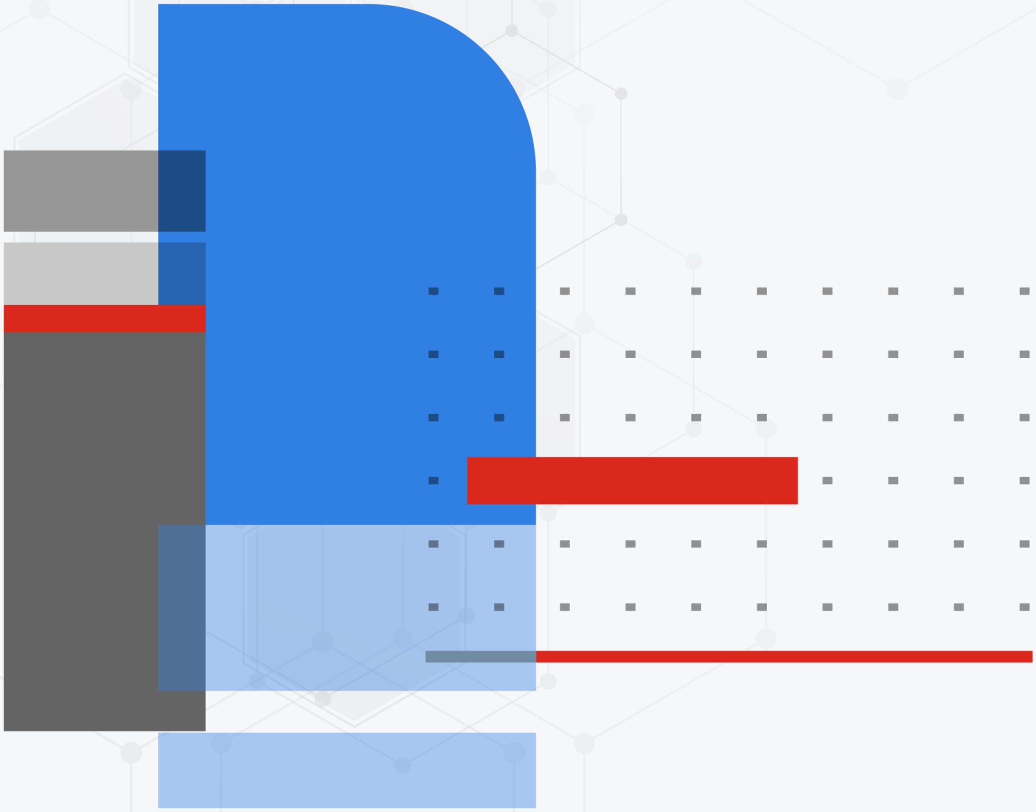
Log Reference

FortiMail 7.2.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

June 12, 2023
FortiMail 7.2.0 Log Reference
00-720-000000-20230612

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-05-17	Initial release.
2022-01-21	Added a note to system event log section.
2023-06-08	Added MS365 log fields to history logs.

About Fortinet logs

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

For information about configuring logging in FortiMail, see the FortiMail Administration Guide.

This section provides information on the following topics:

- Accessing FortiMail log messages
- Log message syntax
- Log types
- Subtypes
- Severity/Priority levels
- Log message cross search

Accessing FortiMail log messages

There are several ways you can access FortiMail log messages:

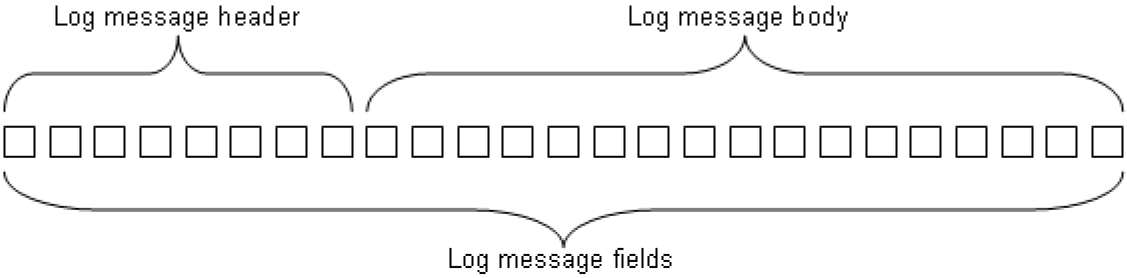
- On the FortiMail web UI, you can view log messages by going to *Monitor* > *Log*. From here you can download log messages to your local PC by clicking *Export* and view them later. For details, see the FortiMail Administration Guide.
- Go to *Log & Report* > *Log Setting* > *Remote* and add a FortiAnalyzer unit as a remote host in order to send log messages to FortiAnalyzer. You can send log messages to any Syslog server from here.

Log message syntax

All FortiMail log messages are comprised of a log header and a log body.

- **Header** — Contains the time and date the log originated, a log identifier, the type of log, the severity level (priority) and where the log message originated.
- **Body** — Describes the reason why the log was created, plus any actions that the FortiMail appliance took to respond to it. **These fields may vary by log type.**

Log message header and body



For example, in the following event log, the bold section is the header and the italic section is the body.

```
date=2012-08-17 time=12:26:41 device_id=FE100C3909600504 log_id=0001001623
type=kevent subtype=admin pri=information user=admin ui=GUI(172.20.120.26)
action=login status=success reason=none msg="User admin login successfully from GUI
(172.20.120.26)"
```

Device ID field

Depending on where you view log messages, log formats may vary slightly. For example, if you view logs on the FortiMail web UI or download them to your local PC, the log messages do not contain the device ID field. If you send the logs to FortiAnalyzer or other Syslog servers, the device ID field will be added.

Endpoint field

Starting from 4.0 MR3, a field called `endpoint` was added to the history and antispam logs. This field displays the endpoint's subscriber ID, MSISDN, login ID, or other identifiers. This field is empty if the sender IP is not matched to any endpoint identifier or if the endpoint reputation is not enabled in the session profiles.

Log_part field

For FortiMail 3.0 MR3 and up, the log header of some log messages may include an extra field, `log_part`, which provides numbered identification (such as 00, 01, and 02) when a log message has been split. Log splitting occurs in FortiMail 3.0 MR3 and up because the log message length was reduced.

Hex numbers in history logs

If you view the log messages on the FortiMail web UI or send the logs to a Syslog server, the dispositions and classifiers are displayed in English terms. However, if you download log files from FortiMail web UI to your PC and open them, the dispositions and classifiers are displayed in hex numbers. For explanation of these numbers, see the Log message dispositions and classifiers on page 17.

Log types

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

FortiMail logs are divided into the following types:

Log Types	Default File Name	Description
History (statistics)	alog	Records all email traffic going through the FortiMail unit.
System Event (kevent)	klog	Records system management activities, including changes to the system configuration as well as administrator and user log in and log outs.
Mail Event (event)	elog	Records mail activities.
Antispam (spam)	slog	Records spam detection events.
Antivirus (virus)	vlog	Records virus intrusion events.
Encryption (encrypt)	nlog	Records detection of IBE-related events.

Email related logs contain a session identification (ID) number, which is located in the session ID field of the log message. The session ID corresponds to all the relevant log types so that the administrator can get all the information about the event or activity that occurred on their network.

History/statistics logs

History logs are used to quickly determine the disposition of a message. History logs describe what action was taken by the FortiMail unit. Administrators use the history logs to quickly determine the status of a message for a specific recipient, then either right-click that log message and select *Cross Search,* or click the *Session ID* link. (See Log message cross search on page 14). All correlating history, event, antivirus and antispam log messages appear in a new tab where you can find out why that particular action was taken.

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

```
date=2012-07-16 time=12:22:56 device_id=FE100C3909600504 log_id=0200001075
type=statistics pri=information session_id="q6GJMuPu003642-q6GJMuPv003642" client_
name="[172.20.140.94]" dst_ip="172.20.140.92" endpoint="" from="user@external.lab"
to="user5@external.lab" subject="" mailer="mta" resolved="OK" direction="in"
```

```
virus="" disposition="Reject" classifier="Recipient Verification" message_
length="188"
```

From the disposition, “Reject”, we know that the FortiMail unit rejected the email message. We then do a session ID cross search to find it within the antispam logs, as in the following:

```
date=2012-07-16 time=12:22:56 device_id=FE100C3909600504 log_id=0300001075
type=spam pri=information session_id="q6GJMuPu003642-q6GJMuPv003642" client_name="
[172.20.140.94]" dst_ip="172.20.140.92" endpoint="" from="user@external.lab"
to="user5@external.lab" subject="" msg="<user5@external.lab>... User unknown"
```

In the above antispam log message, we now know why the FortiMail unit rejected the message because the message failed the recipient verification (User unknown), which is shown in the message field.

System event logs

Kevent 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. For example, “2020-05-22 00:04:28.565 log_id=0704025033 type=kevent subtype=update pri=information msg="Loaded avdb 77.01588(05/21/0020 22:38) using av engine 6.147."

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

Mail event logs

Event logs contain all the SMTP, POP3, IMAP, and webmail activities.

This log type records the metadata of the email messages handled by the FortiMail unit.

Antispam logs

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

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

Antivirus logs

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

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

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

Encryption logs

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

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

Subtypes

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

Log Type	Subtype
kevent	admin config dns ha system update
event	imap pop3 smtp webmail
virus	infected malware-outbreak file-signature
spam	default admin user
statistics	(no subtype)
encrypt	(no subtype)

Severity/Priority 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.

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

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

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

Log message cross search

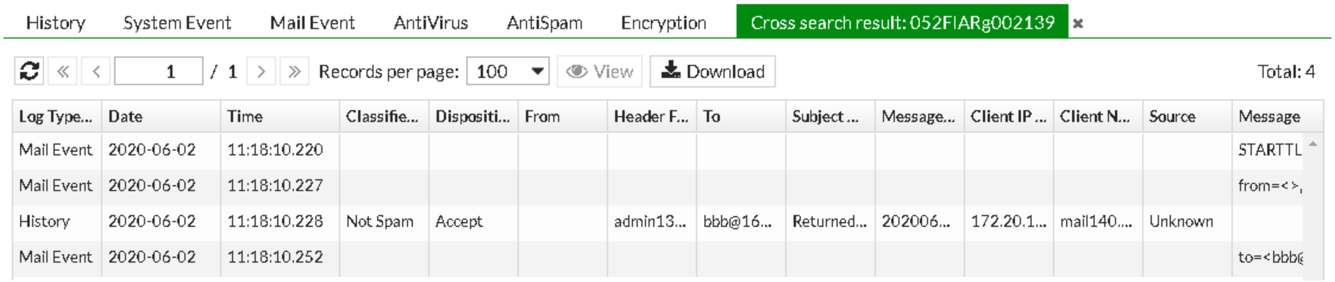
Since different types of log files record different events/activities, the same SMTP session (with one or more email messages sent during the session) or the same email message may be logged in different types of log files. For example, if the FortiMail units detects a virus in an email messages, this event will be logged in the following types of log files:

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

To find and display all log messages triggered by the same SMTP session or the same email message, you can use the cross-search feature.

The cross-search searches log files recorded five minutes before and after the log entry (this design is for performance purpose). Therefore, the search may cover multiple log files but may not cover all the related log files if any log files are recorded out of the ten minutes interval.

To do a cross-search of the log messages



Log Type...	Date	Time	Classifie...	Dispositi...	From	Header F...	To	Subject ...	Message...	Client IP ...	Client N...	Source	Message
Mail Event	2020-06-02	11:18:10.220											STARTTL
Mail Event	2020-06-02	11:18:10.227											from=<>,
History	2020-06-02	11:18:10.228	Not Spam	Accept		admin13...	bbb@16...	Returned...	202006...	172.20.1...	mail140....	Unknown	
Mail Event	2020-06-02	11:18:10.252											to=<bbb@

1. Go to *Monitor* > *Log*.
2. When viewing a log message with a **Session ID** (any tab except *System Event*), right-click the log message. From the pop-up menu, select:
   - Cross Search (Session) to search for the log messages triggered by the same SMTP session. This may result in multiple email messages if multiple messages were sent in the same SMTP session.
   - Cross Search (Message) to search for the log messages triggered by the same email message.

   You can also click the session ID of the log message to search for the log messages triggered by the same SMTP session. This is equivalent to the Cross Search (Session) pop-up menu.

   All correlating history, event, antivirus and antispam log messages will appear in a new tab.

History/Statistics logs

This chapter contains information regarding history, or statistics log messages. History log messages record all mail traffic going through the FortiMail unit.

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

For more information about log message cross search, see Log message cross search on page 14.

Example

If you export the FortiMail log messages to a remote Syslog server (including FortiAnalyzer), a history/statistics log will look like the following:

```
date=2013-02-25 time=07:01:34 device_id=FE100C3909600504 log_
id=0200025843 type=statistics pri=information session_
id="r1PF1YTh025836-r1PF1YTh025836" client_name="172.20.140.108"
dst_ip="172.20.140.13" endpoint="" from="aaa@bbb.com"
to="user1@example.com" polid="0:1:0" domain="" subject=""
mailer="proxy" transfer_time="" scan_time="" resolved=""
direction="unknown" virus="" disposition="0x200" classifier="0x17"
message_length="199986"
```

For the Microsoft 365 view, the following MS365-specific log fields will be added:

```
read_status="read (or unread)" folder="(user email inbox folder)" received_time=""
notification_delay=""
```

Policy ID and domain fields

Starting from v5.0 release, two new fields — policy ID and domain — have been added to history logs.

The policy ID is in the format of x:y:z, where:

- x is the ID of the global access control policy.
- y is the ID of the IP-based policy.
- z is the ID of the recipient-based policy.

If the value of x, y, and z is 0, it means that no policy is matched.

If the matched recipient-based policy is incoming, the protected domain will be logged in the domain field.

If the matched recipient-based policy is outgoing, the domain field will be empty.

Log message dispositions and classifiers

Each history log contains one field called *Classifier* and another called *Disposition*.

The *Classifier* field displays which FortiMail scanner applies to the email message. For example, “Banned Word” means the email message was detected by the FortiMail banned word scanner. The *Disposition* field specifies the action taken by the FortiMail unit.

If you view the log messages on the FortiMail web UI or send the logs to a Syslog server, the dispositions and classifiers are displayed in English terms. However, if you download log files from the FortiMail web UI to your PC and open them, the dispositions and classifiers are displayed in hex numbers.

The following tables map the numbers with English terms.

When the classifier is “Attachment Filter”, a new field “atype” (attachment type) is also displayed. This field is for debug purpose only.

Classifiers

Hex number	Classifier	Hex Number	Classifier
0x00	Undefined	0x2A	Message Cryptography
0x01	User Safe	0x2B	Delivery Control
0x02	User Discard	0x2C	Encrypted Content
0x03	System Safe	0x2D	SPF Failure as Spam
0x04	System Discard	0x2E	Fragmented Email
0x05	RBL	0x2F	Email Contains Image
0x06	SURBL	0x30	Content Requires Encryption
0x07	FortiGuard AntiSpam	0x31	FortiGuard AntiSpam Black IP
0x08	FortiGuard AntiSpam-Safe	0x32	Session Remote
0x09	Bayesian	0x33	FortiGuard Phishing
0x0A	Heuristic	0x34	AntiVirus
0x0B	Dictionary Scanner	0x35	Sender Address Rate Control
0x0C	Banned Word	0x36	SMTP Auth Failure
0x0D	Deep Header	0x37	Access Control List Reject
0x0E	Forged IP (before v5.2 release)	0x38	Access Control List Discard
0x0F	Quarantine Control	0x39	Access Control List Bypass
0x10	Tagged virus (before v4.3 release)	0x3A	FortiGuard Antispam Webfilter
0x11	Attachment Filter(see note above)	0x3B	Newsletter Suspicious

Hex number	Classifier	Hex Number	Classifier
0x12	Grey List	0x3C	TLS Streaming
0x13	Bypass Scan On Auth	0x3D	Policy Match
0x14	Disclaimer	0x3E	Dynamic Safe List
0x15	Defer Delivery	0x3F	Sender Verification
0x16	Session Domain	0x40	Behavior Analysis
0x17	Session Limits	0x41	FortiGuard Spam Outbreak
0x18	Session Safe	0x42	Newsletter
0x19	Session Block	0x43	DMARC
0x1A	Content Monitor and Filter	0x44	File Signature
0x1B	Content Monitor as Spam	0x45	Sandbox
0x1C	Attachment as Spam	0x46	Malware Outbreak
0x1D	Image Spam	0x47	DLP Filter
0x1E	Sender Reputation	0x48	DLP Treated as Spam
0x1F	Access Control List Relay Denied	0x49	DLP Requires Encryption
0x20	Safelist Word	0x4A	Access Control List Safe
0x21	Domain Safe	0x4B	Virus Outbreak
0x22	Domain Block	0x4C	FortiGuard Antispam Webfilter
0x23	SPF (not in use)	0x4D	Impersonation Analysis
0x24	Domain Key (not in use)	0x4E	Session Action
0x25	DKIM (not in use)	0x4F	SPF Sender Alignment
0x26	Recipient Verification	0x50	SPF Check
0x27	Bounce Verification	0x51	Sandbox URL
0x28	Endpoint Reputation	0x52	Sandbox No Result
0x29	SSL Profile Check	0x53	Content Modification
		0x54	DKIM Failure

When the classifier is “Attachment Filter”, a new field “atype” (attachment type) is also displayed. This field is for debug purpose only.

Dispositions

Hex number	Disposition	Hex Number	Disposition
0x00	Undefined	0x10000	Encrypt
0x01	Accept	0x20000	Decrypt
0x04	Reject	0x40000	Alternate Host
0x08	Add Header	0x80000	BCC
0x10	Modify Subject	0x100000	Archive
0x20	Quarantine	0x200000	Customized repackage
0x40	Insert Disclaimer	0x400000	Repackage
0x80	Block	0x800000	Notification
0x100	Replace	0x1000000	Sign
0x200	Delay	0x2000000	Defer
0x400	Forward	0x4000000	HTML to Text
0x800	Disclaimer Body	0x8000000	Sanitize HTML
0x1000	Disclaimer Header	0x10000000	Remove URLs
0x2000	Defer	0x20000000	Deliver to Original Host
0x4000	Quarantine to Review	0x40000000	Content Reconstruction
0x8000	Treat as Spam	0x80000000	URL Click Protection
		0x100000000	Domain Quarantine

The disposition field in a log message may contain one or more dispositions/actions.

DNS resolution result field

Each history log contains one field called *Resolved,* which displays the DNS lookup results of the recipient domain.

This field may contain the following values:

- **OK**: DNS lookup is successful.
- **FAIL**: DNS lookup is not successful.
- **FORGED**: DNS record does not match.
- **TEMP**: The DNS server replies with a temporary failure message.
- **(empty)**: The SMTP connection is terminated at connection time.

System Event Admin logs

This chapter contains information regarding System Event Admin log messages.

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

You can cross-search an System Event Admin log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

The list of event logs presented in this document is not exhaustive.

The admin event logs contain the following messages:

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

User login

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

Webmail login

Type	kevent

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

User login failure

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

WebMail GUI failure

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

Message retrieval failure

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

Message cannot be read

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

Attachment saving failure

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

LCD login

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

LCD login failure

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

System Event Config logs

This chapter contains information about System Event Config log messages.

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

You can cross-search an Kevent Config log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

Example

If you send the FortiMail log messages to a remote Syslog server (including FortiAnalyzer), a config event log would look like the following and the log fields would appear in the following order:

```
date=2012-08-09 time=12: 42:48 device_id=FE100C3909600504 log_id=0000000920
type=kevent subtype=config pri=information user=admin ui=172.20.120.26
module=unknown submodule=unknown msg="changed settings for 'log setting local'"
```

The list of event logs presented in this document is not exhaustive.

The config event logs contain the following messages:

FortiGuard autoupdate settings	Admin password change	FortiMail appearance information
System update setting	HA settings	FortiMail mail gw user group
Interface IP address	SNMP status	Permission of mail
Access methods/status	SNMP config info	Mail server access
Interface status	SNMP CPU threshold	Local domain deletion
Interface status/PPPoE status	SNMP memory threshold	Local domain addition
Interface status/PPPoE settings	SNMP Logdisk threshold	Local user
Management IP	SNMP maildisk threshold	Local domain name
Interface access methods	SNMP deferred mqueue threshold	User group
MTU change	SNMP virus detection threshold	Mail user addition/deletion
Addressing mode of interface access methods	SNMP spam detection threshold	Mail server user addition
Connect option of interface access methods	SNMP community entry	Mail server user set with information
DNS change	SNMP community and host entry	Mail server user added with information

Primary DNS and secondary DNS	FortiMail disclaimer in header for outgoing messages	Mail server user deletion
Default gateway	FortiMail disclaimer in body for incoming messages	Disk quota of email archiving account
Route entry	FortiMail disclaimer in header for incoming messages	Password of email archiving account
Route with destination IP address/netmask	Local domains	Forwarding address for email archiving
Routing entry	POP3 server port number	Password of system quarantine account
System timezone	Relay server name	Forwarding address for system quarantine
Daylight saving time	SMTP auth	Password of mail user
NTP server settings	SMTP over ssl	Display name of mail user
System time	SMTP server port number	User alias
Console pageNo setting	Status of email archiving	POP3 auth profile
Console mode setting	Email archiving account	IMAP auth profile
Idle timeout	Email archiving rotate setting	Email banned word
Authentication timeout	Archiving settings on local server	Local log setting
System language	Archiving settings on remote server	Memory log setting
LCD PIN number	Archiving policy	Log setting
LCD PIN protection	Archiving exempt	Log setting elog
GUI refresh interval	System quarantine account	Log policy
System idle and auth timeout	System quarantine rotate setting	Alertemail setting
Admin addition	System quarantine quota settings	Alertemail SMTP server
Admin change	System quarantine settings	Alertemail target email addresses
Admin deletion	Mail server settings	Alertemail configuration

FortiGuard autoupdate settings

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

System update setting

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

Interface IP address

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

Access methods/status

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

Interface status

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

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

Interface status/PPPoE status

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

Interface status/PPPoE settings

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

Management IP

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

Interface access methods

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

MTU change

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

Addressing mode of interface access methods

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

Connect option of interface access methods

Type	kevent
Subtype	Config
Severity	Information

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

DNS change

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

Primary DNS and secondary DNS

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

Default gateway

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

Route entry

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

Route with destination IP address/netmask

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

Routing entry

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

System timezone

Type	kevent
Subtype	Config
Severity	Information

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

Daylight saving time

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

NTP server settings

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

System time

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

Console pageNo setting

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

Console mode setting

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

Idle timeout

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

Authentication timeout

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

System language

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

LCD PIN number

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

LCD PIN protection

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

GUI refresh interval

Type	kevent
Subtype	Config
Severity	Information

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

System idle and auth timeout

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

Admin addition

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

Admin change

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

Admin deletion

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

Admin password change

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

HA settings

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

SNMP status

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

SNMP config info

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

SNMP CPU threshold

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

SNMP memory threshold

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

SNMP Logdisk threshold

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

SNMP maildisk threshold

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

SNMP deferred mqueue threshold

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

SNMP virus detection threshold

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

SNMP spam detection threshold

Type	kevent
Subtype	Config
Severity	Information

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

SNMP community entry

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

SNMP community and host entry

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

FortiMail disclaimer in header for outgoing messages

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

FortiMail disclaimer in body for incoming messages

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

FortiMail disclaimer in header for incoming messages

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

Local domains

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

POP3 server port number

Type	kevent
Subtype	Config
Severity	Information

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

Relay server name

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

SMTP auth

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

SMTP over ssl

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

SMTP server port number

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

Status of email archiving

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

Email archiving account

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

Email archiving rotate setting

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

Archiving settings on local server

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

Archiving settings on remote server

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

Archiving policy

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

Archiving exempt

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

System quarantine account

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

System quarantine rotate setting

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

System quarantine quota settings

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

System quarantine settings

Type	kevent
Subtype	Config
Severity	Information

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

Mail server settings

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

FortiMail appearance information

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

FortiMail mail gw user group

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

Permission of mail

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

Mail server access

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

Local domain deletion

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

Local domain addition

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

Local user

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

Local domain name

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

User group

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

Mail user addition/deletion

Type	kevent
FortiMail version	3.0
Severity	Information

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

Mail server user addition

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

Mail server user set with information

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

Mail server user added with information

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

Mail server user deletion

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

Disk quota of email archiving account

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

Password of email archiving account

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

Forwarding address for email archiving

Type	kevent
Subtype	Config
Severity	Information

Message	msg=“forwarding address for email archiving has been modified by user <user_name> via CLI (console|telnet|ssh)”
Meaning	An administrator modified the forwarding address for email archiving using the CLI.

Password of system quarantine account

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

Forwarding address for system quarantine

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

Password of mail user

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

Display name of mail user

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

User alias

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

POP3 auth profile

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

IMAP auth profile

Type	kevent
Subtype	Config
Severity	Information

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

Email banned word

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

Local log setting

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

Memory log setting

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

Log setting

Type	kevent

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

Log setting elog

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

Log policy

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

Alertemail setting

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

Alertemail SMTP server

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

Alertemail target email addresses

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

Alertemail configuration

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

System Event DNS logs

This chapter contains information regarding System Event DNS log messages.

Kevent DNS log is a subtype log of the System Event log type. Kevent DNS log messages contain information about the success or failure of the DNS queries.

You can cross-search a Kevent DNS log message to get more information about it. For more information about log message cross search, see see Log message cross search on page 14.

The list of event logs presented in this document is not exhaustive.

DNS query result

Log Type	kevent
Subtype	DNS
Severity	All severity levels
Message	msg=“<log_message_information>”
Meaning	Any DNS query events.

System Event HA logs

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

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

You can cross-search a System Event HA log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

Example

If you send the FortiMail log messages to a remote Syslog server (including FortiAnalyzer), an HA log would look like the following and the log fields would appear in the following order:

```
date=2012-08-09 time=10:30:31 device_id=FE100C3909600504 log_id=0004001036
type=kevent subtype=ha pri=notice user=ha ui=ha action=none status=success
msg="hahbd: heart beat status changed to primary-hearbeat-port1=FAILED;secondary-
hearbeat-port2=OK"
```

The list of event logs presented in this document is not exhaustive.

The HA event logs contain the following messages:

- HA role change
- HA role change
- HA role change
- Heartbeat check
- Synchronization activities

Master startup

Log Type	kevent
Subtype	HA
Severity	Information
Message	msgs=“monitord: main loop starting, entering MASTER mode”
Meaning	The FortiMail unit is entering master mode.

Slave startup

Log Type	kevent
Subtype	HA
Severity	Information
Message	msgs=“configd: main loop starting, entering slave mode”
Meaning	The FortiMail unit is entering slave mode.

HA role change

Log Type	kevent
Subtype	HA
Severity	Information
Message	msgs=“monitord: ** reached retry limit, assuming MASTER role”
Meaning	The FortiMail unit is assuming the primary unit role because the retry limit was reached for connecting to the original primary unit.

Heartbeat check

Log Type	kevent
Subtype	HA
Severity	Notice
Message	msg="hahbd: <message_text>"
Meaning	Heartbeat related activities.

Synchronization activities

Log Type	kevent
Subtype	HA
Severity	Notice
Message	msg="hasyncd: <message_text>"
Meaning	Synchronization related information.

System Event System logs

This chapter contains information regarding Kevent System log messages.

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

You can cross-search a Kevent System log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

The list of event logs presented in this document is not exhaustive.

The system event logs contain the following messages:

- DNS servers
- System firmware upgrade
- System shutdown
- System reload
- System reset
- System firmware upgrade
- Upgrade system firmware failed
- System mode

DNS servers

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

System restart

Type	kevent
Subtype	System

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

System shutdown

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

System reload

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

System reset

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

System firmware upgrade

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

Upgrade system firmware failed

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

System mode

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

System Event Update logs

This chapter contains information regarding System Event Update log messages.

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

You can cross-search a Kevent Update log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

The list of event logs presented in this document is not exhaustive.

FortiGuard update result

Type	kevent
Subtype	Update
Severity	Warning
Message	msg=”Update result: virusdb:<yes|no>, avengine:<yes|no>, spamdb:<yes|no>, asengine:<yes|no>
Meaning	The FortiMail unit updated the following FortiGuard services: • Antivirus engine • Virus database • Spam database • AntiSpam engine

Mail Event IMAP logs

This chapter contains information regarding Event IMAP log messages.

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

You can cross-search an Event IMAP log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

IMAP-related events

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

Mail Event POP3 logs

This chapter contains information regarding Event POP3 log messages.

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

You can cross-search an Event POP3 log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

POP3-related events

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

Mail Event SMTP logs

This chapter contains information regarding Event-SMTP log messages.

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

You can cross-search an Event SMTP log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

The SMTP event logs contain the following messages:

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

SMTP-related events

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

Starting flgrptd

Type	Event
Subtype	SMTP
Severity	Information

Message	msg= “Starting flgrptd”
Meaning	The reporting daemon is starting. The reporting daemon generates the reports that are available in the web-based manager under *Monitor > Report*. The reporting daemon generates the reports by parsing the various log files.

Virus db loaded

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

FortiGuard antispam rule (FSAR) loading

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

FASR readme

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

FortiGuard antispam rule (FSAR) loaded

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

Mail aliases rebuilt

Type	Event
Subtype	SMTP
Severity	Notification
Message	user=mail ui=mail action=unknown status=success msg=“*@*: alias database /var/spool/etc/mail/aliases has been rebuilt”
Meaning	Mail aliases have been rebuilt.

Updated daemon restarted

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

Antivirus database loading

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

Antivirus database loaded

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

Bayesian database training

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

Bayesian database training completed

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

Mail Event Webmail logs

This chapter contains information regarding Event Webmail log messages.

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

You can cross-search an Event Webmail log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

User login

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

Antivirus logs

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

Antivirus log messages have a subtype called “infected”. Antivirus log messages inform you of viruses detected by your FortiMail unit.

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

You can cross-search an antivirus log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

Example

If you send the FortiMail log messages to a remote Syslog server (including FortiAnalyzer), an antivirus log would look like the following and the log fields would appear in the following order:

```
date=2012-07-24 time=17:07:42 device_id=FE100C3909600504 log_id=0100000924
type=virus subtype=infected pri=information from="syntax@www.ca" to="user2@1.ca"
src=172.20.140.94 session_id="q6OL7fsQ018870-q6OL7fsR018870" msg="The file inline-
16-69.dat is infected with EICAR_TEST_FILE."
```

Virus infection

Log Type	encrypt
Subtype	infected
Severity	information
Message	msg=“The file name is infected with <virus_name>”
Meaning	The file contains the specified virus.

Antispam logs

This chapter contains information regarding spam log messages, including an example of a Antispam log message. Antispam log messages notify you of any spammed email.

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

You can cross-search an antispam log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

Example

If you send the FortiMail log messages to a remote Syslog server (including FortiAnalyzer), an antispam log would look like the following and the log fields would appear in the following order:

```
date=2012-07-20 time=14:33:26 device_id=FE100C3909600504 log_id=0300000924
type=spam pri=information session_id="q6KIXPZe008097-q6KIXPZf008097" client_name="
[172.20.140.94]" dst_ip="172.20.140.92" endpoint="" from="syntax@www.ca"
to="user1@1.ca" subject="Email with wd, excel, and rtf test" msg="Detected by
BannedWord test"
```

Spam-related events

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

Encryption logs

This chapter contains information regarding encryption log messages, including an example of an encryption log message. Encryption log messages inform you of any FortiMail IBE encryption activities.

You can cross-search an encryption log message to get more information about it. For more information about log message cross search, see Log message cross search on page 14.

Example

If you send the FortiMail log messages to a remote Syslog server (including FortiAnalyzer), an encryption log would look like the following and the log fields would appear in the following order:

```
date=2012-08-09 time=10:45:27 device_id=FE100C3909600504 log_id=0400005355
type=encrypt pri=information session_id="q79EiV8S007017-q79EiV8T0070170001474"
msg="User user1@1.ca read secure message, id:'q79EiV8S007017-
q79EiV8T0070170001474', sent from: 'user2@2.ca', subject: 'ppt file'"
```

Email encryption

Log Type	encrypt
Severity	Information
Message	msg="<IBE email encryption related information>"
Meaning	The log message records when FortiMail encrypts and decrypts an email, when the email notification is send to the recipient, when the recipient read the encrypted email, and when any IBE user status expires.

FORTINET®

www.fortinet.com