1. FortiMail Log Message Reference

1.1. FortiMail 2.80 Log Messages

Below are log messages generated in FortiMail 2.80. See the *FortiMail Administration Guide* for more information about logging and reporting in FortiMail 2.80.

1.1.1. Event-Config log messages

1.1.1.1. Message ID 090303 -- 010904

1.1.1.1.1. Message ID 090303

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.2. Message ID 010208

Log Type:	event log, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.3. Message ID 010209

Log Type:	event log, config change
Severity:	Information
FortiMail version:	2.80

Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.4. Message ID 010402

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.5. Message ID 010403

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Messages:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=interface msg="Interface port1|port2|... access methods has been changed by user (user name) via CLI(console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.6. Message ID 010404

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.7. Message ID 010405

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=interface msg="interface port1|port2|... status changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=interface msg="PPPoE settings have been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=interface msg="PPPoE settings have been changed by user (user name) via GUI(ip address)"
Meaning:	A user changed the status of an interface using the CLI. A user changed PPPoE settings using the CLI (or web-based manager).

1.1.1.1.8. Message ID 010406

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.9. Message ID 010409

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=(user name) ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.10. Message ID 010410

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=interface msg="MTU has been enabled for interface port1|port2|... by user (user name) via GUI(ip address)"
Meaning:	A user changed MTU to enabled for an interface using the web-based manager.

1.1.1.1.11. Message ID 010414

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.12. Message ID 010415

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.13. Message ID 010416

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.14. Message ID 010601

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.15. Message ID 010602

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.16. Message ID 010702

Log Type:	event, config change
Severity:	Information

FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=routing msg="default gateway has been changed to (gateway address) by user (user name) via GUI (ip address)"
Meaning:	A user changed the default gateway IP address using the web-based manager.

1.1.1.1.17. Message ID 010703

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=routing msg="Route entry (number) has been deleted by user (user name) via CLI(console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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 CLI or web-based manager.

1.1.1.1.18. Message ID 010705

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=routing msg="A route to (dst address/netmask) has been added by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=routing msg="A route to (dst address/netmask) has been added by user (user name) via GUI (ip address)"
Meaning:	A user added a route with dst address/netmask using the CLI or web-based manager.

1.1.1.1.19. Message ID 010706

Log Type:	event, config change
Severity:	Information

FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=routing msg="Routing entry (number) has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.1.20. Message ID 010901

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=time msg="System timezone has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=time msg="System timezone has been changed by user (user name) via GUI (ip address)" user=user name ui=console|SSH(ip)|telnet(ip) 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 system timezone using the CLI or web-based manager. A user changed the option automatically adjust clock for daylight saving time using the web-based manager.

1.1.1.1.21. Message ID 010902

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=time msg="NTP server settings have been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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 CLI or web-based manager.

1.1.1.1.22. Message ID 010904

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=time msg="System time has been changed by user (user name) via CLI (console|telnet|ssh)" user= ui=console|SSH(ip)|telnet(ip) 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 using the CLI. A user changed the system timezone using the web-based manager.

1.1.1.2. Message ID 011001 -- 012101

1.1.1.2.1. Message ID 011001

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.2.2. Message ID 011002

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=option msg="Console mode setting has been changed to line mode by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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 line mode using the CLI. A user changed the console mode setting to batch using the CLI.

1.1.1.2.3. Message ID 011003

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.2.4. Message ID 011004

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.2.5. Message ID 011005

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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)" user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.2.6. Message ID 011006

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=option msg="LCD PIN number has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.2.7. Message ID 011007

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=option msg="LCD PIN protection has been enabled|disbaled by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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 protection enabled or disabled using the CLI.

1.1.1.2.8. Message ID 011008

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=option msg="GUI refresh interval set to (interval) by user (user name) via CLI (console|telnet|ssh)"

	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=option msg="System idle and auth timeout has been changed by user (user name) via GUI (ip address)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=option msg="Auth timeout has been changed by user (user name) via GUI (ip address)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=option msg="System idle and auth timeout has been changed by user (user name) via GUI (ip address)" user=user name ui=console|SSH(ip)|telnet(ip) 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 web-based manager refresh interval set to another interval using the CLI. A user changed auth timeout using the web-based manager. A user changed system idle and auth timeout from the web-based manager.

1.1.1.2.9. Message ID 011101

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user= ui=console|SSH(ip)|telnet(ip) module=system submodule=admin msg="Admin has been added by user via CLI (console|telnet|ssh)" user= ui=console|SSH(ip)|telnet(ip) module=system submodule=admin msg="Admin has been added by user via GUI (ip address)"
Meaning:	A user added an admin user using the CLI or web-based manager.

1.1.1.2.10. Message ID 011102

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user= ui=console|SSH(ip)|telnet(ip) module=system submodule=admin msg="Admin has been changed by user via CLI (console|telnet|ssh)" user= ui=console|SSH(ip)|telnet(ip) module=system submodule=admin msg="Admin has been changed by user via GUI (ip address)"

Meaning:	A user changed an admin user using the CLI or web-based manager.

1.1.1.2.11. Message ID 011103

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user= ui=console|SSH(ip)|telnet(ip) module=system submodule=admin msg="Admin has been deleted by user via CLI (console|telnet|ssh)" user= ui=console|SSH(ip)|telnet(ip) module=system submodule=admin msg="Admin has been deleted by user via GUI (ip address)"
Meaning:	A user deleted an admin user using the CLI or web-based manager.

1.1.1.2.12. Message ID 011103

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user= ui=console|SSH(ip)|telnet(ip) module=system submodule=admin msg="admin %s password has been changed by user via GUI (ip address)"
Meaning:	A user changed and admin user's password using the web-based manager.

1.1.1.2.13. Message ID 011201

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user= ui=console|SSH(ip)|telnet(ip) module=system submodule=ha msg="HA settings have been changed by user via CLI (console|telnet|ssh)"
Meaning:	A user changed HA settings using the CLI.

1.1.1.2.14. Message ID 011301

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user= ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP has been enabled|disabled by user via CLI (console|telnet|ssh)"
Meaning:	A user enabled/disabled SNMP using the CLI.

1.1.1.2.15. Message ID 011303

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP config info changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP CPU threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP Memory threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP Logdisk threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP maildisk threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP Deferred mqueue threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP Virus detection threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP Spam detection threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP community entry (number) has been deleted by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system

	submodule=snmp msg="SNMP community entry (number) host (number) has been deleted by user (user name) via CLI (console|telnet|ssh)"
Meaning:	A user changed SNMP settings in the CLI.

1.1.1.2.16. Message ID 011901

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
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)" user=user name ui=console|SSH(ip)|telnet(ip) 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)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=snmp msg="SNMP Memory threshold value has been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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)" user=user name ui=console|SSH(ip)|telnet(ip) 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)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Local domains has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Relay server name has been modified to (server name) by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="smtp auth has been modified to (auth profile name) by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="smtp over ssl has been modified to enabled|disabled by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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)" user=user name ui=console|SSH(ip)|telnet(ip) module=system

submodule=mailserver-setting msg="smtp over ssl has been modified to enabled|disabled by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="smtp over ssl has been modified to enabled|disabled by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) 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)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="status of email archiving has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="email archiving account has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="email archiving rotate setting has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Archiving settings on local server has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Archiving settings on remote server has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Archiving policy has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Archiving exempt has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="system quarantine account has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="system quarantine rotate setting has been modified by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) 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)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Mail Server settings have been changed by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="FortiMail appearance information has been changed by user (user name) via CLI (console|telnet|ssh)"
user=user name ui=console|SSH(ip)|telnet(ip) module=system

	submodule=mailserver-setting msg="FortiMail mail gw user group has been changed by user (user nam) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="FortiMail mail gw user group has been deleted by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="System quarantine settings have been changed by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="System quarantine settings have been changed by user (user name) via GUI (ip address)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="smtp over ssl has been modified to enabled|disabled by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-setting msg="Mail Server settings have been changed by user (user name) via GUI(ip address)"
Meaning:	This log contains message information about the following settings that were modified, changed or deleted: • FortiMail disclaimer, FortiMail gw user group • local domains • SNMP Memory threshold value • Relay server name • SMTP auth, over SSL, server port number • POP3 server • status of email arching • email archiving • archive settings, policy and exempt • system quarantine • mail server settings

1.1.1.2.17. Message ID 012001

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-access msg="Permission of mail from (address) is set to OK|REJECT|RELAY|DISCARD by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mailserver-access msg="Permission of mail from (address) is deleted by user (user name) via CLI (console|telnet|ssh)" user=user name ui=GUI(ip address) module=system submodule=mailserver-access msg="Permission of mail from (address) is set to OK|REJECT|RELAY|DISCARD by user (user

	name) via GUI(ip address)" user=user name ui=GUI(ip address) module=system submodule=mailserver-access msg="Mail server access % is deleted by user (user name) via GUI(ip address)"
Meaning:	A user set permission of mail using the CLI or web-based manager. A user deleted permission of mail using the CLI. A user deleted mail server access using the web-based manager.

1.1.1.2.18. Message ID 012101

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=unknown msg="local domain (domain name) is deleted by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=unknown msg="Local domain name (domain name) is added by user (user name) via CLI (console|telnet|ssh)" user=user name ui=GUI(ip address) module=system submodule=mailserver-access msg="Permission of mail from (address) is set to OK|REJECT|RELAY|DISCARD by user (user name) via GUI(ip address)" 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 deleted or added a local domain name using the CLI or web-based manager. A user set permission of mail using the web-based manager.

1.1.1.3. Message ID 030101 -- 030902

1.1.1.3.1. Message ID 030101

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=local msg="Local user (user name) has been added by user (user name) via CLI (console|telnet|ssh)" 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 user using the CLI. A user added a local domain name using the web-based manager.

1.1.1.3.2. Message ID 030102

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.3.3. Message ID 030103

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.3.4. Message ID 030302

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=interface msg="User group has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.3.5. Message ID 030303

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=group msg="User group (group name) has been deleted by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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 CLI or web-based manager.

1.1.1.3.6. Message ID 030501

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="mail user (user address) has been added by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="Mail server user (address) is added with information: displayname (display name) by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="Mail server user (address) is set with information: displayname (display name) by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="Mail server user (address) is added with information: displayname (display name) by user (user name) via GUI(ip address)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="Mail server user (address) is set with information: displayname (display name) by user (user name) via GUI(ip address)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="Mail Server User (address) is deleted by user (user name) via GUI(ip address)"
Meaning:	A user added a mail user using the CLI. A user added or deleted a mail server user using the CLI or web-based manager. A user mail server user set information, displayname using the CLI or web-based manager.

1.1.1.3.7. Message ID 030502

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="disk quota of email archiving account has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="password of email archiving account has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="forwarding address for email archiving has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="password of system quarantine account has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="forwarding address for system quarantine has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="password of mail user (user address) has been modified by user (user name) via CLI (console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) 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:	This log message contains information about the following modified settings: • password of email archiving account • system quarantine or mail user • display name of mail user • forwarding address for system quarantine

1.1.1.3.8. Message ID 030503

Log Type:	event, config
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=system submodule=mail msg="mail user (user address) has been deleted by user (user name) via CLI (console|telnet|ssh)"
Meaning:	A user deleted a mail user using the CLI.

1.1.1.3.9. Message ID 030601

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.3.10. Message ID 030602

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.3.11. Message ID 030603

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.3.12. Message ID 030701

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80

Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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 authentication profile using the CLI.

1.1.1.3.13. Message ID 030702

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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)" user=user name ui=console|SSH(ip)|telnet(ip) 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 renamed/modified a POP3 authentication profile using the CLI.

1.1.1.3.14. Message ID 030703

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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 authentication profile using the CLI.

1.1.1.3.15. Message ID 030801

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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 authentication profile using the CLI.

1.1.1.3.16. Message ID 030802

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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 authentication profile using the CLI.

1.1.1.3.17. Message ID 030803

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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 authentication profile using the CLI.

1.1.1.3.18. Message ID 030902

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.4. Message ID 090101 -- 090305

1.1.1.4.1. Message ID 090101

Log Type:	event, config change

Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=log submodule=logsetting msg="Local log setting has been changed by user (user name) via CLI(console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=log submodule=logsetting msg="Memory logsetting has been changed by user (user name) via CLI(console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=log submodule=logsetting msg="Logsetting has been changed by user (user name) via CLI(console|telnet|ssh)" user=user name ui=console|SSH(ip)|telnet(ip) module=log submodule=logsetting msg="Logsetting has been changed by user (user name) via GUI(ip address)"
Meaning:	A user changed a local log setting using the CLI. A user changed memory log setting using the CLI. A user changed a log setting using the CLI or web-based manager.

1.1.1.4.2. Message ID 090112

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.4.3. Message ID 090301

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.1.4.4. Message ID 090302

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) module=log submodule=alertemail msg="Alertemail SMTP server has been changed to and user has been changed to (user) 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.

1.1.1.4.5. Message ID 090305

Log Type:	event, config change
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip) 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.

1.1.2. Event-System log messages

1.1.2.1. Message ID 000001

Log Type:	event, system
Severity:	Warning
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip)|GUI(1p) action=reboot status=none msg="System has been restarted by user (user name) via console|SSH(ip)|telnet(ip)|GUI(ip)"
Meaning:	A user restarted the system using the CLI or web-based manager.

1.1.2.2. Message ID 000002

Log Type:	event, system
Severity:	Warning

FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip)|GUI(ip) action=shutdown status=none msg="System has been shutdown by user (user name) via console|SSH(ip)|telnet(ip)|GUI(ip)"
Meaning:	A user shutdown the system using the CLI or web-based manager.

1.1.2.3. Message ID 000003

Log Type:	event, system
Severity:	Warning
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip)|GUI(ip) action=reload status=none msg="System has been reloaded by user (user name) via console|SSH(ip)|telnet(ip)|GUI(ip)"
Meaning:	A user reloaded the system using the CLI or web-based manager.

1.1.2.4. Message ID 000005

Log Type:	event, system
Severity:	Warning
FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip)|GUI(ip) action=factory_reset status=none msg="System has been reset to factory default by user (user name) via console|SSH(ip)|telnet(ip)|GUI(ip)" user=LCD ui=LCD action=factory_reset status=none msg="System has been reset to factory default by user LCD via LCD"
Meaning:	A user reset the system to factory default using the CLI or web-based manager. The system was reset by a user using the LCD.

1.1.2.5. Message ID 000007

Log Type:	event, system
Severity:	Warning

FortiMail version:	2.80
Message:	user=user name ui=console|SSH(ip)|telnet(ip)|GUI(ip) action=update status=none msg="System firmware has been upgraded by user (user name) via console|SSH(ip)|telnet(ip)|GUI(ip)" user=user name ui=console|SSH(ip)|telnet(ip)|GUI(ip) action=update status=none msg="System firmware has been downgrade by user (user name) via console|SSH(ip)|telnet(ip)|GUI(ip)" user=user name ui=console|SSH(ip)|telnet(ip)|GUI(ip) action=update status=failure msg="Upgrade system firmware failed by user (user name) via console|SSH(ip)|telnet(ip)|GUI(ip)"
Meaning:	A user upgraded/downgraded system firmware using theCLI or web-based manager. A user upgraded system firmware unsuccessfully using the CLI.

1.1.3. Event-Admin log messages

1.1.3.1. Message ID 000001

Log Type:	event, admin
Severity:	Information
FortiMail version:	2.80
Message:	user=user name ui=GUI(ip) action=login status=success reason=none msg="User (user name) login successfully from GUI(ip)" user=user name ui=WebMail action=login status=success reason=none msg="User (user name) from (ip) logged in" user=user name) ui=console|SSH(ip)|telnet(ip) action=login status=success reason=none msg="User (user name) login successfully from console|SSH(ip)|telnet(ip)" user=user name ui=console|SSH(ip)|telnet(ip) action=login status=failure reason=passwd_invalid|name_invalid|ip_blocked|timeout|max_times msg="User (user name) login failed from console|SSH(ip)|telnet(ip)" user=WebMail ui=WebMail action=login status=failure reason=none msg="mailbox_get_header: failed" user=WebMail ui=WebMail action=login status=failure reason=none msg="mailbox_get_num_parts: failed" user=WebMail ui=WebMail action=login status=failure reason=none msg="Could not get message part" user=WebMail ui=WebMail action=login status=failure reason=none msg="Could not save attachment" user=LCD ui=LCD action=login status=success reason=none msg="Login from LCD successfully" user=LCD ui=LCD action=login status=failure reason=none msg="Login from LCD failed"

Meaning:	Administrative events that occurred successfully or unsuccessfully.

1.1.4. Event-SMTP log messages

1.1.4.1. Message ID 000000

Log Type:	event, smtp
Severity:	All severity levels
FortiMail version:	2.80
Message:	user=mail ui=mail action=unknown status=success msg="(any messages smtp related)"
Meaning:	The event-smtp log records any messages that are SMTP-related.

1.1.5. Event-POP3 log messages

1.1.5.1. Message ID 000000

Log Type:	event, pop3
Severity:	All severity levels
FortiMail version:	2.80
Message:	user=mail ui=mail action=unknown status=success msg="(any messages pop3 related)"
Meaning:	The event-pop3 log records any messages that are POP3 related.

1.1.6. Event-IMAP log messages

1.1.6.1. Message ID 000000

Log Type:	event, imap
Severity:	All severity levels.
FortiMail version:	2.80
Message:	user=mail ui=mail action=unknown status=success msg="(any messages imap related)"
Meaning:	The event-imap log records any messages that are IMAP related.

1.1.7. Antispam log message

1.1.7.1. Message ID 080300

Log Type:	Antispam
Severity:	Information
FortiMail version:	2.80
Message:	session_id=“ ” from=“ ” to=“ ” msg=“ ” session_id=“ ” from=“ ” client_name=“ ” to=“ ” msg=“ ”
Meaning:	Information on emails passing through the FortiMail unit. The information can include any of the following: **session_id** The mail session identification number. **from** The sender's email address. **to** The recipient's email address. **msg** The log message. **session_id** The mail session identification number. **from** The sender's email address. **client_name** The name of the client. **to** The recipient's email address. **msg** The log message.

1.1.8. Antivirus log message

1.1.8.1. Message ID 060101

Log Type:	Antivirus
Severity:	All severity levels.
FortiMail version:	2.80
Message:	from=" " to=" " msg= "The file name is infected with virus_name"
Meaning:	Information on mail that may or may not be infected with a virus passing through the FortiMail unit. The information can include any of the following: **From** The sender's email address. **To** The recipient's email address. **Msg** The file name is infected with virus_name.

1.1.9. History log messages

1.1.9.1. Message ID 050100

<table>
<tr><td>Log Type:</td><td>History</td></tr>
<tr><td>Severity:</td><td>Information</td></tr>
<tr><td>FortiMail version:</td><td>2.80</td></tr>
<tr><td>Message:</td><td>session_id=mail session ID from=mail from client_name=" " resolved=" " to=" " subject=" " message_length=number virus=" " disposition=number classifier=number</td></tr>
<tr><td>Meaning:</td><td>Information on emails passing through the FortiMail unit. The information can include any of the following:
<table>
<tr><td>session_id</td><td>The mail session identification number.</td></tr>
<tr><td>from</td><td>The mail from the sender.</td></tr>
<tr><td>client name</td><td>The client's name.</td></tr>
<tr><td>resolved</td><td>Indicates the client name is resolved. Value could be OK | FAIL | FORGED | TEMP</td></tr>
<tr><td>To</td><td>The recipient's email address.</td></tr>
<tr><td>subject</td><td>The mail's subject line.</td></tr>
<tr><td>message length</td><td>The mail message length.</td></tr>
<tr><td>virus</td><td>The name of the virus.</td></tr>
<tr><td>disposition</td><td>The disposition number can be any one of the following:
0 = Not Spam
1=User White
2=User Black, System White, RBL, SURBL, FortiGuard-AntiSpam, FortiGuard-AntiSpam White, Bayesian, Heuristic, Dictionary Scanner, Banned Word, Deep Header, Forged IP, Quarantine Control, Virus, Attachment Filtered, Grey List, Bypass Scan On Auth, Disclaimer, Defer Delivery, Session Domain, Session Limits, Session White, Session Black, Content Monitor and Filter, Content Monitor treated as Spam, Attachment treated as Spam, Image Spam, Sender Reputation</td></tr>
<tr><td>classifier</td><td>ACTION_UNDEFINED =0x0000
ACTION_ACCEPT =0X0001 // Accept the message
ACTION_LOG =0x0002, // Log it only --- Deprecated. It is not used
ACTION_REJECT =0x0004, // Send a reject to the SMTP client</td></tr>
</table>
</td></tr>
</table>

- ACTION_ADD_HEADER =0X0008, // Add a header to the message
- ACTION _MODIFY_SUBJECT =0x0010, // Modify the subject line
- ACTION_QUARANTINE =0x0020, // Quarantine the message
- ACTION_SUMMARY_REPORT =0X0040, //
- ACTION_BLOCK =0x0080, // Block the message.
- ACTION_DELAY =0X0200, // Delay, greylist the message

account:

- ACTION_FORWARD =0x0400, // Forward the message to a review
- ACTION_DISCLAIMER_BODY =0x0800, // Added a disclaimer to the body
- ACTION_DISCLAIMER_HDR =0x1000, // Added a disclaimer to the headers
- ACTION_DEFER =0x2000, // Defer message delivery
- ACTION_REVIEW =0x4000, // Quarantine for review

1.2. Spam Log Messages

1.2.1. Message #001

Log Type	Spam
Log Level	Error
FortiMail Version	FortiMail v2.0, 2.2
Message	ClassifierHeuristic Error
Explanation	The heuristic scanner encountered an error while processing the message. It is a non-fatal error.
Result	The processing of email will continue.

1.2.2. Message #002

Log Type	Spam
Log Level	Error
FortiMail Version	v2.0, 2.2

Message	MediaException(4099), FileMediaImpl.cpp:36, "Could Not open var/spool/mqueue/dfj7J3FBSK010633"
Explanation	The antispam milter is trying to access the data file, but the data file is not there. The reason might be that the email sender aborted sending the email. It is a non-fatal error.
Result	The processing of email will continue.

1.2.3. Message #003

Log Type	Spam
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	MiterTask:*
Explanation	This message indicates a runtime error and results in a temporary failure of the email. The message describes the exception chain that caused the error.
Result	The email will be temporarily failed. The sending MTA will resend the email.

1.2.4. Message #004

Log Type	Spam
Log Level	Error
FortiMail Version	v2.20, 2.2
Message	Millter::getSession: Could not find matching session.
Explanation	Indicates an internal structural error.
Result	The email will be temporarily failed. The sending MTA will resend the email.

1.2.5. Message #005

Log Type	Spam
Log Level	Error
FortiMail Version	v2.0, 2.2

Message	Milter::destroySession: Could not find matching session
Explanation	Error during connection clean-up.
Result	The processing of the email will continue.

1.2.6. Message #006

Log Type	Spam
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	BayesianException(11) , BayesianImpl.cpp:35,\"Database Driver Init failed\"
Explanation	Database driver initialization failed. System will retry until it is successful. It normally happens at reboot time.
Result	Email service is not affected.

1.3. Event Log Messages

1.3.1. Message #001

Log Type	Event
Log Level	Information
FortiMail Version	v2.0, 2.2
Message	j7J3EXqE008385: to=<user1@fortinet.com>, delay=00:00:12, xdelay=00:00:12, mailer=esmtp,pri=122545, relay=[172.20.110.20] [172.20.110.30], dsn=2.0.0, stat=Sent
Explanation	The email has been delivered successfully.
Result	The email passed through.

1.3.2. Message #002

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	Milter (fas_milter): timeout before data read

Explanation	Smtpd did not get reply from scanner in time (timeout value is 4 minutes).
Result	The email passed through.

1.3.3. Message #003

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	milter_read(fas_milter): cmd read returned 0, expecting 5
Explanation	Communication is incorrect between SMTPD and scanner.
Result	The email passed through.

1.3.4. Message #004

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	Milter (fas_milter): to error state
Explanation	Scanner went to error state for the email being processed.
Result	The email passed through.

1.3.5. Message #005

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	Milter (fas_milter): write(Q) returned -1, expected 5: Broken pipe
Explanation	Smtpd tried to send information to scanner, but the link broke. It happens when scanner is restarting.
Result	The email passed through.

1.3.6. Message #006

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	Milter (fas_milter): error connecting to filter: Connection refused by /var/run/fas.sock
Explanation	Smtpd cannot connect to scanner. It indicates a deadlock in the scanner. The scanner will restart.
Result	The email passed through.

1.3.7. Message #007

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	collect: I/O error on connection from [172.22.4.65],
Explanation	Some errors happened while smtpd was receiving smtp data from sending MTA or client. It indicates the sending side stopped sending the email data, or some network problem.
Result	The sending side aborted sending the email.

1.3.8. Message #008

Log Type	Event
Log Level	Warning
FortiMail Version	v2.0, 2.2
Message	collect: premature EOM: unexpected close
Explanation	The remote party did not send End of Message signal.
Result	The sending side aborted sending the email.

1.3.9. Message #009

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	config error: mail loops back to me (MX problem?)
Explanation	The email cannot be delivered to the destination server, and looped back to the FortiMail unit. It indicates DNS configuration error.
Result	The email will not be delivered.

1.3.10. Message #010

Log Type	Event
Log Level	Error
FortiMail Version	v2.0, 2.2
Message	milter_init: failed to open
Explanation	Smtpd failed to initialize connection with scanner. System will retry until it is successfully initialized.
Result	Service is not affected.

1.4. FortiMail Log Message Exceptions

The FortiMail AntiSpam mechanism uses a dynamic error reporting scheme. Therefore it is impossible to create a definitive list of log entries

The FortiMail AntiSpam mechanism uses a dynamic error reporting scheme. Therefore it is impossible to create a definitive list of log entries that may be encountered. Errors are logged using the following format:

Error Reporter: [Title(value),] [Source File Name:] [Line Number,] [message] [,etc...]

The "message" field of a log entry will be constructed accordingly based on the following exception values:

Value	Name	Description
0	Unknown	Indicates a general error that does not fall into one of the following categories.
1	NullReference	Indicates that the caller attempted to use an unitialized referenced object.
2	InvalidArgument	An invalid argument was passed to a function, for example a null pointer was passed.

3	OutOfRange	Indicates a caller attempted to access data outside the legal range.
4	RunTime	Indicates the called method caught an exception or returned an error value.
5	Parse	Indicates a problem parsing a data type, e.g. encountered an invalid email address.
6	Initialization	Indicates an error during variable initialization.