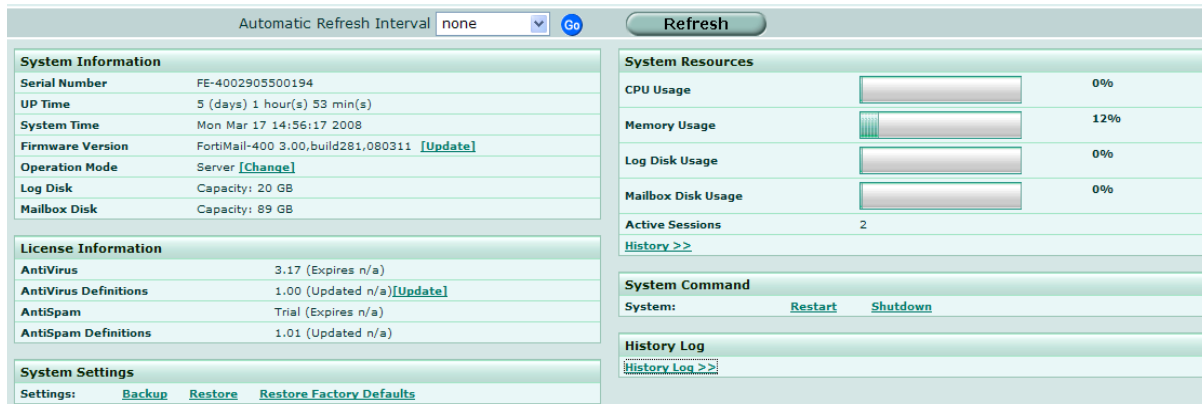
| | |
|---------------|--|
| POP3 | Displays log messages containing only POP3 in the subtype field. |
| IMAP | Displays log messages containing only IMAP in the subtype field. |
| SMTP | Displays log messages containing only SMTP in the subtype field. |
| OTHERS | Displays all lines that have a value other than all of the above subtypes, from Configuration to SMTP. |

What's new in v3.0 MR2

In FortiMail v3.0 MR2 release, the System Status page now includes History logs, and is available whether in advanced management mode or basic management mode. All log messages can be viewed in either basic or advanced management mode.

History logs are now available on the System Status page. You can navigation features, allowing you to download, empty or delete these logs.

Figure 3: History logs on the System Status page



The Log & Report menu also rearranged the order of the log type tabs: History, Event, Antispam, and Antivirus.

A new log message has been added to the Event-SMTP log chapter for 000000.

What's new in v3.0 MR1

FortiMail v3.0 MR1 release now supports a maximum of 1000 log files for the FortiMail-2000 unit and higher.

What's new in v3.0 GA

FortiMail v3.0 GA release removed the log messages for expiremail bayesian database cleanup.

History logs

History log messages record all mail traffic going through the FortiMail unit.

History log messages are identified with the numbers 0400 and have a subcategory called Email History. The Email History subcategory is identified with the numbers 050100.

History log messages, when displayed in the web-based manager, only display the classifier names and disposition names. When viewing history log messages 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 5: 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 6: 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 |
| 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 |

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
--"
```



Note: Log headers in FortiMail v3.0 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.

The history logs contain the following message, listed by the message ID:

050100

| | |
|--------------------------|--|
| Message ID | 050100 |
| Log Type | History |
| FortiMail version | v3.0 GA to MR2 |
| Severity | Information |
| Message | session_id="<mail_session_identification>" from="<sender_email_address>" client_name="<resolved_client_name>" resolved="{OK FAIL FORGED TEMP}" to="<recipient_email_address>" subject="<subject_line>" message_length="<email_message_length>" virus="<virus_name>" disposition="{0 1 2}" classifier="{0xM<number>}" |
| Meaning | The history log contains all log messages generated on the FortiMail unit. See Table 5 on page 23 about disposition field explanations and Table 6 on page 24 for information about classifier field explanations. |

| | |
|--------------------------|---|
| Message ID | 050100 |
| Log Type | History |
| FortiMail version | v3.0 MR3 |
| Severity | Information |
| Message | session_id="<mail_session_identification>" from="<sender_email_address>" mailer=mta client_name="<resolved_client_name>" resolved="{OK FAIL FORGED TEMP}" to="<recipient_email_address>" message_length="<email_message_length>" virus="<virus_name>" disposition="{0 1 2}" classifier="{0xM<number>}" subject="<subject_line>" |
| Meaning | The history log contains all log messages generated on the FortiMail unit. See Table 5 on page 23 about disposition field explanations and Table 6 on page 24 for information about classifier field explanations. |

| | |
|--------------------------|-----------------|
| Message ID | 050100 |
| Log Type | History |
| FortiMail version | v3.0 MR4 and up |
| Severity | Information |

| | |
|-------------------|---|
| Message ID | 050100 |
| Message | session_id=<mail_session_identification> from=<sender_email_address> mailer=mta client_name=<resolved_client_name> resolved="{OK FAIL FORGED TEMP}" to=<recipient_email_address> direction={in out unknown} message_length=<email_message_length> virus=<virus_name> disposition={0 1 2} classifier={0xM<number>} subject=<subject_line> |
| Meaning | The history log contains all log messages generated on the FortiMail unit. See Table 5 on page 23 about disposition field explanations and Table 6 on page 24 for information about classifier field explanations. In this log message, the direction field contains the following: <ul style="list-style-type: none"> • in – indicates that the message is destined for a managed or protected domain • out – indicates that the message is not destined for a managed or protected domain • unknown – indicates that the direction is undetermined |

Event-Config logs

All event logs in FortiMail v3.0 begin with 01. The Event log is a large category, containing six subcategories. The first subcategory is Config and is identified by the message identification number 00, or 0100.

The six subcategories are:

- Event-Config: 0100
- Event-Admin: 0104
- Event-System: 0106
- Event-SMTP: 0113
- Event-POP3: 0111
- Event-IMAP: 0112

Event-Config logs record all configuration changes made to the system of the FortiMail unit, configuration setting, administration, including POP3, SMTP, and IMAP changes.

Example

In this example, an admin user changed the DNS settings using the CLI console access.

```
2008-09-12 13:56:56 log_id=0100010601 log_part=00 type=event subtype=config
pri=information user=admin ui=console module=system submodule=dns msg="DNS
has been changed by user admin via CLI (console)"
```



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.

The Event-Config logs contains the following types of messages, listed by message IDs:

| | | |
|--------|--------|--------|
| 010208 | 011001 | 030303 |
| 010209 | 011002 | 030501 |
| 010402 | 011003 | 030502 |
| 010403 | 011004 | 030503 |
| 010404 | 011005 | 030601 |
| 010405 | 011006 | 030602 |
| 010406 | 011007 | 030603 |
| 010409 | 011008 | 030701 |
| 010410 | 011101 | 030702 |
| 010414 | 011102 | 030703 |
| 010415 | 011103 | 030801 |
| 010416 | 011021 | 030802 |
| 010601 | 011301 | 030803 |
| 010602 | 011303 | 030902 |
| 010702 | 011901 | 090101 |
| 010703 | 012001 | 090112 |
| 010705 | 012101 | 090301 |
| 010706 | 030101 | 090302 |
| 010901 | 030102 | 090303 |
| 010902 | 030103 | 090305 |
| 010904 | 030302 | |

010208

| | |
|--------------------------|--|
| Message ID | 010208 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=update msg="Autoupdate settings have been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed the autoupdate settings using the CLI. |

010209

| | |
|--------------------------|---|
| Message ID | 010209 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=update msg="System update setting has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed a system update setting using the web-based manager. |

010402

| | |
|--------------------------|--|
| Message ID | 010402 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="interface {port1 port2 ...} ip address changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed an interface IP address using the CLI. |

010403

| | |
|--------------------------|--|
| Message ID | 010403 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="Interface {port1 port2 ...} access methods has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the access methods of an interface using the CLI. |

| | |
|--------------------------|--|
| Message ID | 010403 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="interface {port1 port2 ...} status changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the access methods (or status) of an interface using the CLI. |

010404

| | |
|--------------------------|---|
| Message ID | 010404 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="interface {port1 port2 ...} status changed by user<user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the status of an interface using the CLI. |

010405

| | |
|--------------------------|---|
| Message ID | 010405 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="interface {port1 port2 ...} status changed by user<user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the status of an interface using the CLI. |

| | |
|--------------------------|--|
| Message ID | 010405 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| 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 CLI (console telnet ssh)" |
| Meaning | A user changed PPPoE settings using the CLI. |

| | |
|--------------------------|---|
| Message ID | 010405 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| 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 GUI(<ip_address>)" |
| Meaning | A user changed settings using the GUI. |

010406

| | |
|--------------------------|--|
| Message ID | 010406 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="Management IP has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the management IP using the CLI. |

010409

| | |
|--------------------------|--------------|
| Message ID | 010409 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|-------------------|--|
| Message ID | 010409 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="Interface {port1 port2 ...} access methods has been changed by user <user name> via GUI (<ip_address>)" |
| Meaning | A user changed access methods on an interface using the web-based manager. |

010410

| | |
|--------------------------|---|
| Message ID | 010410 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="MTU has been enabled for interface {port1 port2 ...} by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user enabled MTU for an interface using the web-based manager. |

| | |
|--------------------------|--|
| Message ID | 010410 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="MTU has been disabled for interface{ port1 port2 ...} by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user changed MTU to disabled for an interface using the web-based manager. |

010414

| | |
|--------------------------|--|
| Message ID | 010414 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="Interface {port1 port2 ...} has been brought up by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user changed an interface to up using the web-based manager. |

010415

| | |
|--------------------------|--------------|
| Message ID | 010415 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|-------------------|---|
| Message ID | 010415 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="Addressing mode of interface {port1 port2 ...} access methods has been changed by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user changed the access methods of an interface's addressing mode using the web-based manager. |

010416

| | |
|--------------------------|--|
| Message ID | 010416 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="Connect option of interface {port1 port2 ...} access methods has been changed by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user changed the access methods of a connect option for an interface using the web-based manager. |

010601

| | |
|--------------------------|--|
| Message ID | 010601 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=dns msg="DNS has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed DNS settings using the CLI. |

010602

| | |
|--------------------------|---|
| Message ID | 010602 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=dns msg="DNS has been changed to <primary_dns> and <secondary_dns> by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed the primary DNS and secondary DNS using the web-based manager. |

010702

| | |
|--------------------------|--------------|
| Message ID | 010702 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |

| | |
|-------------------|--|
| Message ID | 010702 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=routing msg="default gateway has been changed to <gateway_ip_address> by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed the default gateway IP address using the web-based manager. |

010703

| | |
|--------------------------|--|
| Message ID | 010703 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=routing msg="Route entry <number> has been deleted by user<user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted a route entry using the CLI. |

| | |
|--------------------------|--|
| Message ID | 010703 |
| Log Type | Event-Config log |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=routing msg="Route entry <number> has been deleted by user<user_name> via GUI (<ip_address>)" |
| Meaning | A user deleted a route entry using the web-based manager. |

010705

| | |
|--------------------------|--|
| Message ID | 010705 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=routing msg="A route to <destination_ip_address>/<destination_netmask> has been added by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user added a route with destination IP address/netmask using the CLI. |

| | |
|--------------------------|--|
| Message ID | 010705 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=routing msg="A route to <destination_ip_address>/<destination_netmask> has been added by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user added a route with destination address/netmask using either the CLI or web-based manager. |

010706

| | |
|--------------------------|---|
| Message ID | 010706 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=routing msg="Routing entry <number> has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed a routing entry using the CLI. |

| | |
|--------------------------|---|
| Message ID | 010706 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=routing msg="Routing entry <number> has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed a routing entry using the CLI or web-based manager. |

010901

| | |
|--------------------------|---|
| Message ID | 010901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=time msg="System timezone has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the system timezone using the CLI. |

| | |
|--------------------------|---|
| Message ID | 010901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=time msg="System timezone has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed the system time zone using the web-based manager. |

| | |
|--------------------------|--|
| Message ID | 010901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=time msg="Automatically adjust clock for Daylight Saving time has been changed by user<user_name> via GUI (<ip_address>)" |
| Meaning | A user changed the option automatically adjust clock for daylight saving time using the web-based manager. |

010902

| | |
|--------------------------|--|
| Message ID | 010902 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip-address>)} module=system submodule=time msg="NTP server settings have been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed NTP server settings using the CLI. |

| | |
|--------------------------|---|
| Message ID | 010902 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=time msg="NTP sever settings have been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed NTP server settings using the web-based manager. |

010904

| | |
|--------------------------|---|
| Message ID | 010904 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=time msg="System time has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the system time using the CLI. |

| | |
|--------------------------|---|
| Message ID | 010904 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=time msg="System timezone has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed the system time zone using the web-based manager. |

011001

| | |
|--------------------------|------------------|
| Message ID | 011001 |
| Log Type | Event-Config log |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|-------------------|--|
| Message ID | 011001 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="Console pageNo setting has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the console pageNo setting using the CLI. |

011002

| | |
|--------------------------|---|
| Message ID | 011002 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="Console mode setting has been changed to line mode by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the console mode setting to line mode using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011002 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="Console mode setting has been changed to batch by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the console mode setting to batch using the CLI. |

011003

| | |
|--------------------------|--|
| Message ID | 011003 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip-address>) telnet(<ip_address>)} module=system submodule=option msg="Idle timeout value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the idle timeout value using the CLI. |

011004

| | |
|--------------------------|--|
| Message ID | 011004 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="Authentication timeout value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed authentication timeout value using the CLI. |

011005

| | |
|--------------------------|--|
| Message ID | 011005 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="System language has been changed to {en ja ko ch tra} by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the system language to another language using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011005 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="System language has been changed to {en ja ko ch tra} by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed the system language to another language using the CLI or web-based manager. |

011006

| | |
|--------------------------|--|
| Message ID | 011006 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="LCD PIN number has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the LCD PIN number using the CLI or web-based manager. |

| | |
|--------------------------|--|
| Message ID | 011006 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip-address>)} module=system submodule=option msg="LCD PIN number has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed the LCD PIN number using the CLI or web-based manager. |

011007

| | |
|--------------------------|--------------|
| Message ID | 011007 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|--------------------------|---|
| Message ID | 011007 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="LCD PIN protection has been {enable disable} by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed LCD PIN protection enabled or disabled using the CLI. |
| Message ID | 011007 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="LCD PIN number has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed LCD PIN number using the web-based manager. |

011008

| | |
|--------------------------|---|
| Message ID | 011007 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="GUI refresh interval set to <interval> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed web-based manager refresh interval set to another interval using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011007 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="System idle and auth timeout has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed both system idle and auth timeout using the web-based manager. |

| | |
|--------------------------|--|
| Message ID | 011007 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=option msg="Auth timeout has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed auth timeout from the web-based manager. |

011101

| | |
|--------------------------|--|
| Message ID | 011001 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=admin msg="Admin <user_name> has been added by user <user_name> via CLI (console telnet ssh)" |
| Meaning | An admin user has added a user using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=admin msg="Admin <user_name> has been added by user <user_name> via GUI (<ip_address>)" |
| Meaning | An admin user added a user using the web-based manager. |

011102

| | |
|--------------------------|--|
| Message ID | 011102 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=admin msg="Admin <user_name> has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed an admin user using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011102 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=admin msg="Admin <user_name> has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed an admin user using the CLI or web-based manager. |

011103

| | |
|--------------------------|--------------|
| Message ID | 011103 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|-------------------|--|
| Message ID | 011103 |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=admin msg="Admin <user_name> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted an admin user using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011103 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=admin msg="Admin <user_name> has been deleted by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user deleted an admin user using the CLI or web-based manager. |

| | |
|--------------------------|---|
| Message ID | 011103 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=admin msg="admin <user_name> password has been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed an admin user's password using the web-based manager. |

011021

| | |
|--------------------------|--|
| Message ID | 011021 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=ha msg="HA settings have been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed HA settings using the CLI. |

011301

| | |
|--------------------------|---|
| Message ID | 011301 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP has been {enabled disabled} by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user enabled/disabled SNMP using the CLI. |

011303

- [A user changed SNMP config information using the CLI.](#)
- [A user changed SNMP CPU threshold value using the CLI.](#)

- A user changed the SNMP memory threshold value using the CLI.
- A user changed SNMP log disk threshold value using the CLI.
- A user changed the SNMP mail disk threshold value using the CLI.
- A user changed the SNMP deferred mqueue using the CLI.
- A user changed SNMP virus detection threshold value using the CLI.
- A user changed the SNMP Spam detection threshold value using the CLI.
- A user changed an SNMP community entry using the CLI.
- A user deleted an SNMP community entry and host using the CLI.

| | |
|--------------------------|--|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP config info changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed SNMP config information using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP CPU threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed SNMP CPU threshold value using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP Memory threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the SNMP memory threshold value using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP Logdisk threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed SNMP log disk threshold value using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP maildisk threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the SNMP mail disk threshold value using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP Deferred mqueue threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the SNMP deferred mqueue using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui=console SSH(<ip_address>) telnet(<ip_address>) module=system submodule=snmp msg="SNMP Virus detection threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed SNMP virus detection threshold value using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP Spam detection threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed the SNMP Spam detection threshold value using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP community entry <number> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed an SNMP community entry using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP community entry <entry_number> host <host_number> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted an SNMP community entry and host using the CLI. |

011901

- A user has changed a FortiMail disclaimer body for outgoing messages using the CLI.
- A user has changed a FortiMail disclaimer header for outgoing messages using the CLI.
- A user has changed a FortiMail disclaimer body for incoming messages using the CLI.
- A user has changed a FortiMail disclaimer header for incoming messages using the CLI.
- A user has modified local domains using the CLI.
- A user has modified a POP3 server using the CLI.
- A user has modified a relay server name using the CLI.
- A user has changed SNMP Memory threshold value using the CLI.
- A user has modified SMTP authentication using the CLI.
- A user has modified SMTP over SSL using the CLI.
- A user has modified SMTP server port number using the CLI.
- A user has modified the status of email archiving using the CLI.
- A user has modified the status of the email archiving account using the CLI.
- A user has modified an email archiving rotate setting using the CLI.
- A user has modified archiving settings on the local server using the CLI.
- A user has modified archiving settings on a remote server using the CLI.

- A user has modified an archiving policy using the CLI.
- A user has modified an archiving exempt setting using the CLI.
- A user has modified the system quarantine account using the CLI.
- A user has modified a system quarantine rotate setting using the CLI.
- A user has modified system quarantine quota settings using the CLI.
- A user has changed system quarantine settings using the web-based manager.
- A user has changed system quarantine settings using the CLI.
- A user has changed mail server settings using the CLI.
- A user has changed FortiMail appearance information using the CLI.
- A user has changed a FortiMail mail gateway user group using the CLI.
- A user has deleted a FortiMail mail gateway user group using the CLI.
- A user has modified to enable or disable SMTP over SSL using the CLI.
- A user changed mail server settings using the web-based manager.

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user name> ui=console SSH(<ip>) telnet(<ip>) module=system submodule=mailserver-setting msg="FortiMail disclaimer in body for outgoing messages has been changed by user <user name> via CLI (console telnet ssh)" |
| Meaning | A user has changed a FortiMail disclaimer body for outgoing messages using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="FortiMail disclaimer in header for outgoing messages has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed a FortiMail disclaimer header for outgoing messages using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="FortiMail disclaimer in body for incoming messages has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed a FortiMail disclaimer body for incoming messages using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="FortiMail disclaimer in header for incoming messages has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed a FortiMail disclaimer header for incoming messages using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Local domains has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified local domains using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="POP3 server port number has been modified to <port number> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified a POP3 server using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Relay server name has been modified to <server name> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified a relay server name using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=snmp msg="SNMP Memory threshold value has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed SNMP Memory threshold value using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="smtp auth has been modified to <auth_profile_name> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified SMTP authentication using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="smtp over ssl has been modified to {enabled disabled} by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified SMTP over SSL using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui=console SSH(<ip_address>) telnet(<ip_address>) module=system submodule=mailserver-setting msg="SMTP server port number has been modified to <port_number> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified SMTP server port number using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="status of email archiving has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified the status of email archiving using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="email archiving account has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified the status of the email archiving account using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="email archiving rotate setting has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified an email archiving rotate setting using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Archiving settings on local server has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified archiving settings on the local server using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Archiving settings on remote server has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified archiving settings on a remote server using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Archiving policy has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified an archiving policy using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Archiving exempt has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified an archiving exempt setting using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="system quarantine account has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified the system quarantine account using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="system quarantine rotate setting has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified a system quarantine rotate setting using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="System quarantine quota settings on local server has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified system quarantine quota settings using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="System quarantine settings have been changed by user <use_name> via GUI (<ip_address>)" |
| Meaning | A user has changed system quarantine settings using the web-based manager. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="System quarantine settings have been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed system quarantine settings using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Mail Server settings have been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed mail server settings using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="FortiMail appearance information has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed FortiMail appearance information using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="FortiMail mail gw user group has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has changed a FortiMail mail gateway user group using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="FortiMail mail gw user group has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has deleted a FortiMail mail gateway user group using the CLI. |

| | |
|--------------------------|--|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="smtp over ssl has been modified to {enable disable} by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user has modified to enable or disable SMTP over SSL using the CLI. |

| | |
|--------------------------|---|
| Message ID | 011901 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-setting msg="Mail Server settings have been changed by user<user_name> via GUI(<ip_address>)" |
| Meaning | A user changed mail server settings using the web-based manager. |

012001

| | |
|--------------------------|---|
| Message ID | 012001 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-access msg="Permission of mail from <email_address> is set to {OK REJECT RELAY DISCARD} by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user set permission of mail using the CLI. |

| | |
|--------------------------|--------------|
| Message ID | 012001 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|-------------------|--|
| Message ID | 012001 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mailserver-access msg="Permission of mail from <email_address> is deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted permission of mail using the CLI. |

| | |
|--------------------------|---|
| Message ID | 012001 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui=GUI(<ip_address>) module=system submodule=mailserver-access msg="Permission of mail from <email_address> is set to {OK REJECT RELAY DISCARD} by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user set the permission of mail from a specified email address using the web-based manager. |

| | |
|--------------------------|--|
| Message ID | 012001 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui=GUI(<ip_address>) module=system submodule=mailserver-access msg="Mail server access <string> is deleted by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user deleted mail server access using the web-based manager. |

012101

| | |
|--------------------------|---|
| Message ID | 012101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=unknown msg="local domain <domain_name> is deleted by user <user_name> via CLI (console telnet ssh)" |
| Message | A user deleted a local domain using the CLI. |

| | |
|--------------------------|--|
| Message ID | 012101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=unknown msg="Local domain name <domain_name> is added by user <user_name> via CLI (console telnet ssh)" |
| Message | A user added a local domain using the CLI. |

| | |
|--------------------------|--------------|
| Message ID | 012101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |

| | |
|-------------------|---|
| Message ID | 012101 |
| Severity | Information |
| Message | user=<user_name> ui=GUI(<ip_address>) module=system submodule=mailserver-access msg="Permission of mail from <email_address> is set to {OK REJECT RELAY DISCARD} by user <user_name> via GUI(<ip_address>)" |
| Message | A user set permission of mail using the web-based manager. |

| | |
|--------------------------|--|
| Message ID | 012101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui=GUI(<ip_address>) module=system submodule=unknown msg="Local domain name <domain_name> is added by user <user_name> via GUI(<ip_address>)" |
| Message | A user added a local domain using the web-based manager. |

030101

| | |
|--------------------------|---|
| Message ID | 030101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=local msg="Local user <user_name> has been added by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user added a local user using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui=GUI(<ip_address>) module=system submodule=unknown msg="Local domain name <domain_name> is added by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user added a local domain name using the web-based manager. |

030102

| | |
|--------------------------|--|
| Message ID | 030102 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=local msg="Local user <user_name> has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified a local user using the CLI. |

030103

| | |
|--------------------------|---|
| Message ID | 030103 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=local msg="Local user <user_name> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted a local user using the CLI. |

030302

| | |
|--------------------------|---|
| Message ID | 030302 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="User group <group_name> has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified a user group using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030302 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=interface msg="User group <group_name> has been modified by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user modified a user group using the CLI or web-based manager. |

030303

| | |
|--------------------------|--|
| Message ID | 030303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui=console SSH(<ip_address>) telnet(<ip_address>) module=system submodule=group msg="User group <group_name> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted a user group using the CLI. |

| | |
|--------------------------|---|
| Message ID | 030303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=group msg="User group <group_name> has been deleted by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user deleted a user group using the web-based manager. |

030501

- A user added a mail user using the CLI.
- A user added a specified mail server user using the CLI.
- A user sets a mail server user with information using the CLI.
- A user added a mail server user with information using the web-based manager.
- A user sets a mail server user with information using the web-based manager.
- A user deletes a mail server user using the web-based manager.

| | |
|--------------------------|--|
| Message ID | 030501 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="mail user <user_address> has been added by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user added a mail user using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030501 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="Mail server user <email_address> is added with information: displayname <display_name> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user added a specified mail server user using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030501 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="Mail server user <email_address> is set with information: displayname <display_name> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user sets a mail server user with information using the CLI. |

| | |
|--------------------------|---|
| Message ID | 030501 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="Mail server user <email_address> is added with information: displayname <display_name> by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user added a mail server user with information using the web-based manager. |

| | |
|--------------------------|--|
| Message ID | 030501 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="Mail server user <email_address> is set with information: displayname <display_name> by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user sets a mail server user with information using the web-based manager. |

| | |
|--------------------------|---|
| Message ID | 030501 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="Mail Server User <email_address> is deleted by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user deletes a mail server user using the web-based manager. |

030502

- A user modified the disk quota of the email archiving account using the CLI.
- A user modified the email archiving account password using the CLI.
- A user modified the forwarding address for email archiving using the CLI.
- A user modified the system quarantine account password using the CLI.
- A user modified the system quarantine forwarding address using the CLI.
- A user modified the password of a mail user using the CLI.
- A user modified the display name of a specific mail user using the CLI.

| | |
|--------------------------|--|
| Message ID | 030502 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="disk quota of email archiving account has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified the disk quota of the email archiving account using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030502 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="password of email archiving account has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified the email archiving account password using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030502 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="forwarding address for email archiving has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified the forwarding address for email archiving using the CLI. |

| | |
|--------------------------|---|
| Message ID | 030502 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="password of system quarantine account has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified the system quarantine account password using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030502 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="forwarding address for system quarantine has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified the system quarantine forwarding address using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030502 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="password of mail user <user_email_address> has been modified by user <user name> via CLI (console telnet ssh)" |
| Meaning | A user modified the password of a mail user using the CLI. |

| | |
|--------------------------|--|
| Message ID | 030502 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="display name of mail user <user_address> has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified the display name of a specific mail user using the CLI. |

030503

| | |
|--------------------------|--|
| Message ID | 030503 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=mail msg="mail user <user_email_address> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted a mail user using the CLI. |

030601

| | |
|--------------------------|--------------|
| Message ID | 030601 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|-------------------|--|
| Message ID | 030601 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=alias msg="User alias <alias_name> has been added by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user added a user alias using the web-based manager. |

030602

| | |
|--------------------------|---|
| Message ID | 030602 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=alias msg="User alias <alias_name> has been modified by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user modified a user alias using the web-based manager. |

030603

| | |
|--------------------------|--|
| Message ID | 030603 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=alias msg="User alias <alias_name> has been deleted by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user deleted a user alias using the web-based manager. |

030701

| | |
|--------------------------|---|
| Message ID | 030701 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=pop3 msg="POP3 auth profile <profile_name> has been added by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user added a POP3 auth profile using the CLI. |

030702

| | |
|--------------------------|--------------|
| Message ID | 030702 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |

| | |
|-------------------|--|
| Message ID | 030702 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=pop3 msg="POP3 auth profile <profile_name> has been renamed to <new_profile_name> by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user renamed a POP3 auth profile using the CLI. |

| | |
|--------------------------|---|
| Message ID | 030702 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=pop3 msg="POP3 auth profile <profile_name> has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified a POP3 auth profile using the CLI. |

030703

| | |
|--------------------------|--|
| Message ID | 030703 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=pop3 msg="POP3 auth profile <profile_name> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted a POP3 auth profile using the CLI. |

030801

| | |
|--------------------------|--|
| Message ID | 030801 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=system submodule=imap msg="IMAP auth profile <profile_name> has been added by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user added an IMAP auth profile using the CLI. |

030802

| | |
|--------------------------|---|
| Message ID | 030802 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=user submodule=imap msg="IMAP auth profile <profile_name> has been modified by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user modified an IMAP auth profile using the CLI. |

030803

| | |
|--------------------------|--|
| Message ID | 030803 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=user submodule=imap msg="IMAP auth profile <profile_name> has been deleted by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user deleted an IMAP auth profile using the CLI. |

030902

| | |
|--------------------------|--|
| Message ID | 030902 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=emailfilter submodule=bword msg="email banned word was removed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user removed an email banned word using the CLI. |

090101

| | |
|--------------------------|--|
| Message ID | 090101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=logsetting msg="Local log setting has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed a local log setting using the CLI. |

| | |
|--------------------------|---|
| Message ID | 090101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=logsetting msg="Memory logsetting has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed memory log setting using the CLI. |

| | |
|--------------------------|---|
| Message ID | 090101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=logsetting msg="Log setting has been changed by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user changed a log setting using the CLI. |

| | |
|--------------------------|---|
| Message ID | 090101 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=logsetting msg="Log setting has been changed by user <user name> via GUI (<ip_address>)" |
| Meaning | A user changed a log setting using the web-based manager. |

090112

| | |
|--------------------------|--|
| Message ID | 090112 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=logsetting msg="Log setting elog has been cleared by user <user_name> via CLI (console telnet ssh)" |
| Meaning | A user cleared elog using the CLI. |

| | |
|--------------------------|--|
| Message ID | 090112 |
| Log Type | Event-Config |
| FortiMail version | 3.0(MR3 and up) |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=logsetting msg="Log Policy has been modified by user admin via GUI(<ip_address>)" |
| Meaning | The user, admin, has edited a log policy from a specified IP address. |

090301

| | |
|--------------------------|---|
| Message ID | 090301 |
| Log Type | Event-Config log |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=alertemail msg="Alertemail setting has been changed by user admin via CLI (console telnet ssh)" |
| Meaning | An admin user changed the alert email setting using the CLI. |

090302

| | |
|--------------------------|--|
| Message ID | 090302 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=alertemail 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 | A user changed the alertemail SMTP server to and a user was changed using the web-based manager. |

090303

| | |
|--------------------------|--|
| Message ID | 090303 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=alertemail msg="Alertemail target email addresses been changed by user <user_name> via GUI (<ip_address>)" |
| Meaning | A user changed alert email target email addresses using the web-based manager. |

090305

| | |
|--------------------------|---|
| Message ID | 090305 |
| Log Type | Event-Config |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} module=log submodule=alertemail msg="Alertemail configuration has been modified by user <user_name> via GUI(<ip_address>)" |
| Meaning | A user modified alert email configuration using the web-based manager. |

Event-System logs

Event-System log messages are a subcategory of event logs and are identified by 06, or 0106. There are different event-system log messages and each are identified by the message identification numbers, for example, 000003.

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.

Example

In this example, an admin user successfully updated the virus and IDS database from the web-based manager.

```
2008-10-10 09:11:31 log_id=0106000013 log_part=00 type=event subtype=system
pri=warning user=admin ui=GUI(172.20.130.27) action=update status=success
msg="Virus and IDS database has been updated successfully by user admin via
GUI(172.20.130.27)"
```



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.

The Event-System logs contains the following messages, listed by message IDs:

000000
000001
000002
000003
000005
000007
000008

000000

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log Type | Event-System |
| FortiMail version | 3.0(MR3 and up) |
| Severity | Warning |
| Message | user=DNS ui=DNS action=unknown status=success msg= "DNS: Connection timed out. No servers could be reached." |
| Meaning | The user could not reach any DNS servers before a time out occurred. |

| | |
|--------------------------|-----------------|
| Message ID | 000000 |
| Log Type | Event-System |
| FortiMail version | 3.0(MR4 and up) |

| | |
|-------------------|---|
| Message ID | 000000 |
| Severity | Information |
| Message | user=DNS ui=DNS action=unknown status=success msg= "DNS: External server:[<ip_address>], [netmask_address], private ip query: [enabled], dns cache: [enabled]." |
| Meaning | |

000001

| | |
|--------------------------|--|
| Message ID | 000001 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=reboot status=none msg="System has been restarted by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user restarted the system using the CLI or web-based manager. |

000002

| | |
|--------------------------|---|
| Message ID | 000002 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=<user_name> ui=console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>) action=shutdown status=none msg="System has been shutdown by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user shutdown the system using the CLI or web-based manager. |

000003

| | |
|--------------------------|--|
| Message ID | 000003 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>) action=reload status=none msg="System has been reloaded by user <user_name> via {console SSH(<ip_address>) telnet (<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user reloaded the system using the CLI or web-based manager. |

000005

| | |
|--------------------------|--------------|
| Message ID | 000005 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |

| | |
|-------------------|---|
| Message ID | 000005 |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=factory_reset status=none msg="System has been reset to factory default by user <user_name> via {console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user reset the system to factory default using the CLI or web-based manager. |

| | |
|--------------------------|---|
| Message ID | 000005 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Messages | user=LCD ui=LCD action=factory_reset status=none msg="System has been reset to factory default by user LCD via LCD" |
| Meaning | The system was reset by LCD (user) using the LCD. |

000007

| | |
|--------------------------|---|
| Message ID | 000007 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=update status=none msg="System firmware has been upgraded by user <user_name> via {console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user upgraded/downgraded system firmware using the CLI or web-based manager. |

| | |
|--------------------------|--|
| Message ID | 000007 |
| Log Type | Event-System |
| Severity | Warning |
| FortiMail version | 3.0 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=update status=none msg="System firmware has been downgrade by user <user_name> via {console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user downgraded system firmware using the console, telnet, or web-based manager. |

| | |
|--------------------------|---|
| Message ID | 000007 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=update status=failure msg="Upgrade system firmware failed by user <user_name> via {console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user upgraded system firmware unsuccessfully using the CLI, console, telnet, or web-based manager. |

000008

- A user changed the mode to gateway mode using the CLI, web-based manager or LCD.
- A user changed the mode to server mode using the CLI, web-based manager or LCD.
- A user changed the mode to transparent mode using the CLI, web-based manager or LCD.
- An LCD user changed the mode to gateway mode using the LCD.
- An LCD user changed the mode to server mode using LCD.
- A user changed the mode to transparent mode using LCD.

| | |
|--------------------------|---|
| Message ID | 000008 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Messages | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=switch_mode status=success msg="System has been changed to gateway mode by user <user_name> via console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)" |
| Meaning | A user changed the mode to gateway mode using the CLI, web-based manager or LCD. |

| | |
|--------------------------|--|
| Message ID | 000008 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=swtich_mode status=success msg="System has been changed to server mode by user <user_name> via {console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)}" |
| Meaning | A user changed the mode to server mode using the CLI, web-based manager or LCD. |

| | |
|--------------------------|---|
| Message ID | 000008 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)} action=swtich_mode status=success msg="System has been changed to transparent mode by user <user_name> via console SSH(<ip_address>) telnet(<ip_address>) GUI(<ip_address>)" |
| Meaning | A user changed the mode to transparent mode using the CLI, web-based manager or LCD. |

| | |
|--------------------------|---|
| Message ID | 000008 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=LCD ui=LCD action=switch_mode status=success msg="System has been changed to gateway mode by user LCD via LCD" |
| Meaning | An LCD user changed the mode to gateway mode using the LCD. |

| | |
|--------------------------|---|
| Message ID | 000008 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=LCD ui=LCD action=factory_reset status=none msg="System has been changed to server mode by user LCD via LCD" |
| Meaning | An LCD user changed the mode to server mode using LCD. |

| | |
|--------------------------|--|
| Message ID | 000008 |
| Log Type | Event-System |
| FortiMail version | 3.0 |
| Severity | Warning |
| Message | user=LCD ui=LCD action=factory_reset status=none msg="System has been changed to transparent mode by user LCD via LCD" |
| Meaning | A user changed the mode to transparent mode using LCD. |

Event-Update logs

Event-Update log messages are a subtype category of the event log and are identified by the numbers 0110. Event-Update log messages contain information about the success or failure of an update of FortiGuard services, such as updating the virus database.

Example

```
2008-09-18 15:19:55 log_id=011000012 log_part=00 type=event
subtype=update pri=warning msg="Update result: virusdb:yes,
avengine:yes, spamdb:yes, asengine:yes"
```



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.

The Event-Update logs contain the following message, listed by the message ID:

000000

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log type | Event-Update |
| FortiMail version | 3.0(MR4) |
| 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-Admin logs

Event-Admin log messages are a subcategory of event logs and are identified by 04, or 0104. All Event-Admin log messages have the same log message identification number, 000001.

Event-Admin log messages inform you of administration changes made to your FortiMail unit.

Example

In this example, an admin user successfully logs into the web-based manager.

```
2008-09-10 10:12:01 log_id=0104000001 log_part=00 type=event subtype=admin
pri=information user=admin ui=GUI(10.10.10.4) action=login status=success
reason=none msg="User admin login successfully from GUI(10.10.10.4)
```



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.

The Event-Admin logs contain the following message, listed by the message ID:

000001

- A user successfully logged into the web-based manager.
- A user from a specified IP address logged into the WebMail.
- A user successfully logged in using the console, SSH, or telnet.
- A user failed to log in using the console, SSH, or telnet.
- The WebMail GUI cannot display the email message, or the quarantined message in the web-based manager.
- Specific information in a message cannot be retrieved.
- The message cannot be read from the mailbox.
- An unknown failure occurred when trying to prepare the attachment for a user to download.
- An LCD user successfully logged in using the LCD.
- An LCD user failed to log in using the LCD.

| | |
|--------------------------|--|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Messages | user=<user_name> ui=GUI(<ip_address>) action=login status=success reason=none msg="User <user_name> login successfully from GUI(<ip_address>)" |
| Meaning | A user successfully logged into the web-based manager. |

| | |
|--------------------------|-------------|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |

| | |
|-------------------|---|
| Message ID | 000001 |
| Message | user=<user_name> ui=WebMail action=login status=success reason=none msg="User <user_name> from <ip_address> logged in" |
| Meaning | A user from a specified IP address logged into the WebMail. |

| | |
|--------------------------|--|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=<user_name> ui={console SSH(<ip_address>) telnet(<ip_address>)} action=login status=success reason=none msg="User <user_name> login successfully from {console SSH(<ip_address>) telnet(<ip_address>)}" |
| Meaning | A user successfully logged in using the console, SSH, or telnet. |

| | |
|--------------------------|---|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=<user_name> ui=console SSH(<ip_address>) telnet(<ip_address>) action=login status=failure reason={passwd_invalid name_invalid ip_blocked timeout max_times} msg="User <user_name> login failed from {console SSH(<ip_address>) telnet(<ip_address>)}" |
| Meaning | A user failed to log in using the console, SSH, or telnet. |

| | |
|--------------------------|--|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=WebMail ui=WebMail action=login status=failure reason=none msg="mailbox_get_header: failed" |
| Meaning | The WebMail GUI cannot display the email message, or the quarantined message in the web-based manager. |

| | |
|--------------------------|---|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=WebMail ui=WebMail action=login status=failure reason=none msg="mailbox_get_num_parts: failed" |
| Meaning | Specific information in a message cannot be retrieved. |

| | |
|--------------------------|--|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=WebMail ui=WebMail action=login status=failure reason=none msg="Could not get message part" |
| Meaning | The message cannot be read from the mailbox. |

| | |
|--------------------------|---|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=WebMail ui=WebMail action=login status=failure reason=none msg="Could not save attachment" |
| Meaning | An unknown failure occurred when trying to prepare the attachment for a user to download. |

| | |
|--------------------------|---|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=LCD ui=LCD action=login status=success reason=none msg="Login from LCD successfully" |
| Meaning | An LCD user successfully logged in using the LCD. |

| | |
|--------------------------|---|
| Message ID | 000001 |
| Log Type | Event-Admin |
| Severity | Information |
| FortiMail version | 3.0 |
| Message | user=LCD ui=LCD action=login status=failure reason=none msg="Login from LCD failed" |
| Meaning | An LCD user failed to log in using the LCD. |

Event-SMTP logs

Event-SMTP log messages are a subcategory of event logs and are identified by 13, or 0113. All Event-SMTP log messages have the same message identification number, 000000.

Event-SMTP log messages inform you of any SMTP-related events that occur.

Example

In this example, an email on the SMTP server to recipient `user1` was delayed for five seconds and the sender is a local user.

```
2008-09-21 14:03:55 log_id=0113000000 log_part=00 type=event subtype=smt
pri=information user=mail ui=mail action=unknown status=success
msg="k9AGUoZT004116: to=user1@example.com, delay=00:00:05, mailer=local,
pri=0, dsn=5.1.1, stat=User unknown"
```



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.

The Event-SMTP logs contain the following message, listed by the message ID:

000000

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0 |
| Severity | All severity levels |
| Message | user=mail ui=mail action=unknown status=success msg="<log_message_information>" |
| Meaning | Any SMTP-related events. |

| | |
|--------------------------|---|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0 (MR2) |
| Severity | Information |
| Message | user=mail ui=mail action=unknown status=success 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. |

| | |
|--------------------------|------------------|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0 (MR3 and up) |
| Severity | Information |

| | |
|-------------------|---|
| Message ID | 000000 |
| Message | user=mail ui=mail action=NONE status=N/A session_id= " " 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. |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0(MR2 and up) |
| Severity | Notification |
| Message | user=mail ui=mail action=unknown status=success msg="*@*: alias database /var/spool/etc/mail/aliases has been rebuilt" |
| Meaning | |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0(MR2 and up) |
| Severity | Information |
| Message | user=mail ui=mail action=unknown status=success msg="Starting flgrptd" |
| Meaning | |

| | |
|--------------------------|---|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0(MR2) |
| Severity | Notification |
| Message | user=mail ui=mail action=unknown status=success msg="alias database /var/spool/etc.mail/aliases has been rebuilt" |
| Meaning | |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | user=mail ui=mail action=unknown status=success msg= "0 aliases, longest 0 bytes, 0 bytes total" |
| Meaning | |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log Type | Event-SMTP |
| FortiMail version | 3.0(MR2 and up) |
| Severity | Information |
| Message | user=mail ui=mail action=unknown status=success msg="Successfully loaded virus db: /var/spool/etc/virus" |
| Meaning | |

Event-POP3 logs

Event-POP3 log messages are a subcategory of event logs and are identified by the numbers 11, or 0111. All Event-POP3 log messages have the same message identification number, 000000.

Event-POP3 log messages inform you of any POP3-related events.

Example

The following is an example of an Event-POP3 log message.

```
2008-10-05 09:45:56 log_id=0111000000 log_part=00 type=event subtype=pop3
pri=information user=mail ui=mail action=unknown status=success
msg="accept=5; sockfd=4; clilen=16; cli_addr=172.31.130.26:33220\n"
```



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.

The Event-POP3 logs contain the following message, listed by the message ID:

000000

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log Type | Event-POP3 |
| FortiMail version | 3.0 |
| Severity | All severity levels |
| Message | user=mail ui=mail action=unknown status=success msg="<log_message_information>" |
| Meaning | Any POP3-related event. |

Event-IMAP logs

Event-IMAP log messages are a subcategory of event logs and are identified by the number 12, or 0112. All Event-IMAP log messages have the same message identification number, 000000.

Event-IMAP log messages inform you of any IMAP-related messages.

Example

In this example, a mail user successfully debugged a password for a particular email user.

```
2008-09-19 15:19:55 log_id=0112000000 log_part=00 type=event subtype=imap
pri=debug user=mail ui=mail action=unknown status=success
msg="fortimail_debug:valpwd:user=user1@example.com, passwd=*****"
```



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.

The Event-IMAP logs contain the following message, listed by the message ID:

000000

| | |
|--------------------------|---|
| Message ID | 000000 |
| Log type | Event-IMAP |
| FortiMail version | 3.0 |
| Severity | All severity levels |
| Message | user=mail ui=mail action=unknown status=success msgs="<log_message_information>" |
| Meaning | Any IMAP-related events. |

Event-HA logs

Event-HA log messages are a subcategory of event logs and are identified by the number 07, or 0107. All Event-HA log messages have the same message identification number, 000000.

Event-HA log messages inform you of any high availability problems that may occur within a high availability cluster.

Example

In this example, a FortiMail unit is becoming the primary unit in a HA cluster.

```
2008-09-18 15:19:55 log_id=010700000 log_part=00 type=event subtype=ha
pri=information user=ha ui=ha action=unknown status=success msg="monitord:
main loop starting, entering MASTER mode"
```



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.

The Event-HA logs contain the following message, listed by the message ID:

000000

| | |
|--------------------------|---|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success msgs="monitord: main loop starting, entering MASTER mode" |
| Meaning | The FortiMail unit is entering primary mode. |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success msgs="configd: main loop starting, entering master mode" |
| Meaning | |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success msgs="monitord: starting pre-able" |
| Meaning | |

| | |
|--------------------------|---|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success msgs="configd: main loop starting, entering slave mode" |
| Meaning | The FortiMail unit is entering subordinate mode. |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success msgs="configd: main loop stopping" |
| Meaning | |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success msgs="backupd: main loop starting, entering master mode" |
| Meaning | |

| | |
|--------------------------|--|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success msgs="backupd: main loop stopping" |
| Meaning | |

| | |
|--------------------------|---|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |
| Message | user=ha ui=ha action=unknown status=success 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. |

| | |
|--------------------------|-------------|
| Message ID | 000000 |
| Log type | Event-HA |
| FortiMail version | 3.0(MR4) |
| Severity | Information |

| | |
|-------------------|---|
| Message ID | 000000 |
| Message | user=ha ui=ha action=unknown status=success msgs="monitord: main loop starting, entering MASTER mode" |
| Meaning | |

Anti-virus logs

Anti-virus log messages are identified with the numbers 02 and have a subcategory called virus detect with a message identification number, 00, or 0200. Anti-virus log messages inform you of viruses that your FortiMail unit detected.

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.

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.

The anti-virus logs contain the following message, listed by the message ID:

060101

| | |
|--------------------------|--|
| Message ID | 060101 |
| Log Type | Anti-virus |
| FortiMail version | 3.0 |
| Severity | All severity levels. |
| Message | from="<sender_email_address>" to="<recipient_email_address>" msg="The file name is infected with <virus_name>" |
| Meaning | The file contains the specified virus. |

Anti-spam logs

Anti-spam log messages are identified with numbers 05 and have a subcategory called spam detect, which is identified by the message identification number 080300, or 0501080300. Anti-spam log messages notify you of any spammed email.

The FortiMail Anti-spam 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.

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.

The anti-spam logs contain the following log message, listed by the message ID:

080300

| | |
|--------------------------|--|
| Message ID | 080300 |
| Log Type | Spam, Detected |
| FortiMail version | 3.0 |
| Severity | Information |
| Message | session_id="<identification_number>" from="<sender_email_address>" to="<recipient_email_address>" msg="<log_message_information>" session_id="<identification_number>" from="<sender_email_address>" client_name="<resolved_client_name>" to="<recipient_email_address>" msg="<log_message_information>" |
| Meaning | Any spam-related events. |

Anti-spam log message with no message ID

The following log message table contains no message identification number because the log message can have a different message identification number every time the FortiMail unit records this particular log message.

| | |
|--------------------------|-----------------|
| Log Type | Spam, Detected |
| FortiMail version | 3.0(MR3 and up) |
| Severity | Notification |

| | |
|----------------|--|
| Message | session_id="<identification_number>" from="<sender_email_address>" to="<recipient_email_address>" msg="Deep Header Scanner Rules Reload - Finished." |
| Meaning | Rule loading has been completed. |

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com