



FortiGate Log Message Reference™

Version 4.0 MR1

Reference

The FortiGate Log Message Reference is published periodically and, therefore, contains only information that was gathered at the date of publication. Make sure to visit the Fortinet Knowledge Center on a regular basis to verify that you have the current, up-to-date version of the FortiGate Log Message Reference.

FortiGate Log Message Reference

Version 4.0 MR1

31 August 2009

01-410-82627-20090831

© Copyright 2009 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

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

Contents

Introduction	11
Before you begin.....	11
How this reference is organized	11
Document conventions	12
IP addresses.....	12
Cautions, Notes and Tips	12
Typographical conventions	13
Registering your Fortinet product.....	13
Fortinet products End User License Agreement	13
Customer service and technical support.....	14
Training	14
Fortinet documentation	14
Tools and Documentation CD.....	14
Fortinet Knowledge Base	14
Comments on Fortinet technical documentation	14
FortiGate 4.0 log messages	15
Log header variations.....	15
DLP archive logs	15
Debug log messages	16
Traffic	17
10001	18
13001	18
16001	18
16002	19
16003	19
Event-Administration.....	21
32001	22
32002	22
32003	23
32004	23
32005	24
32006	25
32007	28
32008	30
32009	31
32010	32
32011	34
32012	35
32013	36

32014	38
32015	40
32016	40
32017	41
32020	41
32021	41
32022	42
32086	42
32087	42
32095	43
32101	43
32102	44
32103	44
32104	45
32105	45
32120	46
32121	53
32122	55
32123	61
32124	61
32125	61
32126	62
32127	62
32128	62
32129	63
32130	63
32131	63
32132	63
32133	64
32134	64
32135	65
32136	65
32137	66
32138	66
32139	67
32140	75
32141	76
32142	77
32143	78
32144	78
32145	79
32148	79
32149	80
32150	80
32151	81
32152	81

32156	81
32157	82
32160	84
32163	85
32164	85
32165	85
32170	86
32171	86
32172	87
32180	87
32200	87
32545	88
32546	88
Event-System	89
20001	90
20002	91
20031	91
20032	91
20033	91
20034	92
20035	92
20036	92
20037	92
20038	93
20039	93
20040	93
20041	94
20042	94
20043	94
20044	94
20045	95
20046	95
20047	95
20048	95
20049	96
20050	96
20051	96
20052	96
20053	97
20054	97
20055	97
20056	97
20057	98
20058	98
20059	98
20060	98

20061	99
20062	99
20063	99
20064	99
20065	100
20066	100
20067	100
20068	100
20069	101
20070	101
20071	101
20072	101
20073	102
20074	102
20075	102
20076	102
20077	103
20078	103
20079	103
20080	103
20081	104
20082	104
20083	104
20084	104
20090	105
20099	105
20100	105
20101	105
20200	106
20201	106
20202	106
20203	107
22000	107
22001	107
22002	107
22004	108
22005	108
22006	108
22009	109
22010	109
22100	109
22101	110
22102	110
22103	111
22800	111
22801	111

22802	111
22803	112
22911	112
22912	112
22913	112
22914	113
Event-DHCP service.....	115
26001	115
26002	115
Event-Firewall authentication	117
38001	118
38002	119
38003	119
38010	120
38011	120
38012	120
38020	121
Event-Chassis	123
99503	124
99504	124
99505	124
99506	124
99507	125
99508	125
99509	125
Event-IPSec negotiation	127
23002	128
23004	128
23005	128
23007	129
23008	129
23009	129
23008	129
23009	130
23011	131
23012	131
Event-L2TP/PPP/PPPoE	133
29001	134
29002	134
29003	134
29004	134
29009	135
29011	135

29012	135
29013	135
29014	135
29015	136
29016	136
29022	136
29024	136
30004	136
30005	137
30006	137
30007	137
30008	138
30009	138
31004	138
31005	138
31006	139
31007	139
31008	139
31009	139
Event-SSLVPN.....	141
99601	142
99602	142
99603	142
99604	142
99703	143
99705	143
99706	143
99707	143
99708	144
99709	144
99710	144
99805	144
99806	145
99807	145
99808	145
99809	145
99810	146
99811	146
99812	146
99820	146
99825	147
99826	147
99827	147
99840	147
99841	148
99842	148

99843	148
99844	148
Event-VIP SSL	149
45001	150
45003	150
45005	151
45007	151
45009	151
45011	152
45012	152
45013	152
45015	152
45017	153
45019	153
45023	154
45027	154
45029	154
45031	154
Event-WAN Acceleration	155
48001	156
48003	156
48005	156
48007	156
48009	157
48011	157
48012	157
48013	157
48015	158
48017	158
48019	158
48023	158
48027	159
48029	159
48031	159
48100	159
48101	160
48102	160
48123	160
48124	160
48127	161
48129	161
48131	162
48132	162
48200	162
48201	163

48205	163
48300	163
48301	163
Event-LDB-monitor	165
46000	166
46001	166
46002	166
46003	166
46004	167
46005	167
46100	167
46101	167
Event-his-performance	169
47001	169
.....	169
Event-HA	171
35001	171
Event-pattern	173
41000	174
41001	175
41002	175
Data Leak Prevention	177
110000	177
Application Control	179
116000	180
116001	180
116002	180
116003	181
116010	181
116011	181
116013	182
116020	182
Antivirus	183
60000	184
63000	184
63001	185
63002	185
66000	186
Attack	187
70000	187
73001	187

Spam filter	189
SMTP	190
80000	190
80001	190
80002	190
80003	191
80004	191
80005	191
80006	192
80007	192
80008	192
80010	193
80011	193
80012	193
80014	194
80008	194
POP3	195
83003	195
83005	195
83006	195
83007	196
83008	196
83011	196
IMAP	197
86006	197
Webfilter	199
90000	200
91000	200
91005	200
91010	201
93002	201
93003	201
93004	202
93006	202
93007	203
93013	203
99001	203
99501	204
99510	204
99511	204
DLP archives	205
40000	206
60000	206

70000	206
80000	207

Introduction

This reference provides detailed information about all log messages that are recorded by the FortiGate unit. It is intended for administrators that are already logging FortiGate features and require information about a specific log message that was recorded, such as an event-admin log message with the log ID 32005.

This chapter includes the following topics:

- [Before you begin](#)
- [Document conventions](#)
- [Registering your Fortinet product](#)
- [Fortinet products End User License Agreement](#)
- [Customer service and technical support](#)
- [Training](#)
- [Fortinet documentation](#)

Before you begin

Before you begin using this guide, take a moment to note the following:

- The information in this reference applies to all FortiGate units and models currently running FortiOS 4.0 and higher.
- You have enabled logging of FortiGate features. If you have not chosen a log device, or not enabled logging of FortiGate features, see the [Logging and Reporting in FortiOS 4.0 User Guide](#).
- Each log message is written as it would appear in the Raw format on the web-based manager.
- The log message tables in this reference indicate the firmware maintenance release each log message is recorded in, whenever applicable. The firmware maintenance release informs readers which firmware maintenance release records each log message. If no firmware maintenance release is applicable, the firmware version is used (as in the initial release of this document) and indicates the log message carries forward through all FortiOS 4.0 maintenance releases.

Log messages generated in one firmware maintenance release (or firmware version) to another may not contain the exact information because of changes to existing features or new features.

- This reference is published periodically, and therefore, contains only information gathered at the date of publication.

How this reference is organized

This document describes what log messages are recorded by the FortiGate unit.

This document contains the following chapters:

[FortiGate 4.0 log messages](#) provides an overview of what log header types look like, what DLP archives are, and a detailed example with explanation of a debug log message.

The following chapters are grouped by log type with the exception of the event log, and include only log messages for that log type. The event log type chapters are grouped by subtype, for example event-system, due to the large amount of subtypes associated with the event log.

- [Traffic](#)
- [Event-Administration](#)
- [Event-System](#)
- [Event-DHCP service](#)
- [Event-Firewall authentication](#)
- [Event-Chassis](#)
- [Event-IPSec negotiation](#)
- [Event-L2TP/PPP/PPPoE](#)
- [Event-SSLVPN](#)
- [Event-VIP SSL](#)
- [Event-WAN Acceleration](#)
- [Event-LDB-monitor](#)
- [Event-his-performance](#)
- [Event-HA](#)
- [Event-pattern](#)
- [Data Leak Prevention](#)
- [Application Control](#)
- [Antivirus](#)
- [Attack](#)
- [Spam filter](#)
- [Webfilter](#)
- [DLP archives](#)

Document conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

Cautions, Notes and Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.



Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.



Note: Presents useful information, usually focused on an alternative, optional method, such as a shortcut, to perform a step.



Tip: Highlights useful additional information, often tailored to your workplace activity.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input*	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are not secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <code>VPN > IPSEC > Auto Key (IKE)</code> .
Publication	For details, see the FortiGate Administration Guide . Note: Links typically go to the most recent version. To access earlier releases, go to http://docs.fortinet.com/ . This link appears at the bottom of each page of this document.

Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

Fortinet products End User License Agreement

See the [Fortinet products End User License Agreement](#).

Customer service and technical support

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

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

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

Training

Fortinet Training Services provides a variety of training programs to serve the needs of our customers and partners world-wide. Visit the Fortinet Training Services web site at <http://campus.training.fortinet.com>, or email training@fortinet.com.

Fortinet documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

Tools and Documentation CD

The documentation for your product is available on the Fortinet Tools and Documentation CD shipped with your product. The documents on this CD are current at shipping time. For the most current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

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

FortiGate 4.0 log messages

FortiGate logs provide historical and current analysis of network activity to help identify security issues, reducing network misuse and abuse.

For more information about configuring logging in FortiOS 4.0, see the [FortiGate Administration Guide](#). The [Logging and Reporting in FortiOS 4.0 User Guide](#) contains additional information about log messages and logging in general in FortiOS 4.0, and is located on the Fortinet Tech Docs web site.

This section describes:

- [Log header variations](#)
- [DLP archive logs](#)
- [Debug log messages](#)



Note: In FortiOS 4.0 MR1, content archive logs are now called DLP archive logs. This maintenance release also includes a reduction in log size which may affect your schedule of uploading or rolling of log files to a FortiAnalyzer unit.

Log header variations

Log headers are the beginning of the log and inform you of the time the log was recorded, what FortiGate recorded the log, and the firmware version the log was recorded including other important information. The following header is standard format when viewing logs in Raw format in the web-based manager:

```
2009-03-14 05:18:20 devname=FGT50B3G06500085 device_id=FGT50B3G06500085
log_id=0954110000 type=dlp subtype=dlp pri=notice vd=root fwver=04000
```

Log header formats can vary from the above header format when you are viewing logs from a different logging location, such as a Syslog or WebTrends server. For example, a Syslog device can display log information with commas if the Comma Separated Values (CSV) format is enabled.

The following examples show what information is in log headers as well as how that information is displayed.

Remote Syslog log header format

Logs sent to a Syslog server, or multiple Syslog servers, displays log headers as follows:

```
date=2009-04-31 time=06:04:45 devname=FGT-50B device_id=FGT50B3G06500085
log_id=1059116020 type=app-crt1 subtype=app-crt1-all pri=notice, vd=root
fwver=040000
```

WebTrends log header format

Logs sent to a remote NetIQ WebTrends firewall reporting server display log headers as follows:

```
id=firewall time="2009-04-31 15:05:55" fw=FGT50B3G0606500085 pri=5
log_id=0100030101 type=event subtype=admin
```

DLP archive logs

DLP archive logs are historical logs that have been stored on a FortiAnalyzer unit or FortiGuard Analysis server. These log types are:

- Email

- FTP
- Web (HTTP, HTTPS)
- IM/P2P
- VoIP

Configuring DLP archiving is enabled within the DLP sensor. DLP archiving of spam email messages is configured only in the protection profile.

There are two default DLP sensors that you can use for DLP archiving, Content_Archive and Content_Summary. The Content_Archive sensor provides full DLP archiving, which includes all content, for example, email messages include the entire message and attachments. The Content_Summary sensor provides only the meta data about the content, for example, email message summary records only the email header.

For more information about configuring and enabling DLP archiving, see the [UTM User Guide](#). For detailed information about the fields in a DLP archived log message, see [Logging and Reporting in FortiOS 4.0 User Guide](#).

Debug log messages

Debug log messages are only generated if the log severity level is set to Debug. The Debug severity level is the lowest log severity level and is rarely used. This severity level usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly. Debug log messages are generated by all types of FortiGate features.

If you want more detailed information about log messages, similar to the following log messages, see [Logging and Reporting in FortiOS 4.0 User Guide](#).

The following is an example of a debug log message:

```
2009-04-25 17:25:54 log_id=0315093000 type=webfilter subtype=urlfilter
pri=debug msg="found in cache"
```

Table 2: Explanation of an example of a Debug log message

date=(2009-04-25)	The year, month and day of when the event occurred in the format yyyy-mm-dd.
time=(17:25:54)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
log_id=(0315093000)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits represent the message ID.
type=(webfilter)	The section of system where the event occurred. There are eleven log types in FortiOS 4.0. For more information about each log type, see Logging and Reporting in FortiOS 4.0 User Guide .
subtype=(urlfilter)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(debug)	The severity level of the event. There are six severity levels to specify.
msg=("found in cache")	Explains the activity or event that the FortiGate unit recorded.

Traffic

Traffic log messages record the network traffic going through the FortiGate unit.

In the `policyid` field of traffic log messages, the number may be zero because any policy that is automatically added by the FortiGate unit is indexed as zero. For more information, see the Fortinet Knowledge Base article, [Firewall policy=0](#).

10001

13001

16001

16002

16003

10001

Message ID	10001
Log Type	Traffic log – Allowed
Severity	Notification
FortiOS version	4.0
Messages	SN=<session_number> duration=<value_seconds> carrier_ep=<foscarrieronly_end-point_identification> user=<username> group=<groupname> rule=<value_webtrend> policyid=<value_policyid> proto=<protocol> service=<network_service> app_type=<application_or_program> status=accept src=<source_ip_address> srcname={<ip_address> <domain_name>} dst=<destination_ip_address> dstname={<ip_address> <domain_name>} src_int=<source_interface_name> dst_int=<destination_interface_name> sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets> rcvd_pkt=<value_packets> src_port=<source_port> dst_port=<destination_port> vpn={<vpn_name> n/a} tran_ip=<nat_ipaddress> tran_port=<nat_port> dir_disp={org replay} tran_disp={noop snat dnat}
Meaning	Information on the traffic passing through the FortiGate unit.

13001

Message ID	13001
Log Type	Traffic log – Violation
Severity	Notification
FortiOS version	4.0
Messages	SN=<session_number> duration=<value_seconds> carrier_ep=<foscarrieronly_end-point_identification> user=<username> group=<groupname> rule=<value_webtrend> policyid=<value_policyid> proto=<protocol> service=<network_service> app_type=<application_or_program> status=accept src=<source_ip_address> srcname={<ip_address> <domain_name>} dst=<destination_ip_address> dstname={<ip_address> <domain_name>} src_int=<source_interface_name> dst_int=<destination_interface_name> sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets> rcvd_pkt=<value_packets> src_port=<source_port> dst_port=<destination_port> vpn={<vpn_name> n/a} tran_ip=<nat_ipaddress> tran_port=<nat_port> dir_disp={org replay} tran_disp={noop snat dnat}
Meaning	Information on the traffic passing through the FortiGate unit.

16001

Message ID	16001
Log Type	Traffic log – Policy other traffic
Severity	Notification
FortiOS version	4.0
Messages	SN=<session_number> duration=<value_seconds> carrier_ep=<foscarrieronly_end-point_identification> user=<username> group=<groupname> rule=<value_webtrend> proto=<protocol> service=<network_service> app_type=<application_or_program> status={deny accept} src=<source_ip_address> srcname={<ip_address> <domain_name>} dst=<destination_ip_address> dstname={<ip_address> <domain_name>} src_int=<source_interface_name> dst_int=<destination_interface_name> sent=<value_bytes> rcvd=<value_bytes> src_port=<source_port> rule=<rule_number> vpn=<vpn_name> tran_ip=<nat_ipaddress> tran_port=<nat_port>
Meaning	Traffic log for starting a session.

16002

Message ID	16002
Log Type	Traffic log – Policy other traffic
Severity	Warning
FortiOS version	4.0
Messages	SN=<session_number> duration=<value_seconds> carrier_ep=<foscarrieronly_end-point_identification> user=<username> group=<groupname> rule=<value_webtrend> policyid=<value_policyid> proto=<protocol> service=<network_service> app_type=<application_or_program> status={deny accept} src=<source_ip_address> srcname={<ip_address> <domain_name>} dst=<destination_ip_address> dstname={<ip_address> <domain_name>} src_int=<source_interface_name> dst_int=<destination_interface_name> sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets> rcvd_pkt=<value_packets> src_port=<source_port> rule=<rule_number> vpn=<vpn_name> tran_ip=<nat_ipaddress> tran_port=<nat_port> dir_disp={org replay} tran_disp=noop
Meaning	Traffic log for allowed ICMP packet.

16003

Message ID	16003
Log Type	Traffic log – Policy other traffic
Severity	Notification
FortiOS version	4.0
Messages	SN=<session_number> duration=<value_seconds> carrier_ep=<foscarrieronly_end-point_identification> user=<username> group=<groupname> rule=<value_webtrend> policyid=<value_policyid> proto=<protocol> service=<network_service> app_type=<application_or_program> status={deny accept} src=<source_ip_address> srcname={<ip_address> <domain_name>} dst=<destination_ip_address> dstname={<ip_address> <domain_name>} src_int=<source_interface_name> dst_int=<destination_interface_name> sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets> rcvd_pkt=<value_packets> src_port=<source_port> rule=<rule_number> vpn=<vpn_name> tran_ip=<nat_ipaddress> tran_port=<nat_port> dir_disp={org replay} tran_disp=noop
Meaning	Traffic for disallowed ICMP packet.

Event-Administration

Event-Administration log messages record what admin users are configuring on the FortiGate unit, and what is occurring on the FortiGate unit. For example, memory storage is becoming full.

32001	32120	32150
32002	32121	32151
32003	32122	32152
32004	32123	32156
32005	32124	32157
32006	32125	32160
32007	32126	32163
32008	32127	32164
32009	32128	32165
32010	32129	32170
32011	32130	32171
32012	32131	32172
32013	32132	32180
32014	32133	32200
32015	32134	32545
32016	32135	32546
32017	32136	
32020	32137	
32021	32138	
32022	32139	
32086	32140	
32087	32141	
32095	32142	
32120	32143	
32101	32144	
32102	32145	
32103	32148	
32104	32149	
32105		

32001

Message ID	32001
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user= LCD ui= LCD action= login status= success reason= none msg=\ “Login from LCD successfully”
Meaning	A user has logged into the system successfully from the LCD.

Message ID	32001
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user= <administrator_name> ui= {GUI CLI console} action= login status= success reason= none msg=\ “Administrator <administrator_name> logged in successfully from {GUI CLI console}”
Meaning	An administrator logged in successfully.

32002

Message ID	32002
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user= LCD ui= LCD action= login status= failure reason= passwd_invalid msg=\ “Login from LCD failed”
Meaning	The specified user has failed to log in from the LCD because of an incorrect password.
Action	Ensure and verify that administrators and users have the correct passwords.

Message ID	32002
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user= <administrator_name> ui= {GUI CLI console} action= login status= failed reason=\ “<string>” msg=\ “Administrator <administrator_name> login failed from {GUI CLI console}”
Meaning	An administrator failed to log in.

Message ID	32002
Log Type	Event Log - Administration Event
Severity	Alert
FortiOS version	4.0
Messages	user= test ui= cli action= login status= failed reason= test msg= “Alarm testing”
Meaning	An alarm test was initiated.

Message ID	32002
Log Type	Event Log - Administration Event
Severity	Alert
FortiOS version	4.0
Messages	user=<administrator_name> action= login status= failed reason= exceed_limit msg=\“ Login disabled from IP <ip_address> for <seconds> seconds because of too many bad attempts. ”
Meaning	An administrator failed to log in.

32003

Message ID	32003
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} action= logout status= success msg=\“ Administrator <administrator_name> <log_message> ”
Meaning	An administrator logged out.

32004

Message ID	32004
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	action= error-mode reason= self-test msg=\“ Alarm testing ”
Meaning	Alarm testing is occurring on the FortiGate unit.

Message ID	32004
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	action= error-mode reason=<reason> msg=\“ System enters error mode due to <string> ”
Meaning	A FIPS error mode log message.

32005

Message ID	32005
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=login status=failure reason=<string> msg=\“User <administrator_name> login failed from {GUI CLI console LCD}”
Meaning	An administrator has failed to log in.
Action	Ensure and verify that administrators and users have the correct login information.

32006

- The specified administrator has successfully logged into the system.
- The specified administrator has logged in to the system successfully.
- The log disk size is now too big. A rolled log file was deleted to free up space.
- The log disk is almost full.
- The log disk size has the indicated amount used.
- The FortiGate unit has started.
- The log disk is full.
- The System is exiting out of error mode.
- Memory logs are full; system entered error mode. Disk logs are full; system entered error mode. Logs full; system entered error mode.
- The memory log is becoming full.
- A super admin has entered this vdom.
- A super-admin administrator has entered the specified VDOM.

Message ID	32006
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=login status=success reason=none msg="User <administrator_name> login accepted from {GUI CLI console LCD}"
Meaning	The specified administrator has successfully logged into the system.

Message ID	32006
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=login status=success reason=none msg="User <administrator_name> login successfully from {GUI CLI console LCD}"
Meaning	The specified administrator has logged in to the system successfully.

Message ID	32006
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg="Disk logs exceed <integer>% of disk size. Deleted rolled log file name <filename.log>"
Meaning	The log disk size is now too big. A rolled log file was deleted to free up space.

Message ID	32006
Log Type	Event Log - Administration Event
Severity	Warning/Emergency
FortiOS version	4.0

Message ID	32006
Messages	msg=\ “Log disk is <integer>% full. system will {stop logging overwrite old message} once passed <integer>%\”
Meaning	The log disk is almost full.
Message ID	32006
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	msg=\ “Log disk is <integer>% full.\”
Meaning	The log disk size has the indicated amount used.
Message ID	32006
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	msg=\ “Fortigate started”
Meaning	The FortiGate unit has started.
Message ID	32006
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg=\ “Disk has rolled the max number of times. It will not roll logs again until deleting some of the rolled logs.”
Meaning	The log disk is full.
Message ID	32006
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	System exiting out of error mode.
Meaning	The System is exiting out of error mode.
Message ID	32006
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	Memory logs are full system entered error mode. Disk logs are full system entered error mode. Logs full system entered error mode.
Meaning	Memory logs are full; system entered error mode. Disk logs are full; system entered error mode. Logs full; system entered error mode.

Message ID	32006
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg="Memory <logfile name> log is {75% 90% 95%} full"
Meaning	The memory log is becoming full.

Message ID	32006
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=vdom-switch reason=none msg="User <administrator_name> has entered the virtual domain <vdom_name>"
Meaning	A super admin has entered this vdom.

Message ID	32006
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=vdom-switch reason=none msg="User <administrator_name> has entered the virtual domain <vdom_name>"
Meaning	A super-admin administrator has entered the specified VDOM.

32007

- The GUI session of the specified administrator has been dropped because of inactivity.
- The session of the specified administrator has been dropped abnormally.
- The administrator user was disconnected.
- The administrator logged in normally.
- The administrator deleted a specified number of logs from the FortiGate unit.
- The administrator removed filtered log messages from the specified log file.
- The administrator cleared the log disk.
- The administrator exited normally.
- There is not enough storage space for the configuration file because of short flash space.
- A super admin has left the current VDOM.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= logout status= success reason= exit msg="GUI session timeout from {GUI CLI console LCD} "
Meaning	The GUI session of the specified administrator has been dropped because of inactivity.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= logout status= success reason= terminate msg="User <administrator_name> terminates the session from <interface_name>"
Meaning	The session of the specified administrator has been dropped abnormally.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= disconnect user msg="The login session of user <administrator_name> is disconnected by <string> from {GUI CLI console LCD}"
Meaning	The administrator user was disconnected.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Notice
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=logout status=success reason=exit msg="User <administrator_name> logs out from <interface_name>"
Meaning	The administrator logged in normally.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Notice
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} log=<filename> msg="User <administrator_name> has deleted <integer> rolled <log_type> log files from {disk memory}"
Meaning	The administrator deleted a specified number of logs from the FortiGate unit.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} log=<log_name> msg="User <administrator_name> has removed data from disk/memory logs from {disk memory}"
Meaning	The administrator removed filtered log messages from the specified log file.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Notice
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} log=<log_name> msg="User <administrator_name> has cleared disk log from <string>"
Meaning	The administrator cleared the log disk.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=logout status=success reason=exit msg="User <administrator_name> logs out from {GUI CLI}"
Meaning	The administrator exited normally.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	msg="Cannot store config due to short of flash space: require <value> blocks, only <value> free blocks left on flash disk."
Meaning	There is not enough storage space for the configuration file because of short flash space.

Message ID	32007
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=vdom-switch reason=none msg="User <administrator_name> has left the virtual domain <vdom_name>"
Meaning	A super admin has left the current VDOM.

32008

Message ID	32008
Log Type	Event Log - Administration Event
Severity	Notice
FortiOS version	4.0
Messages	user=<user_name> ui=GUI log=<log_name> msg="User <user_name> has viewed the memory/disk logs from <log_name>"
Meaning	The specified user has viewed the specified log files in memory or on the disk.

Message ID	32008
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} log=<log_name> msg="User <administrator_name> has viewed the memory logs from {GUI CLI console}"
	user=<administrator_name> ui={GUI CLI console} log=<log_name> msg="User <administrator_name> has viewed the disk logs from {GUI CLI console}"
Meaning	The specified user displayed the memory logs.
	The specified user displayed the disk logs.

32009

Message ID	32009
Log Type	Event Log - Administration Event
Severity	Alert
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=login status=failure reason=<string> msg=\“User <administrator_name> login failed from {GUI CLI console LCD}”
Meaning	The specified administrator has failed to log in after three attempts from either a network address or via a console connection. After five failed login attempts, the Fortinet device automatically terminates the connection.
Action	Ensure and verify that administrators have the correct login information.

32010

- Log rolling reached the maximum number.
- The amount of logs exceeds the disk size and the rolled log file was deleted.
- The log disk has reached a specific percentage point that, once passed, the system will either overwrite the logs or stop logging.
- Log is full.
- Log is 75% full.
- Log is 90% full.

Message ID	32010
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg=\ <i>"Disk has rolled the max number of times, it will not roll logs again until deleting of the old rolled logs"</i> \
Meaning	Log rolling reached the maximum number.

Message ID	32010
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg=\ <i>"Disk logs exceeded <percentage> of disk size. Deleted rolled log file name <log_name>"</i> \
Meaning	The amount of logs exceeds the disk size and the rolled log file was deleted.

Message ID	32010
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg=\ <i>"Log disk is at <percentage> full. System will {overwrite do no log} once passed."</i> \
Meaning	The log disk has reached a specific percentage point that, once passed, the system will either overwrite the logs or stop logging.

Message ID	32010
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	msg=\ <i>"Log disk is <percentage> full."</i> \
Meaning	Log is full.

Message ID	32010
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	msg=\ Memory <percentage> log is 75% full \
Meaning	Log is 75% full.

Message ID	32010
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=\ Memory <percentage> log is 90% full. \
Meaning	Log is 90% full.

32011

- The FortiGate system started up.
- The FortiGate system entered error mode when memory logs are full.
- The FortiGate system entered error mode when disk logs are full.
- The FortiGate system entered error mode when the logs are full.
- The log disk is full.
- The FortiGate unit entered CC error mode because its memory is full.
- The FortiGate unit entered CC error mode because its disk is full.
- The FortiGate unit entered CC error mode. No reason is known.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	msg=\“ FortiGate started \”
Meaning	The FortiGate system started up.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	Memory logs are full system entered error mode.
Meaning	The FortiGate system entered error mode when memory logs are full.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	Disk logs are full system entered error mode.
Meaning	The FortiGate system entered error mode when disk logs are full.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	Logs full system entered error mode.
Meaning	The FortiGate system entered error mode when the logs are full.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg=\“ Log disk is at <percentage> full. System will <string> content archive data. \”
Meaning	The log disk is full.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	action= error-mode reason= memory-log-full msg=\ “CC error: Memory logs are full. System entered error mode.”
Meaning	The FortiGate unit entered CC error mode because its memory is full.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	action= error-mode reason= disk-log-full msg=\ “CC error: Disk logs are full. System entered error mode.”
Meaning	The FortiGate unit entered CC error mode because its disk is full.

Message ID	32011
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	action= error-mode reason= unknown msg=\ “CC error: Unknown. System entered error mode.”
Meaning	The FortiGate unit entered CC error mode. No reason is known.

32012

Message ID	32012
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	System exiting out of error mode.
Meaning	The FortiGate system is exiting out of error mode.

32013

- A user has cleared the disk log from either the web-based manager or CLI.
- A user has deleted rolled log files.
- A user cleared all current logs.
- A user has cleared FortiGuard logs from the specified location.
- A user has cleared FortiGuard Analysis Service logs from the specified location.
- A user has removed filtered data from memory logs.
- A user cleared logs associated with the FortiGuard Analysis Service.
- A user has removed filtered data from disk logs.

Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI} log=<log_id> msg=\“User <user_name> has cleared disk log from {GUI CLI}”
Meaning	A user has cleared the disk log from either the web-based manager or CLI.

Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI} log=<log_id> msg=\“User <user_name> has deleted rolled <integer> log files from {GUI CLI}”
Meaning	A user has deleted rolled log files.

Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI} log=<log_id> msg=\“User <user_name> has cleared all current logs <percentage_memory> from {GUI CLI}”
Meaning	A user cleared all current logs.

Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI} period=<value> msg=\“User <user_name> has cleared logs (FortiGuard Log) from {GUI CLI}”
Meaning	A user has cleared FortiGuard logs from the specified location.

Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0

Message ID	32013
Messages	user=<administrator_name> ui={GUI CLI} period=<value> msg=\“User <administrator_name> has cleared logs (FortiGuard Analysis Service) from {GUI CLI}\”
Meaning	A user has cleared FortiGuard Analysis Service logs from the specified location.
Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI} log=<log_id> msg=\“User <user_name> has removed filtered data from memory logs from {GUI CLI}\”
Meaning	A user has removed filtered data from memory logs.
Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI} period=<value> msg=\“User <user_name> has cleared logs (FortiGuard Analysis Service) from {GUI CLI}\”
Meaning	A user cleared logs associated with the FortiGuard Analysis Service.
Message ID	32013
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI} log=<log_id> msg=\“User <user_name> has removed filtered data from disk logs from {GUI CLI}\”
Meaning	A user has removed filtered data from disk logs.

32014

- The FDS support license is expiring.
- The FDS AV license is expiring.
- The FDS IPS license is expiring.
- The FortiGuard customer support license expires in the specified number of days.
- The FortiGuard Antivirus update license will expire in the specified number of days.
- The FortiGuard IPS update license will expire in the specified number of days.
- The FortiGuard web filtering license will expire in the specified number of days.
- The FortiGuard anti-spam license will expire in the specified number of days.
- The FortiGuard analysis service license will expire in the specified number of days.
- The FortiGuard management service license will expire in the specified number of days.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=\ <i>FDS support license will expire in <integer> day(s)</i> \
Meaning	The FDS support license is expiring.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=\ <i>FDS AV license will expire in <integer> day(s)</i> \
Meaning	The FDS AV license is expiring.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=\ <i>FDS IPS license will expire in <integer> day(s)</i> \
Meaning	The FDS IPS license is expiring.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=\ <i>FortiGuard customer support license will expire in <value> day(s)</i> \
Meaning	The FortiGuard customer support license expires in the specified number of days.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=“ FortiGuard AV update license will expire in <value> day(s) ”
Meaning	The FortiGuard Antivirus update license will expire in the specified number of days.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=“ FortiGuard IPS upate license will expire in <value> day(s) ”
Meaning	The FortiGuard IPS update license will expire in the specified number of days.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=“ FortiGuard web filtering license will epxire in <value> day(s) ”
Meaning	The FortiGuard web filtering license will expire in the specified number of days.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=“ FortiGuard anti-spam license will expire in <value> day(s) ”
Meaning	The FortiGuard anti-spam license will expire in the specified number of days.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg=“ FortiGuard analysis service license will expire in <value> day(s) ”
Meaning	The FortiGuard analysis service license will expire in the specified number of days.

Message ID	32014
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0

Message ID	32014
Messages	msg="FortiGuard management service license will expire in <value> day(s)"
Meaning	The FortiGuard management service license will expire in the specified number of days.

32015

Message ID	32015
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	msg="Log disk is <percentage> full"
Meaning	Log disk is full.

32016

Message ID	32016
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg="FortiGuard disk quota is <value> use. System will {overwrite no log} once passed all quota is used."
Meaning	The FortiGuard disk quota is full and the system will either overwrite or stop logging when the quota is used.

Message ID	32016
Log Type	Event Log - Administration Event
Severity	Emergency
FortiOS version	4.0
Messages	msg="FortiGuard Analysis Service disk quota is <value> used. System will {overwrite no log} once passed all quota is used."
Meaning	The FortiGuard Analysis Service disk quota is full and the system will either overwrite or stop logging when the quota is used.

Message ID	32016
Log Type	Event Log - Administration Event
Severity	Information
FortiOS version	4.0
Messages	msg="FortiGuard Analysis Service disk quota is <value> used."
Meaning	The FortiGuard Analysis Service disk quota is full.

32017

Message ID	32017
Log Type	Event Log - Administration Event
Severity	Alert
FortiOS version	4.0
Messages	msg="FortiGuard daily quota is reached. System stops logging until <value> sec later."
Meaning	The FortiGuard daily quota is reached.

Message ID	32017
Log Type	Event Log - Administration Event
Severity	Alert
FortiOS version	4.0
Messages	msg="FortiGuard Analysis Service daily quota is reached. System stops logging until <seconds> sec later."
Meaning	The FortiGuard Analysis Service daily quota is full.

32020

Message ID	32020
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	ui=https msg="Corrupted MAC packet detected."
Meaning	A corrupted MAC packet was detected.

Message ID	32020
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	ui=sshv2 msg="Corrupted MAC packet detected."
Meaning	A corrupted MAC packet was detected.

32021

Message ID	32021
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	ui={GUI <ip_address> CLI console} msg="User <user_name> disabled virtual domain root from {GUI <ip_address> CLI console}"
Meaning	The user disabled the virtual domain root from the web-based manager, CLI or console.

32022

Message ID	32022
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	ui={GUI <ip_address> CLI console} msg="User admin enabled virtual domain root from {GUI <ip_address> CLI console}"
Meaning	The user enabled a virtual domain root from the web-based manager, CLI, or console.

32086

Message ID	32086
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} action=mode_change status=fail msg="System failed in changing to {nat transparent} mode by <string> via <string>"
Meaning	The change to the operating mode of the FortiGate unit failed or was successful.

Message ID	32086
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	user=LCD ui=LCD action=<action_type> status=success msg="System has been changed to transparent mode LCD via LCD"
Meaning	The system mode has been changed to transparent mode in the LCD from the LCD interface.

32087

Message ID	32087
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	user=LCD ui=LCD action=<action_type> status=success msg="System has been changed to NAT mode LCD via LCD"
Meaning	System has been changed to NAT mode by user LCD via the LCD.

32095

Message ID	32095
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action={reboot shutdown reload backup factory_reset restore upgrade switch_mode download upload clear_mlog del_log update downgrade del_session bootup} status={success failure} msg="<action_type> by user <administrator_name> via GUI <ip_address>"
Meaning	The specified administrator has performed one of the following actions on the firewall via the GUI: <ul style="list-style-type: none"> • reboot • shutdown • reload • backup • factory reset • restore (all types of configuration files) • firmware upgrade • switch mode • download (all types of configuration files) • upload • clear log in memory buffer • delete log • upgdate virus or IPS signatures • downgrade firmware • delete session • bootup

32101

Message ID	32101
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} profile=<string> msg="User <administrator_name> added new access profile <string> from {GUI CLI console}"
Meaning	A user added a new access profile.

32102

Message ID	32102
Log Type	Event Log - Administration Event
Severity	Variable
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} module=<string> submodule=<string> msg=\“User <administrator_name> made a change via <string>: <string>\”
Meaning	A user has changed the configuration for a specific sub-module via the web-based manager.

Message ID	32102
Log Type	Event Log - Administration Event
Severity	Variable
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} module=<string> submodule=<string> msg=\“<administrator_name> made a change from <string>: <string>\”
Meaning	A user has changed the configuration.

Message ID	32102
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} profile=<string> filed=<string> old=<string> new=<string> msg=\“User <administrator_name> changed the setting of access profile <string> from <string>\”
Meaning	An access profile setting was changed.

32103

Message ID	32103
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} profile=<string> msg=\“User <administrator_name> deleted an access profile <profile_name> from <string>\”
Meaning	A user deleted deleted an access profile.

32104

Message ID	32104
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	admin=<administrator_name> msg=\ “FortiGate <string> failed”
Meaning	An administrator has failed to update the FortiGate unit.

32105

Message ID	32105
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	admin=<administrator_name> msg=\ “Fortigate <string> virdb(<value>) idsdb(<value>) aven(<value>) idsen(<value>) from <string>”
Meaning	An administrator has update the databases and engines sucessfully.

Message ID	32105
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	status= update virdb= yes msg=\ “Fortigate updated virdb (<value>”
Meaning	An administrator has updated AV database successfully.

Message ID	32105
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	status= update idsdb= yes msg=\ “Fortigate updated idsdb (<value>”
Meaning	An administrator has updated the IDS database successfully.

32120

- An administrator added a new interface.
- An administrator changed an interface setting.
- An administrator added a new admin user.
- An administrator added an IP address.
- An administrator added an ipsec phase2-interface entry.
- An administrator added an ipsec manualkey.
- An administrator loaded a CRL certificate.
- An administrator loaded a CA certificate
- An administrator loaded a Local Certificate.
- An administrator loaded a REMOTE certificate.
- An administrator added ipsec phase1 entry.
- An administrator added an ipsec phase1 entry.
- An administrator added an ipsec concentrator.
- An administrator added an ipsec phase2 entry.
- An administrator added a windows AD entry.
- An administrator added a user group.
- An administrator changed the status of a grayware entry.
- An administrator added a file pattern.
- An administrator added an IP pool entry.
- An administrator added a virtual IP entry.
- An administrator added a VIP group.
- An administrator added an address group.
- An administrator added a service group.
- An administrator added a firewall service.
- An administrator added a one-time schedule.
- An administrator added a recurring schedule.
- An administrator added a virtual ip entry.
- An administrator added an IP address.
- An administrator added an IPv6 address group.
- An administrator added a zone.
- An administrator added a report chart widget.
- An administrator added a report summary entry.
- An administrator added a report dataset.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} intf=<interface_name> msg="User <administrator_name> added a new interface from {GUI CLI console LCD}."
Meaning	An administrator added a new interface.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} intf=<interface_name> field=mode old=<string> new=<string> msg="User <administrator_name> changed the mode setting of interface <interface_name> from {GUI CLI console LCD}."
Meaning	An administrator changed an interface setting.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<user_name> msg="User <administrator_name> added an admin user <user_name> from {GUI CLI console}."
Meaning	An administrator added a new admin user.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<user_name> msg="User <administrator_name> added an address <ip_address> from {GUI CLI console}."
Meaning	An administrator added an IP address.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<phase2_name> phase1name=<phase2_name> msg="User <administrator_name> added an ipsec phase2-interface entry <phase2_name> from {GUI CLI console}."
Meaning	An administrator added an ipsec phase2-interface entry.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification

Message ID	32120
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<key_name> remote-gw=<gateway_ip> interface={dmz wan1 wan2 internal external ...} msg="User <administrator_name> added an ipsec manualkey <key_name> from {dmz wan1 wan2 internal external ...}admin user <user_name> from {GUI CLI console}."
Meaning	An administrator added an ipsec manualkey.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> loaded a CRL certficiate <certificate_name> from {GUI CLI console}."
Meaning	An administrator loaded a CRL certificate.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> loaded a CA certificate <certificate_name> from {GUI CLI console}."
Meaning	An administrator loaded a CA certificate

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<user_name> msg="User <administrator_name> added an admin user <user_name> from {GUI CLI console}."
Meaning	An administrator added a new admin user.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> loaded local certificate <certificate_name> from {GUI CLI console}."
Meaning	An administrator loaded a Local Certificate.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0

Message ID	32120
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> loaded a REMOTE certificate <certificate_name> from {GUI CLI console}."
Meaning	An administrator loaded a REMOTE certificate.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<phase1_name> remote-gw=<gateway_ip> interface={dmz wan1 wan2 internal external ...} msg="User <administrator_name> added an ipsec phase1-interface entry {dmz wan1 wan2 internal external ...} from {GUI CLI console}."
Meaning	An administrator added ipsec phase1 entry.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<phase1_name> remote-gw=<gateway_ip> msg="User <administrator_name> added an ipsec phase1 <phase1_name> from {GUI CLI console}."
Meaning	An administrator added an ipsec phase1 entry.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<concentrator_name> msg="User <administrator_name> added an ipsec concentrator <concentrator_name> from {GUI CLI console}."
Meaning	An administrator added an ipsec concentrator.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<phase2_name> phase1name=<phase2_name> msg="User <administrator_name> added an ipsec phase2 <phase2_name> from {GUI CLI console}."
Meaning	An administrator added an ipsec phase2 entry.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0

Message ID	32120
Messages	user=<administrator_name> ui={GUI CLI console} name=<ADuser_name> server=<AD_server_ip> msg="User <administrator_name> added a windows AD entry <ADuser_name> from {GUI CLI console}."
Meaning	An administrator added a windows AD entry.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<group_name> msg="User <administrator_name> added a user group <group_name> from {GUI CLI console}."
Meaning	An administrator added a user group.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<grayware_name> old_status={enable disabled} new_status={enabled disabled} msg="User <administrator_name> changed the status of a grayware entry <grayware_name> from {GUI CLI console}."
Meaning	An administrator changed the status of a grayware entry.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<pattern_name> msg="User <administrator_name> added a file pattern <pattern_name> from {GUI CLI console}."
Meaning	An administrator added a file pattern.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<ippool_name> msg="User <administrator_name> added an IP pool entry <ippool_name> from {GUI CLI console}."
Meaning	An administrator added an IP pool entry.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0

Message ID	32120
Messages	user=<administrator_name> ui={GUI CLI console} name=<vip_name> msg="User <administrator_name> added a virtual ip entry <vip_name> from {GUI CLI console}."
Meaning	An administrator added a virtual IP entry.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<vip_group_name> msg="User <administrator_name> added a vip group <vip_group_name> from {GUI CLI console}."
Meaning	An administrator added a VIP group.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<group_name> msg="User <administrator_name> added an address group <group_name> from {GUI CLI console}."
Meaning	An administrator added an address group.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<group_name> msg="User <administrator_name> added a service group <group_name> from {GUI CLI console}."
Meaning	An administrator added a service group.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<service_name> msg="User <administrator_name> added a firewall service <service_name> from {GUI CLI console}."
Meaning	An administrator added a firewall service.
Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<schedule_name> msg="User <administrator_name> added a one-time schedule <schedule_name> from {GUI CLI console}."
Meaning	An administrator added a one-time schedule.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<schedule_name> msg="User <administrator_name> added a recurring schedule <schedule_name> from {GUI CLI console}."
Meaning	An administrator added a recurring schedule.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<vip_name> msg="User <administrator_name> added a virtual ip entry <vip_name> from {GUI CLI console}."
Meaning	An administrator added a virtual ip entry.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<ip_name> msg="User <administrator_name> added an address <ip_name> from {GUI CLI console}."
Meaning	An administrator added an IP address.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<ipv6_name> msg="User <administrator_name> added an address group <ipv6_name> from {GUI CLI console}."
Meaning	An administrator added an IPv6 address group.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI(ip_address) CLI console} action=add-zone zone=<zone_name> msg="User <administrator_name> added new zone <zone_name> from {GU(ip_address) CLI console}."
Meaning	An administrator added a zone.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification

Message ID	32120
FortiOS version	4.0(MR1)
Messages	user=<administrator_name> name=<name> ui={GUI(ip_address) CLI console} msg="User <administrator_name> added a report chart widget <widget_name> from {GU(ip_address) CLI console}."
Meaning	An administrator added a report chart widget.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0(MR1)
Messages	user=<administrator_name> name=<name> ui={GUI(ip_address) CLI console} msg="User <administrator_name> added a report summary entry <entry_name> from {GU(ip_address) CLI console}."
Meaning	An administrator added a report summary entry.

Message ID	32120
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0(MR1)
Messages	user=<administrator_name> name=<name> ui={GUI(ip_address) CLI console} msg="User <administrator_name> added a report dataset <dataset_name> from {GU(ip_address) CLI console}."
Meaning	An administrator added a report dataset.

32121

Message ID	32121
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	<p>user=<administrator_name> ui={GUI CLI console LCD} intf={internal external dmz <other>...} field=ip old=<ip_address>:<ip_mask> new=<ip_address>:<ip_mask> msg="User <administrator_name> changed the setting of an interface from {GUI CLI console LCD}"</p> <p>user=<administrator_name> ui={GUI CLI console LCD} intf={internal external dmz <other>...} field=access old={HTTPS PING HTTP SSH SNMP TELNET} new={HTTPS PING HTTP SSH SNMP TELNET} msg="User <administrator_name> changed the setting of an interface from {GUI CLI console LCD}"</p>
Meaning	The administrator changed the specified interface settings from "old" to "new".

Message ID	32121
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0

Message ID	32121
Messages	user=<administrator_name> ui={GUI CLI console LCD} intf={internal external dmz <other>...} field=status old={up down} new={up down} msg="User <administrator_name> changed the status of interface {internal external dmz <other>...} from {GUI CLI console LCD}"
Meaning	The administrator changed the interface status setting.
Message ID	32121
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} field=mtu old={up down} new={up down} msg="User <administrator_name> changed the mtu setting of interface <interface_name> from {GUI CLI console LCD}"
Meaning	The administrator changed an interface setting.
Message ID	32121
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} field=status old=<ip_address> new=<ip_address> msg="User <administrator_name> changed the ip setting of the interface <interface_name> from {GUI CLI console LCD}"
Meaning	The administrator changed an interface setting.

32122

- The administrator deleted the specified interface.
- An administrator deleted an admin user.
- An administrator deleted an ipsec phase2-interface entry.
- The administrator deleted an ipsec manualkey.
- An administrator deleted a CA certificate.
- An administrator has removed all CA certificates.
- An administrator deleted a local certificate.
- An administrator deleted all local certificates.
- An administrator deleted a CRL certificate.
- An administrator deleted all CRLs.
- An administrator deleted an ipsec phase1-interface entry.
- An administrator deleted an ipsec phase1 entry.
- An administrator deleted an ipsec concentrator entry.
- An administrator deleted an ipsec phase2 entry.
- An administrator deleted a windows AD entry.
- An administrator deleted a user group.
- An administrator deleted a file pattern.
- An administrator deleted an IP pool entry.
- An administrator deleted an address group.
- An administrator deleted a service group.
- An administrator deleted a firewall service.
- An administrator deleted a one-time schedule.
- An administrator deleted a recurring schedule
- An administrator deleted a virtual ip entry.
- An address is deleted.
- An administrator deleted an IPv6 address group.
- An administrator deleted an address.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} intf=<interface_name> msg="User <administrator_name> deleted an interface from {GUI CLI console LCD}"
Meaning	The administrator deleted the specified interface.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<user_name> msg="User <administrator_name> deleted an admin user <user_name> from {GUI CLI console LCD}"
Meaning	An administrator deleted an admin user.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<name> phase2name=<phase2_name> msg="User <administrator_name> deleted an ipsec phase2-interface entry <phase2_name> from {GUI CLI console}"
Meaning	An administrator deleted an ipsec phase2-interface entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<manualkey_name> remote-gw=<gateway_ip> msg="User <administrator_name> deleted an ipsec manualkey <manualkey_name> from {GUI CLI console}"
Meaning	The administrator deleted an ipsec manualkey.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> removed a CA certificate <certificate_name> from {GUI CLI console}."
Meaning	An administrator deleted a CA certificate.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> removed all CA certificates from {GUI CLI console}."
Meaning	An administrator has removed all CA certificates.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> deleted a local certificate <certificate_name> from {GUI CLI console}"
Meaning	An administrator deleted a local certificate.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> removed all local certificates from {GUI CLI console}"
Meaning	An administrator deleted all local certificates.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> removed a CRL certificate <certificate_name> from {GUI CLI console}"
Meaning	An administrator deleted a CRL certificate.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} msg="User <administrator_name> removed all CRL certificates from {GUI CLI console}"
Meaning	An administrator deleted all CRLs.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<phase1_name> remote-gw=<gateway_ip> interface={dmz internal external wan1 ...} msg="User <administrator_name> deleted an ipsec phase1-interface entry <phase1_name> from {GUI CLI console}"
Meaning	An administrator deleted an ipsec phase1-interface entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<phase1_name> remote-gw=<gateway_ip> msg="User <administrator_name> deleted an ipsec phase1 <phase1_name> from {GUI CLI console}"
Meaning	An administrator deleted an ipsec phase1 entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<concentrator_name> msg="User <administrator_name> deleted an ipsec concentrator <concentrator_name> from {GUI CLI console}"
Meaning	An administrator deleted an ipsec concentrator entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<name> phase1name=<phase1_name> msg="User <administrator_name> deleted an ipsec phase2 <phase2_name> from {GUI CLI console}"
Meaning	An administrator deleted an ipsec phase2 entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<winad> server=<server_ip> msg="User <administrator_name> deleted a windows AD entry <winad_name> from {GUI CLI console}"
Meaning	An administrator deleted a windows AD entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<group_name> msg="User <administrator_name> deleted a user group <group_name> from {GUI CLI console}"
Meaning	An administrator deleted a user group.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<pattern_name> msg="User <administrator_name> deleted a file pattern <pattern_name> from {GUI CLI console}"
Meaning	An administrator deleted a file pattern.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<ippool_name> msg="User <administrator_name> deleted a IP pool entry <ippool_name> from {GUI CLI console}"
Meaning	An administrator deleted an IP pool entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<group_name> msg="User <administrator_name> deleted an address group <group_name> from {GUI CLI console}"
Meaning	An administrator deleted an address group.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<group_name> msg="User <administrator_name> deleted a service group <group_name> from {GUI CLI console}"
Meaning	An administrator deleted a service group.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<service_name> msg="User <administrator_name> deleted a firewall service <service_name> from {GUI CLI console}"
Meaning	An administrator deleted a firewall service.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<schedule_name> msg="User <administrator_name> deleted a one-time schedule <schedule_name> from {GUI CLI console}"
Meaning	An administrator deleted a one-time schedule.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<schedule_name> msg="User <administrator_name> deleted a recurring schedule <schedule_name> from {GUI CLI console}"
Meaning	An administrator deleted a recurring schedule

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<vip_name> msg="User <administrator_name> deleted a virtual ip entry <vip_name> from {GUI CLI console}"
Meaning	An administrator deleted a virtual ip entry.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<address_name> msg="User <administrator_name> deleted an address <address_name> from {GUI CLI console}"
Meaning	An address is deleted.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<ipv6_name> msg="User <administrator_name> deleted an address group <ipv6_name> from {GUI CLI console}"
Meaning	An administrator deleted an IPv6 address group.

Message ID	32122
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} name=<address_name> msg="User <administrator_name> deleted an address <address_name> from {GUI CLI console}"
Meaning	An administrator deleted an address.

32123

Message ID	32123
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} seq=<value_order> device={internal external dmz} distance=<value_hops> dst=<ip_address> status={up down} flags=<string> msg="User <administrator_name> added a new static routing entry from {GUI CLI console LCD} (<ip_address>)"
Meaning	The administrator added the specified static route entry.

32124

Message ID	32124
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} seq=<value_order> old_device={internal external dmz <other> ...} old_distance=<value_hops> old_priority=<admin_priority> old_dst=<ip_address> old_status={up down} old_flags=<string> new_device={internal external dmz <other> ...} new_distance=<value_hops> new_priority=<admin_priority> new_dst=<ip_address> new_status={up down} new_flags=<string> msg="User <administrator_name> changed the setting of a new static routing entry from {GUI CLI console LCD}"
Meaning	The administrator made the specified changes to the static route entry.

32125

Message ID	32125
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} seq=<value_order> device={internal external dmz <other> ...} distance=<value_hops> priority=<admin_priority> dst=<ip_address> status={up down} flags=<string> msg="User <administrator_name> deleted a static routing entry from {GUI CLI console LCD}"
Meaning	The administrator deleted the specified static route entry.

32126

Message ID	32126
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} seq=<order_number> msg="User <administrator_name> added a new firewall policy from {GUI CLI console LCD}"
Meaning	The administrator added a new firewall policy.

32127

Message ID	32127
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} old_sintf=<interface_name> old_dintf=<interface_name> old_saddr=<ip_address> old_daddr=<ip_address> old_schd=<schedule_name> old_svr=<network_service> old_act=<string> old_nat=<string> old_log=<string> new_sintf=<interface_name> new_dintf=<interface_name> new_saddr=<ip_address> new_daddr=<ip_address> new_schd=<schedule_name> new_svr=<ip_address> new_schd=<schedule_name> new_srv=<network_service> new_act=<string> new_nat=<string> new_log=<string> msg="User <administrator_name> changed a firewall policy from {GUI CLI console LCD}"
Meaning	The administrator made the specified changes to a firewall policy.

32128

Message ID	32128
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} seq=<policy_id> sintf=<interface_name> dintf=<interface_name> saddr=<ip_address> daddr=<ip_address> schd=<schedule_name> svr=<network_service> act=<string> nat=<string> log=<string> msg="User <administrator_name> deleted a firewall policy from from {GUI CLI console LCD}"
Meaning	The administrator deleted a firewall policy.

32129

Message ID	32129
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> status={enable disable} msg="User <administrator_name> added a local user from {GUI CLI console LCD}"
Meaning	The administrator added a new local administrator.

32130

Message ID	32130
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> old_status=<string> new_status=<string> passwd=<password> msg="User <administrator_name> changed a local user's setting from {GUI CLI console LCD}"
Meaning	The administrator added a new local administrator. The administrator changed the specified settings for a local administrator.

32131

Message ID	32131
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> status={enable disable} msg="User <administrator_name> deleted a local user <administrator_name> deleted a local user from {GUI CLI console LCD}"
Meaning	The administrator deleted the specified local administrator from the system.

32132

Message ID	32132
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<server_name> server=<server_address> msg="User <administrator_name> added a radius user from {GUI CLI console LCD}"
Meaning	The administrator added a RADIUS server to the server list, deleted the specified local administrator from the system.

Message ID	32132
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<server_name> server=<server_address> msg="User <administrator_name> added TACACS+ server <server_address> from {GUI CLI console LCD}"
Meaning	The administrator added a new TACACS+ server to the server list.

32133

Message ID	32133
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> old_server=<server_address> new_server=<server_address> secret=<sever_secret> msg="User <administrator_name> changed a radius' setting user from {GUI CLI console LCD}"
Meaning	The administrator made the specified changes to the RADIUS server entry.

Message ID	32133
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> old_server=<server_address> new_server=<server_address> key=<key> msg="User <administrator_name> changed a TACACS+ server <server_address> setting from {GUI CLI console LCD}"
Meaning	An administrator changed a TACACS+ server's setting.

32134

Message ID	32134
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> server=<server_address> msg="User <administrator_name> deleted a radius user from {GUI CLI console LCD}"
Meaning	The administrator deleted the RADIUS server from the server list.

Message ID	32134
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0

Message ID	32134
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> server=<server_address> msg="User <administrator_name> deleted a TACACS+ server <server_address> from {GUI CLI console LCD}"
Meaning	An administrator deleted a TACACS+ server.

32135

Message ID	32135
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<server_name> server=<server_address> msg="User <administrator_name> added an ldap user from {GUI CLI console LCD}"
Meaning	The administrator added a new LDAP server to the list.

Message ID	32135
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<user_name> policy={permit deny} msg="User <administrator_name> added an im/p2p {AIM ICQ MSN Yahoo} user <user_name> from {GUI CLI console LCD}"
Meaning	An administrator added an IM/P2P user.

32136

Message ID	32136
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> old_server=<server_address> old_port=<port_num> old_cn=<value_cn> old_dn=<dn_name> new_server=<server_address> new_port=<port_num> new_cn=<value_cn> new_dn=<dn_name> msg="User <administrator_name> changed an ldap user's setting from {GUI CLI console LCD}"
Meaning	The administrator made the specified changes to an LDAP server entry.

32137

Message ID	32137
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> server=<server_address> msg="User <administrator_name> deleted an ldap user from {GUI CLI console LCD}"
Meaning	The administrator deleted the LDAP server from the list.

32138

Message ID	32138
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= <i>reboot</i> msg="User <administrator_name> rebooted the device from {GUI CLI console LCD}"
	user=<administrator_name> ui={GUI CLI console LCD} action= <i>shutdown</i> msg="User <administrator_name> shut down the device from {GUI CLI console LCD}"
Meaning	The administrator rebooted the FortiGate unit.
	The administrator shut down the FortiGate unit.

32139

- The administrator performed a reset to factory default settings.
- The administrator formatted the local disk.
- The administrator restored the image firmware.
- The administrator restored a backup of the configuration.
- The administrator imported a certificate.
- The administrator restored a complete configuration.
- The administrator updated the firmware.
- The administrator uploaded an image with an invalid RSA signature.
- The administrator uploaded an image with a valid RSA signature and new public key.
- The administrator uploaded an image with a valid RSA signature.
- The administrator uploaded an image that does not have a valid RSA signature.
- The administrator uploaded an image that contains an RSA signature with a new key.
- The administrator uploaded an image and it does not have a valid CC signature.
- The auto-install restored configuration from the USB key.
- The auto-install restored the firmware image from the USB key.
- An admin user updated the virus and IDS database.
- An admin user updated the IDS database.
- An admin user formatted the log disk.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=factory-reset msg=\“User <administrator_name> reset to the factory settings from {GUI CLI console LCD}”\
Meaning	The administrator performed a reset to factory default settings.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=format-disk msg=\“User <administrator_name> formatted the log disk from {GUI CLI console LCD}”\
Meaning	The administrator formatted the local disk.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-image msg=\“User <administrator_name> restored the image from {GUI CLI console LCD}”\
Meaning	The administrator restored the image firmware.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-image msg=\“User <administrator_name> restored the image from {GUI CLI console LCD} (<ip_address> -> <ip_address>)”\
Meaning	The administrator restored the image firmware.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-configuration msg=\“User <administrator_name> restored the configuration from {GUI CLI console LCD}”\
Meaning	The administrator restored a backup of the configuration.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=import-certificate msg=\“User <administrator_name> imported the certificate from {GUI CLI console LCD}”\
Meaning	The administrator imported a certificate.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-all-configuration msg=\“User <administrator_name> restored all the configuration from {GUI CLI console LCD}”\
Meaning	The administrator restored a complete configuration.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=update msg=\“User <administrator_name> updated the firmware from {GUI CLI console LCD}”\
Meaning	The administrator updated the firmware.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image has an invalid RSA signature.”\
Meaning	The administrator uploaded an image with an invalid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does have a valid RSA signature with a new public key.”\
Meaning	The administrator uploaded an image with a valid RSA signature and new public key.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does have a valid RSA signature.”\
Meaning	The administrator uploaded an image with a valid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does not have a valid RSA signature.”\
Meaning	The administrator uploaded an image that does not have a valid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-diag-app msg=\“User <administrator_name> loaded a diagnostic application from {GUI CLI console LCD} with serial number <serial_number>. The executable result = <string>\”\
Meaning	The administrator loaded a diagnostic application.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-forticlient msg=\“User <administrator_name> restored the image <image_name> from {GUI CLI console LCD}\”\
Meaning	The administrator restored a FortiClient firmware image.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD} the new image has an invalid RSA signature.\”\
Meaning	The administrator loaded a new image; however, it has an invalid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-image msg=\“User <administrator_name> loaded the image from {GUI CLI console LCD} the new image has RSA signature with new key.\”\
Meaning	The administrator loaded a firmware image that contains an RSA signature with a new key.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=loaded-image msg=\“User <administrator_name> loaded the image from {GUI CLI console LCD} the new image does not support CC mode.\”\
Meaning	The administrator loaded a firmware image that does not support CC mode.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-image msg=\“User <administrator_name> restored image from {GUI CLI console LCD} (<ip_address> -> <ip_address>).\”\
Meaning	The administrator restored an image.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-configuration msg=\“User <administrator_name> restored the configuration from {GUI CLI console LCD}.\”\
Meaning	The administrator restored a configuration.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-configuration msg=\“User <administrator_name> failed to restore the configuration from {GUI CLI console LCD}.\”\
Meaning	The administrator failed to restore the configuration.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=update-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image has an invalid CC signature.\”\
Meaning	There was an error updating the image.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=update-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image has an invalid RSA signature.\”\
Meaning	The administrator updated an image that has an invalid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= update-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does have a valid RSA signature with new public key.”\
Meaning	The administrator loaded an image with a valid RSA signature with a new public key.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= update-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does have a valid RSA signature.”\
Meaning	The administrator loaded an image that contains a valid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= update-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does not have a valid RSA signature.”\
Meaning	The administrator loaded an image that does not contain a valid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= update-image msg=\“User <administrator_name> updated the image from {GUI CLI console LCD} (<ip_address> -> <ip_address>).”\
Meaning	The administrator updated an image.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= loaded-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image has RSA signature with new key.”\
Meaning	The administrator uploaded an image that contains an RSA signature with a new key.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=restore-image msg=\“User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image has an invalid CC signature.”\
Meaning	The administrator uploaded an image and it does not have a valid CC signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=auto-install ui=usb action=restore-configuration msg=\“User auto install restored the configuration from usb.”\
Meaning	The auto-install restored configuration from the USB key.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=auto-install ui=usb action=restore-image msg=\“User auto install restored the image from usb (<ip_address> -> <ip_address>).”\
Meaning	The auto-install restored the image.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=auto-install ui=usb action=restore-image msg=\“User <administrator_name> restored the configuration from usb.”\
Meaning	The auto-install restored the firmware image from the USB key.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=update msg=\“User <admin_user> requested a virus and IDS engine/definitions update from {GUI CLI console LCD}”\
Meaning	An admin user updated the virus and IDS database.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=update msg= “User <admin_user> requested an IDS engine/definitions update from {GUI CLI console LCD}”
Meaning	An admin user updated the IDS database.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=update msg= “User <admin_user> formatted the log disk from {GUI CLI console LCD}”
Meaning	An admin user formatted the log disk.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=“system” action=restore-image msg= “System loaded an image from FortiGuard Management, the new image has an invalid CC signature.”
Meaning	The system encountered an error when trying to restore an image from the FortiGuard Analysis and Management Service.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=“system” action=loaded-image msg= “System loaded an image from FortiGuard Management, the new image has an invalid RSA signature.”
Meaning	The system loaded an image that contains an invalid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user=“system” action=loaded-image msg= “System loaded an image from FortiGuard Management, the new image does have a valid RSA signature with a new public key.”
Meaning	The system loaded an image containing a valid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user= "system" action= loaded-image msg=\ "System loaded an image from FortiGuard Management, the new image has a valid RSA signature." \
Meaning	The system loaded an image that contains a valid RSA signature.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Critical
FortiOS version	4.0
Messages	user= "system" action= restore-image msg=\ "System restored the image from FortiGuard Management (<ip_address> -> <ip_address>)."' \
Meaning	The system restored an image from the FortiGuard Analysis and Management Service.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	user= "system" action= restore-template msg=\ "System restored configuration template <template_name> from management station." \
Meaning	The system restored a template from the management station.

Message ID	32139
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	user= "system" action= restore-configuration msg=\ "System failed to restore configuratino from management station." \
Meaning	The system failed to load a configuration file from the management station.

32140

Message ID	32140
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} field={mode virtual-domain hostname ip-overlap auth-timeout detection-interval} old-value=<value_ip_overlap> new_value=<value> msg= "User <administrator_user> changed global setting from {GUI CLI console LCD}"
Meaning	The administrator has changed the global setting specified in the 'field' field.

Message ID	32140
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=time_change field=date-time msg="User <administrator_user> changed the global settings from {GUI CLI console LCD}"
Meaning	The administrator has changed the global time setting.

Message ID	32140
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} field=date-time msg="The ntp daemon changed time from <old_time> to <new_time>"
Meaning	The NTP time is updated.

32141

Message ID	32141
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	id=<id_value> msg=<log_message_information>
Meaning	DHCPD (client) or DHCPD (server) log information.

32142

- The administrator backed up the current configuration to a file.
- The administrator backed up the specified file.
- The administrator failed to back up the specified file.
- The administrator backed up all the logs.
- The administrator failed to back up all log files.

Message ID	32142
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= backup msg="User <administrator_name> backed up the configuration from {GUI CLI console LCD}"
Meaning	The administrator backed up the current configuration to a file.

Message ID	32142
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= backup msg="User <administrator_name> backed up <file_name> log from {GUI CLI console LCD}"
Meaning	The administrator backed up the specified file.

Message ID	32142
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= backup msg="User <administrator_name> failed to backup <file_name> log from {GUI CLI console LCD}"
Meaning	The administrator failed to back up the specified file.

Message ID	32142
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= backup msg="User <administrator_name> backed up all the logs from {GUI CLI console LCD}"
Meaning	The administrator backed up all the logs.

Message ID	32142
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0

Message ID	32142
Messages	action= backup reason= service-portal msg="System backed up configuration to Management Station per service portal request."
Meaning	The system backed up a configuration file to the management station because the central management server requested it.

Message ID	32142
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= backup status= success msg="Automatic configuration backup to Management Station succeeded"
Meaning	A configuration file was automatically backed up to the mangement station successfully.

Message ID	32142
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= backup msg="User <administrator_name> failed to back up all the logs from {GUI CLI console LCD}"
Meaning	The administrator failed to back up all log files.

32143

Message ID	32143
Log Type	Event Log - Administration Event
Severity	Critical/Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action= loaded-image msg="User <administrator_name> loaded a wrong image from {GUI CLI console LCD}" user=<administrator_name> ui={GUI CLI console LCD} msg="User <administrator_name> changed a policy routing entry."
Meaning	The administrator loaded the wrong image type. The administrator changed the policy routing entry.

32144

Message ID	32144
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} iff=<incoming_interface> src=<ip_address> dst=<ip_address> proto=<protocol_name> ports=<port_range> off=<outgoing_interface> gw=<gateway_ip_address> msg="User <administrator_name> added a policy routing entry"
Meaning	An administrator added a policy routing entry.

32145

Message ID	32145
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} iff=<incoming_interface> src=<ip_address> dst=<ip_address> proto=<protocol_name> ports=<port_range> off=<outgoing_interface> gw=<gateway_ip_address> msg="User <administrator_name> deleted a policy routing entry"
Meaning	An administrator deleted a policy routing entry.

Message ID	32145
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	msg="Found a new connection to <connection_name> (<connection_ip>)"
Meaning	Found a new neighbor.

Message ID	32145
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	msg="Found a new connection to <connection_name> (<connection_ip>)"
Meaning	Lost a neighbor.

32148

Message ID	32148
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI} action=crl-update crl=<crl> msg="User <administrator_name> requested a CRL update from {GUI CLI}"
Meaning	An administrator required a CRL update.

Message ID	32148
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI} action=<action_type> obj=<object> entry=<entry> msg="Administrator <administrator_name> of <location> from {GUI CLI}"
Meaning	The specified administrator changed a configuration.

32149

Message ID	32149
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI} ret=<value> msg="Command failed: <value>. Return code <value>."
Meaning	A command failure occurred.

32150

Message ID	32150
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} msg="User <administrator_name> added protection profile <protection_profile_name>"
Meaning	An administrator has added a new protection profile to the FortiGate unit.

Message ID	32150
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=add msg="User <administrator_name> added new protection profile <protection_profile_name> from {GUI CLI console LCD}"
Meaning	An administrator added a new protection profile.

Message ID	32150
Log Type	Event Log - Administration Event
Severity	Warning
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=password-changed admin-user=<administrator_name> field=password msg="Admin user <administrator_name> changed password of admin user <administrator_name>"
Meaning	An administrator changed the password of another administrator.

32151

Message ID	32151
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=modify msg="User <administrator_name> changed protection profile <protection_profile_name> from {GUI CLI console LCD}"
Meaning	An administrator changed the specified protection profile.

32152

Message ID	32152
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=delete msg="User <administrator_name> deleted protection profile <protection_profile_name> from {GUI CLI console LCD}"
Meaning	An administrator deleted the specified protection profile.

32156

Message ID	32156
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} old_word=<word> old_lang=<language> old_type={wildcard regular expression} old_status={enable disable} new_word=<word> new_lang=<language> new_type={wild card regular expression} new_status={enable disable} msg="User <administrator_name> changed webfilter banned word entry"
Meaning	An administrator changed a webfilter banned word entry.

32157

- An administrator added an antispam banned word entry.
- An administrator added an antispam IP black/white entry.
- An administrator added an antispam trusted ip entry.
- An administrator added a webfilter banned word entry.
- An administrator added a webfilter override entry.
- An administrator added a URL filter entry.
- An administrator deleted an antispam banned word entry.
- An administrator deleted an antispam email black/white entry.
- An administrator deleted an antispam IP black/white entry.
- An administrator deleted an antispam trusted ip entry.
- An administrator deleted a webfilter banned word entry.
- An administrator deleted a webfilter exempt word entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} pattern=<word> status={enable disable} msg="User <administrator_name> added antispam banned word entry <word> from {GUI CLI console LCD}"
Meaning	An administrator added an antispam banned word entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} ip=<ip_address> status={enable disable} msg="User <administrator_name> added antispam IP black/white entry <ip_address> from {GUI CLI console LCD}"
Meaning	An administrator added an antispam IP black/white entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} ip=<ip_address> status={enable disable} msg="User <administrator_name> added antispam trusted ip entry <ip_address> from {GUI CLI console LCD}"
Meaning	An administrator added an antispam trusted ip entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification

Message ID	32157
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} word=<word> lang={western Chinese simplified Chinese traditional Japanese Korean French Thai} pattern_type={wildcard regular expression} status={enable disable} msg="User <administrator_name> added webfilter banned word entry <word> from {GUI CLI console LCD}"
Meaning	An administrator added a webfilter banned word entry.
Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} url=<web_url> user=<user_name> msg="User <administrator_name> added webfilter override entry <web_url> from {GUI CLI console LCD}"
Meaning	An administrator added a webfilter override entry.
Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} url=<web_url> status={enable disable} msg="User <administrator_name> added URL filter entry <web_url> from {GUI CLI console LCD}"
Meaning	An administrator added a URL filter entry.
Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} pattern=<word> status={enable disable} msg="User <administrator_name> deleted antispam banned word entry <word> from {GUI CLI console LCD}"
Meaning	An administrator deleted an antispam banned word entry.
Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} email_patter=<email_address> status={enable disable} msg="User <administrator_name> deleted antispam email black/white entry <email_address> from {GUI CLI console LCD}"
Meaning	An administrator deleted an antispam email black/white entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} ip=<ip_address> status={enable disable} msg="User <administrator_name> deleted antispam IP black/white entry <ip_address> from {GUI CLI console LCD}"
Meaning	An administrator deleted an antispam IP black/white entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} ip=<ip_address> status={enable disable} msg="User <administrator_name> deleted antispam trusted ip entry <ip_address> from {GUI CLI console LCD}"
Meaning	An administrator deleted an antispam trusted ip entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} word=<word> lang={western Chinese simplified Chinese traditional Japanese Korean French Thai} pattern_type={wildcard regular expression} status={enable disable} msg="User <administrator_name> deleted webfilter banned word entry <word> from {GUI CLI console LCD}"
Meaning	An administrator deleted a webfilter banned word entry.

Message ID	32157
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} url=<web_url> status={enable disable} msg="User <administrator_name> deleted URL filter entry <web_url> from {GUI CLI console LCD}"
Meaning	An administrator deleted a webfilter exempt word entry.

32160

Message ID	32160
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} msg="User <administrator_name> changed group <group_name>'s status"
Meaning	An administrator changed the IPS group.

32163

Message ID	32163
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} old_word=<old_word> old_lang={western Chinese simplified Chinese traditional Japanese Korean French Thai} old_pattern_type={wildcard regular expression} old_status={enable disable} new_word=<word> new_lang={western Chinese simplified Chinese traditional Japanese Korean French Thai} new_pattern_type={wild card regular expression} new_status={enable disable} msg="User <administrator_name> changed webfilter exempt word entry <old_word> from {GUI CLI console LCD}"
Meaning	An administrator changed a webfilter exempt word entry.

32164

Message ID	32164
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} word=<word> lang={western Chinese simplified Chinese traditional Japanese Korean French Thai} pattern_type={wildcard regular expression} status={enable disable} msg="User <administrator_name> added webfilter exempt word entry <word> from {GUI CLI console LCD}"
Meaning	An administrator added a webfilter exempt word entry.

32165

Message ID	32165
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} word=<word> lang={western Chinese simplified Chinese traditional Japanese Korean French Thai} pattern_type={wildcard regular expression} status={enable disable} msg="User <administrator_name> deleted webfilter exempt word entry <word> from {GUI CLI console LCD}"
Meaning	An administrator deleted a webfilter exempt word entry.

32170

Message ID	32170
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=config-add status="success" reason="none" msg="User <administrator_name> added multicast firewall policy <policy_name> from {GUI CLI console LCD}" new_id=<value> new_sintf=<source_interface> new_dintf=<destination_interface> new_saddr=<source_ipaddress> new_daddr=<destination_address> new_nat_addr=<ip_address> new_dnat_addr=<destination_ipaddress> new_action=<action_type> new_proto=<protocol> new_start_port=<port_number> new_end_port=<port_number>
Meaning	A multicast firewall policy was added.

Message ID	32170
Log Type	Event Log - Administration Event
Severity	Alert
FortiOS version	4.0
Messages	action=alarm alarm_id=<identification_number> groupid=<group_identification> msg=<log_message_information>
Meaning	An alarm was triggered.

32171

Message ID	32171
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=config-edit status="success" reason="none" msg="User <administrator_name> changed multicast firewall policy <policy_name> from {GUI CLI console LCD}" pol_id=<policy_identification> old_sintf=<source_interface> old_dintf=<destination_interface> old_saddr=<source_ipaddress> old_daddr=<destination_address> old_action=<action_type> old_start_port=<port_number> old_end_port=<port_number> new_sintf=<source_interface> new_dintf=<destination_interface> new_saddr=<source_ipaddress> new_daddr=<destination_address> new_nat_addr=<ip_address> new_dnat_addr=<destination_ipaddress> new_action=<action_type> new_proto=<protocol> new_start_port=<port_number> new_end_port=<port_number>
Meaning	A multicast firewall policy settings changed. .

Message ID	32171
Log Type	Event Log - Administration Event
Severity	Alert
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=alarm-ack alarm_id=<identification_number> actime=<seconds> msg=<log_message_information>
Meaning	An alarm was triggered.

32172

Message ID	32172
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=config-delete status="success" reason="none" msg="User <administrator_name> removed multicast firewall policy <policy_name> from {GUI CLI console LCD}" old_id=<identification> old_sintf=<source_interface> old_dintf=<destination_interface> old_saddr=<source_ipaddress> old_daddr=<destination_address> old_nat_addr=<ip_address> old_nat_addr=<ip_address> old_action=<action_type> old_proto=<protocol> old_start_port=<port_number> old_end_port=<port_number>
Meaning	A multicast firewall policy was removed.

32180

Message ID	32180
Log Type	Event Log - Administration Event
Severity	Error
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=backup status=failure msg="User <administrator_name> failed to backup the configuration from {GUI CLI console LCD} to management station"
Meaning	The administrator failed to back up the configuration file to the management station.

Message ID	32180
Log Type	Event Log - Administration Event
Severity	Error
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} action=backup status=failure msg="Automatic configuration backup to Management Station failed"
Meaning	An automatic back up of a configuration file to the management station failed.

32200

Message ID	32200
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console LCD} upload={url-exempt-list url-block-list word-block-list} num=<value> msg="User <administrator_name> uploaded URL block list from {GUI CLI console LCD}"
Meaning	The administrator has uploaded the new web filter list specified in the 'upload' field.

32545

Message ID	32545
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	user=<none> ui=<none> action=<reboot> msg="System will reboot due to scheduled daily restart."
Meaning	System restart.

32546

Message ID	32546
Log Type	Event Log - Administration Event
Severity	Notification
FortiOS version	4.0
Messages	action=upload_request msg="Content Archive data is being uploaded to FortiAnalyzer"
Meaning	Content archive files are being uploaded to a FortiAnalyzer unit.

Event-System

Event-System log messages record events that occur in the FortiGate system, such as administrators logging in and out, or events occurring on the interfaces.

20001	20058	20101
20002	20059	20200
20031	20060	20201
20032	20061	20202
20033	20062	20203
20034	20063	22000
20035	20064	22001
20036	20065	22002
20037	20066	22004
20038	20067	22005
20039	20068	22006
20040	20069	22009
20041	20070	22010
20042	20071	22100
20043	20072	22101
20044	20073	22102
20045	20074	22103
20046	20075	22800
20047	20076	22801
20048	20077	22802
20049	20078	22803
20050	20079	22911
20051	20080	22912
20052	20081	22913
20053	20082	22914
20054	20083	
20055	20084	
20056	20099	
20057	20100	

20001

- Routing information has changed because the gateway is up/down.
- Problem contacting the modem.
- The FortiGate unit has attempted to redial the IPS from the modem and could not connect after the set number of redial attempts.
- The wireless user has been disconnected.
- Problem contacting the modem.

Message ID	20001
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	interface={ <i>internal external dmz other ...</i> } status={ <i>up down</i> } msg= <i>Ping server is {up down}</i>
Meaning	Routing information has changed because the gateway is up/down.

Message ID	20001
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	modem: unable to open modem device - check hardware
Meaning	Problem contacting the modem.
Action	Verify the modem connections and settings.

Message ID	20001
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	modem: Redial limit exceeded... giving up
Meaning	The FortiGate unit has attempted to redial the IPS from the modem and could not connect after the set number of redial attempts.
Action	Reset the modem to attempt the connection.

Message ID	20001
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	Client < <i>wireless_user</i> > is disassociated.
Meaning	The wireless user has been disconnected.

Message ID	20001
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	modem: unable to open modem device - check hardware

Message ID	20001
Meaning	Problem contacting the modem.
Action	Verify the modem connections and settings.

20002

Message ID	20002
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	user= system ui= system action=<action_type> status= failure msg= “Can’t resolve the IP address of <email_address>”
Meaning	The domain name configured for an alert email recipient cannot be resolved.
Action	Verify the email addresses configured for alert emails.

20031

Message ID	20031
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Interface <interface_name> Out of memory in <memory_sector>
Meaning	The FortiGate flash memory is full in the specified sector.
Action	Delete logs stored to the local disk, perform other maintenance to free memory space.

20032

Message ID	20032
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Interface <interface_name> not found in <memory_sector>
Meaning	The FortiGate unit cannot find the specified interface.
Action	Check configuration of the interface and check any physical connections.

20033

Message ID	20033
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	Using Mobile IPv6 extensions
Meaning	An interface uses Mobile IPv6 extensions

20034

Message ID	20034
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	MinRtrAdvInterval for must be between <start_range_seconds> and <end_range_seconds>
Meaning	The minimum time allowed between sending unsolicited multicast router advertisements from the specified interface (using Mobile IPv6 extensions) must be configured with in the specified range. Range is specified in seconds.
Action	Reconfigure router according to MaxRtrAdvInterval.

20035

Message ID	20035
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	MinRtrAdvInterval for must be between <start_range_seconds> and <end_range_seconds> for <interface_name>
Meaning	The minimum time allowed between sending unsolicited multicast router advertisements from the specified interface must be configured within the specified range. Range is specified in seconds.
Action	Reconfigure router according to MinRtrAdvInterval

20036

Message ID	20036
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	MaxRtrAdvInterval for <interface_name> must be between <start_range_seconds> and <end_range_seconds>
Meaning	The maximum time allowed between sending unsolicited multicast router advertisements from the specified interface, using Mobile IPv6 extensions, must be configured within the specified range. Range is specified in seconds.

20037

Message ID	20037
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	MaxRtrAdvInterval must be between <start_range_seconds> and <end_range_seconds> for <interface_name>

Message ID	20037
Meaning	The maximum time allowed between sending unsolicited multicast router advertisements from the specified interface must be configured within the specified range. Range is specified in seconds.
Action	Reconfigure router according to MaxRtrAdvInterval.

20038

Message ID	20038
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	AdvLinkMTU must be zero or between <start_range_bytes> and <end_range_bytes> for <interface_name>
Meaning	The value placed in MTU options sent by the router must be either zero or between the specified range for the specified interface. A value of zero indicates that no MTU options are sent.
Action	Reconfigure router according to range.

20039

Message ID	20039
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	AdvLinkMTU must be zero or greater than <value_bytes> for <interface_name>
Meaning	The value placed in MTU options sent by the router must be either zero or greater than the specified value for the specified interface. A value of zero indicates that no MTU options are sent.
Action	Reconfigure router according to range.

20040

Message ID	20040
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	AdvReachableTime must be less than <value> for <interface_name>
Meaning	The value to be placed in the Reachable Time field in the Router Advertisement message sent by the router must be less than the specified value for the specified interface. A value of zero means unspecified by this router.
Action	Reconfigure router according to specified value.

20041

Message ID	20041
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	AdvCurHopLimit must not be greater than <value_hop_limit> for <interface_name>
Meaning	The default value to be placed in the CurHopLimit field in the Router Advertisement message sent by the router must not be greater than the specified value for the specified interface.
Action	Reconfigure router according to specified value.

20042

Message ID	20041
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	AdvDefaultLifetime for <interface_name> must be zero or between <start_range_seconds> and <end_range_seconds>
Meaning	The value to be placed in the Router Lifetime field of Router Advertisements sent from the interface in seconds, must be either zero or between the specified range. A value of zero indicates that the router is not to be used as a default router.
Action	Reconfigure router according to specified range.

20043

Message ID	20043
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	HomeAgentLifetime must be between <value> and <value> for <interface_name>
Meaning	HomeAgentLifetime in Router Advertisement packet is out of range.
Action	Reconfigure router according to specified range.

20044

Message ID	20044
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	AdvHomeAgentFlag must be set with HomeAgentInfo
Meaning	AdvHomeAgentFlag and HomeAgentLifetime in Router Advertisement packet must be set with HomeAgentInfo.
Action	Reconfigure router according to specified range.

20045

Message ID	20045
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Invalid prefix length for <string>
Meaning	Prefix length is too long.
Action	Adjust packet prefix length.

20046

Message ID	20046
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	AdvValidLifetime must be greater than AdvPreferredLifetime for <string>
Meaning	The value to be placed in the Valid Lifetime in the Prefix Information option, in seconds, must be greater than the AdvPreferredLifetime.
Action	Adjust packet prefix length.

20047

Message ID	20047
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Can't create socket (AF_INET6): <string>
Meaning	The IPv6 router advertisement daemon failed to create an IPv6 socket.

20048

Message ID	20048
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Setsockopt(IPV6_PKTINFO): <string>
Meaning	The IPv6 router advertisement daemon failed to set IPV6_PKTINFO option.

20049

Message ID	20049
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Setsockopt(IPV6_CHECKSUM): <string>
Meaning	The IPv6 router advertisement daemon failed to set IPV6_CHECKSUM option.

20050

Message ID	20050
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Setsockopt(IPV6_UNICAST_HOPS): <string>
Meaning	The IPv6 router advertisement daemon failed to set IPV6_UNICAST_HOPS option.

20051

Message ID	20051
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Setsockopt(IPV6_MULTICAST_HOPS): <string>
Meaning	The IPv6 router advertisement daemon failed to set IPV6_MULTICAST_HOPS option.

20052

Message ID	20052
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Setsockopt (IPV6_HOPLIMIT): <string>
Meaning	The IPv6 router advertisement daemon failed to set IPV6_HOPLIMIT option.

20053

Message ID	20053
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Setsockopt(ICMPV6_FILTER): <string>
Meaning	The IPv6 router advertisement daemon failed to set ICMPV6_FILTER option.

20054

Message ID	20054
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	radvd receive signal= <value_signal> \n
Meaning	The IPv6 router advertisement daemon received the specified signal and is going to exit.

20055

Message ID	20055
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Can not create query to interface at <string>:<string>:<value>
Meaning	The IPv6 router advertisement daemon cannot create query to interface by using cmf_query_create().

20056

Message ID	20056
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Interfal error in cmf_query_for_each()!
Meaning	The IPv6 router advertisement daemon encounters an internal error when it uses cmf_query_for_each().

20057

Message ID	20057
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Interface <string> : <value> not found in the list!
Meaning	The IPv6 router advertisement daemon failed to find a virtual interface by interface index.

20058

Message ID	20058
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Interface <string> : <value> reloaded! Interface <string> : <value> unloaded!
Meaning	The IPv6 router advertisement daemon reloaded/unloaded the specified interface.

20059

Message ID	20059
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Received packet with no pkt_info!
Meaning	The IPv6 router advertisement daemon received a packet with no pkt_info.

20060

Message ID	20060
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Received icmpv6 packet with invalid length: <value_bytes>
Meaning	The IPv6 router advertisement daemon received an ICMPv6 packet with invalid length.

20061

Message ID	20061
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	icmpv6 filter failed
Meaning	The IPv6 router advertisement daemon received an unwanted type of ICMPv6 packet.

20062

Message ID	20062
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Received icmpv6 RA packet with invalid length. <value_bytes>
Meaning	The IPv6 router advertisement daemon received an ICMPv6 RA packet with invalid length.

20063

Message ID	20063
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Received icmpv6 packet with non-linklocal source address
Meaning	The IPv6 router advertisement daemon received ICMPv6 RA packet with non-linklocal source address..

20064

Message ID	20064
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Received icmpv6 RS packet with invalid length: <value_bytes>
Meaning	The IPv6 router advertisement daemon received ICMPv6 RS packet with invalid length.

20065

Message ID	20065
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Received icmpv6 RS/RA packet with invalid code: <value_code>
Meaning	The IPv6 router advertisement daemon received ICMPv6 RS/RA packet with invalid code.

20066

Message ID	20066
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Received RS or RA with invalid hoplimit <value_hops> from <interface_name>
Meaning	The IPv6 router advertisement daemon received ICMPv6 RS/RA packet with wrong hoplimit.

20067

Message ID	20070
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Our AdvCurHopLimit on <interface_name> doesn't agree with <interface_name>
Meaning	The AdvCurHopLimit on the specified FortiGate interface does not agree with the value on the specified remote interface. A value of zero means unspecified by this router.
Action	Configure the interfaces with the same AdvCurHopLimit value.

20068

Message ID	20068
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Our AdvManagerFlag on <interface_name> doesn't agree with <interface_name>
Meaning	The AdvManagerFlag value (True/False) on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action	Configure the interface with the same AdvManagerFlag value.

20069

Message ID	20069
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Our AdvOtherConfigFlag on <interface_name> doesn't agree with <interface_name>
Meaning	The AdvOtherConfigFlag value (True/False) on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action	Configure the interfaces with the same AdvOtherConfigFlag value.

20070

Message ID	20070
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Our AdvReachableTime on <interface_name> doesn't agree with <interface_name>
Meaning	The AdvReachableTime configured on the specified FortiGate interface does not agree with the value on the specified remote interface. A value of zero means unspecified by this router. The value must be no greater than 3,600,000 seconds or 1 hour.
Action	Configure the interfaces iwth the same AdvReachableTime value.

20071

Message ID	20071
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	our AdvRetransTimer on <interface_name> doesn't agree with <interface_name>
Meaning	The AdvRetransTimer value on the specified FortiGate interface does not agree with the value on the specified remote interface. A value of zero means unspecified (by this router).
Action	Configure the interfaces with the same AdvRetransTimer value.

20072

Message ID	20072
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	trailing garbage in RA on <interface_name> from <interface_name>
Meaning	The IPv6 router advertisement daemon found extra data in an RA packet from the specified source.

20073

Message ID	20073
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	zero length option in RA on <interface_name> from <interface_name>
Meaning	The IPv6 router advertisement daemon found in an RA packet with no option data from the specified source.

20074

Message ID	20074
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	option length greater than total length in RA on <interface_name> from <interface_name>
Meaning	The option length is greater than the total length in an RA packet from the specified source.

20075

Message ID	20075
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	our AdvLinkMTU on <interface_name> doesn't agree with <interface_name>
Meaning	The AdvLinkMTU value on the specified FortiGate interface does not agree with the specified remote interface. A value of zero indicates that no MTU options are sent.
Action	Configure the interfaces with the same AdvLinkMTU value.

20076

Message ID	20076
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	our AdvValidLifetime on <interface_name> for <value> doesn't agree with <interface_name>
Meaning	The AdvValidLifetime value on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action	Configure the interfaces with the same AdvValidLifetime value.

20077

Message ID	20077
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	our AdvPreferredLifetime on <interface_name> for <value> doesn't agree with <interface_name>
Meaning	The AdvPreferredLifetime value on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action	Configure the interfaces with the same AdvPreferredLifetime value.

20078

Message ID	20078
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	Invalid option <value_option> in RA on <interface_name> from <location>
Meaning	The IPv6 router advertisement daemon found the specified invalid option in an RA packet from the specified source from a remote site.

20079

Message ID	20079
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	radvd started\n
Meaning	The IPv6 router advertisement daemon is ready to serve.

20080

Message ID	20080
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	recvmmsg: <string>
Meaning	Recvmmsg() in the IPv6 router advertisement daemon failed.

20081

Message ID	20081
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	received a bogus IPV6_HOPLIMIT from the kernel! len=<value_bytes>, data=<value>
Meaning	The IPv6 router advertisement daemon received a packet with a wrong IPV6_HOPLIMIT.

20082

Message ID	20082
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	received a bogus IPV6_PKINFO from the kernel! len=<value_bytes>, index=<value_index>
Meaning	The wrong IPv6 router advertisement daemon received a packet with a wrong IPV6_PKINFO.

20083

Message ID	20083
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	problem checking all-routers membership on <interface_name>
Meaning	Radvd failed to check if joined the all-routers membership group.

20084

Message ID	20084
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	sendmsg: <string>
Meaning	Sendmsg () in the IPv6 router advertisement daemon failed.

Message ID	20084
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	sendmsg: <string>
Meaning	Sendmsg () in radvd failed.

20090

Message ID	20090
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	int=<interface_name> status=<status_type> msg=\ <i>“interface <interface_name> link status is <status_type>”</i>
Meaning	The interface link status has changed.

20099

Message ID	20099
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	action= <i>interface-stat-change</i> status= <i>DOWN</i> msg=\ <i>“Link monitor: Interface <interface_name> was turned down\”</i> action= <i>interface-stat-change</i> status= <i>UP</i> msg=\ <i>“Link monitor: Interface <interface_name> was turned up\”</i>
Meaning	The interface was turned up and now the status of that interface is UP.

20100

Message ID	20100
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	The FortiGuard Web Filtering category list has been updated. Please verify the protection profile settings are still correct.
Meaning	FortiGuard Web Filtering category has been updated.

20101

Message ID	20101
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	FortiGuard license is expired.
Meaning	FortiGuard license is expired.
Action	Renew FortiGuard license.

Message ID	20101
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0

Message ID	20101
Messages	action=<upload> status=<type_status> file=<file_name> user=<user_name> server=<ip_address> port=<port_name> msg="<file_name> upload reached the <server_ip_address> state <status_name>"
Meaning	Status of the uploaded file.
Message ID	20101
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	action=<upload> error=<type_error> file=<file_name> user=<user_name> server=<ip_address> port=<port_name> msg="<file_name> upload error"
Meaning	File upload error.

20200

Message ID	20200
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI console} action=self-test test=<test_type> msg="Administrator <administrator_name> initiates the <test_type> self-test from"
Meaning	An administrator initiated a self-test type from a specific location.

20201

Message ID	20201
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui={GUI CLI } action=self-test test=all msg="Administrator <administrator_name> initiates all self-tests from <location>"
Meaning	An administrator initiated all self-tests from a specified location.

20202

Message ID	20202
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	action=daemon-startup daemon=<daemon_type> pid=<pid> msg="Daemon <daemon_type> started."
Meaning	The daemon started.

20203

Message ID	20203
Log Type	Event log – System Event
Severity	Information
FortiOS version	4.0
Messages	action= <i>daemon-shutdown</i> daemon=<daemon_type> pid=<pid> msg=" <i>Daemon <daemon_type> shutdown.</i> "
Meaning	The daemon was shut down.

22000

Message ID	22000
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	lengths of packets does not match
Meaning	Packet lengths do not match.

Message ID	22000
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	msg=" <i>Packet length does not match that specified in the request header.</i> "
Meaning	The packet length does not match what is specified in the request header.

22001

Message ID	22001
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	msg=" <i>Protocol version <version_number> is not supported.</i> "
Meaning	The specified version of the protocol is not supported.

22002

Message ID	22002
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Other request <request_type> than http is not supported.
Meaning	Only HTTP is supported.

Message ID	22002
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Other requests <string> than http & ftp is not supported.
Meaning	Requests other than HTTP, HTTPS, FTP, MAIL, and AV are not supported.

Message ID	22002
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	msg=“ Request type <type> is not supported. ”
Meaning	Request other than HTTP, HTTPS, FTP, MAIL, and AV are not supported.

22004

Message ID	22004
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	Socket () failed: <string>
Meaning	The system failed to create a socket or failed to create a HA socket.

22005

Message ID	22005
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	failed to create a <value> /udp socket to receive URL request failed to create a <value> /udp socket to relay URL request
Meaning	The system failed to create a UDP socket to receive URL requests.

22006

Message ID	22006
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	failed to register for cmdb events
Meaning	The system failed to register for cmdb events.

22009

Message ID	22009
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	id={ <i>user_group</i> <i>firewall_policy</i> } status= <i>failure</i> msg= “failed to find its AV protection profile”
Meaning	The specified user group or firewall policy could not find its protection profile.

22010

Message ID	22010
Log Type	Event log – System Event
Severity	Error
FortiOS version	4.0
Messages	process=< <i>string</i> > reason=< <i>string</i> > msg=\“ failed to send urlfilter packet! ”
Meaning	The sendto () failed.

22100

Message ID	22100
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	file=< <i>file_name</i> > size=< <i>integer</i> > limit=< <i>integer</i> > avail=< <i>integer</i> > action= <i>content-archive</i> status= <i>drop</i> reason= <i>memory-limit</i> msg=\“ File <file_name> is not transferred to FortiAnalyzer due to exceeding memory usage limit. ”
Meaning	Quarantine has dropped a FortiAnalyzer transfer job due to limited memory.

Message ID	22100
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	count=< <i>value</i> > duration=< <i>seconds</i> > limit=< <i>value</i> > used=< <i>string</i> > action= <i>content-archive</i> status= <i>drop</i> reason= <i>memory-limit</i> msg=\“ In the past <seconds> seconds, <value> files were not transferred to FortiAnalyzer due to exceeding memory usage limit. ”
Meaning	Quarantine dropped FortiAnalyzer transfer jobs because there was limited available memory.

22101

Message ID	22101
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Messages	file=<file_name> size=<value> limit=<integer> avail=<integer> action= content-archive status= drop reason= memory-limit msg=\ File <file-name> is not transferred to FortiAnalyzer due to exceeding memory usage limit. \
Meaning	Quarantine has dropped a FortiAnalyzer transfer job due to memory limit.

Message ID	22101
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Message	file=<file_name> size=<value> action= content-archive status= fail msg=\ Failed to transfer file <file_name> to FortiAnalyzer <ip_address> \
Meaning	Failed to send a file to the FortiAnalyzer unit.

Message ID	22101
Log Type	Event log – System Event
Severity	Warning
FortiOS version	4.0
Message	file=<file_name> size=<value> action=<action_type> status= fail msg=\ Failed to transfer file <file_name> to FortiAnalyzer <ip_address> \
Meaning	Failed to send a file to the FortiAnalyzer unit.

22102

Message ID	22102
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	msg=\ Log disk failure is imminent, logs should be backed up \
Meaning	Erroneous SMART status

22103

Message ID	22103
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	reason= buffer-overflow msg= “ FortiGuard Analysis Service buffer is reset due to a buffer overflow (system overload). Some log data may be lost. ”
Meaning	The FortiGuard log buffer was reset because of a system overload. Current log data and possibly old log data may be lost.
Action	Reopen FortiGuard log pipe.

22800

Message ID	22800
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	service=<name> mode=<string> msg= “ The system has <value> session fail mode ”
	service=<name> conserve= on total=<value> free=<value> entermargin=<value> exitmargin=<value> msg= “ The system has entered conserve mode ”
Meaning	Scan services session fail mode.
	Scan services entered conserve mode.

22801

Message ID	22801
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	service=<value> conserve= on total=<value> free=<value> entermargin=<value> exitmargin=<value> msg= “ The system exited conserve mode ”
Meaning	The system exited conserve mode.

22802

Message ID	22802
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	service=<value> sysconserve= on total=<value> free=<value> entermargin=<value> exitmargin=<value> msg= “ The system has entered conserve mode ”
Meaning	System services entered conserve mode.

22803

Message ID	22803
Log Type	Event log – System Event
Severity	Critical
FortiOS version	4.0
Messages	service=<value> sysconserve= exit total=<value> free=<value> entermargin=<value> exitmargin=<value> msg= “The system exited conserve mode”
Meaning	System services exited conserve mode.

22911

Message ID	22911
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	server={ Home Alter } action= up msg= “FortiGuard Analysis Service {Home Alter} server is up”
Meaning	The FortiGuard Analysis Service server is up.

22912

Message ID	22912
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	server={ Home Alter } action= down msg= “FortiGuard Analysis Service {Home Alter} server is down”
Meaning	The FortiGuard Analysis Service server is down.

22913

Message ID	22913
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	server={ Home Alter } action= disconnect msg= “FortiGuard Analysis Service {Home Alter} server is disconnected”
Meaning	The FortiGuard Analysis Service server has been disconnected.

22914

Message ID	22914
Log Type	Event log – System Event
Severity	Notification
FortiOS version	4.0
Messages	server={ <i>Home Alter</i> } action= <i>change</i> msg= <i>"FortiGuard Analysis Service server is changed to {Home Alter}"</i>
Meaning	The FortiGuard Analysis Service server was changed to "disable" on the FortiGuard Analysis and Management Service portal web site.

Event-DHCP service

Event-DHCP service log messages record DHCP service events.

26001

Message ID	26001
Log Type	Event log – DHCP service event
Severity	Error
FortiOS version	4.0
Messages	dhcp_msg=<string> dir=<string> mac=<mac_address 2X> ip=<ip_address> lease=<string> hostname=<name> msg=<log_message_information>
Meaning	DHCP request and response log.

26002

Message ID	26002
Log Type	Event log – DHCP service event
Severity	Error
FortiOS version	4.0
Messages	No shared network for network <interface_name> (ip_address) Address range <ip_address> to <ip_address>, netmask <netmask_address> spans <string>! Address range <ip_address> to <ip_address> netmask <netmask_address> not on net <string>!
Meaning	No shared network found. The IP address range spans multiple subnets. The IP address range doesn't belong to the net.

Event-Firewall authentication

Event-Firewall authentication log messages record authentication events that occur within the FortiGate firewall.

38001

38002

38010

38012

38012

38001

Message ID	38001
Log Type	Event Log - Firewall Authentication
Severity	Notification
FortiOS version	4.0
Messages	ipproto=<protocol> src=<source_address> dst=<destination_address> adgroup=<group_name> user=<user_name> ui={GUI CLI console} action=FSAE-auth status=success msg=\'AD group <group_name> user <administrator_name> succeeded in authentication.\'
Meaning	The specified administrator succeeded in authentication.

Message ID	38001
Log Type	Event Log - Firewall Authentication
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> group=<group_name> ui={GUI CLI console} action=authenticate status=success msg="User <administrator_name> succeeded in authentication."
Meaning	The specified administrator succeeded in authentication.

Message ID	38001
Log Type	Event Log - Firewall Authentication
Severity	Notification
FortiOS version	4.0
Messages	adgroup=<group_name> user=<user_name> group=<group_name> ui={GUI CLI console} action=NTLM-auth status=failure reason=<string> msg=\'AD domain <virtual domain_name> user<administrator_name> failed in authentication.\'
Meaning	The specified administrator failed to authenticate in the specified AD virtual domain.

Message ID	38001
Log Type	Event Log - Firewall Authentication
Severity	Notification
FortiOS version	4.0
Messages	adgroup=<group_name> user=<user_name> group=<group_name> ui={GUI CLI console} action=NTLM-auth status=success msg=\'AD group<group_name> user<administrator_name> succeeded in authentication.\'
Meaning	The specified administrator succeeded in authentication.

38002

Message ID	38002
Log Type	Event Log - Firewall Authentication
Severity	Warning
FortiOS version	4.0
Messages	user=<user_name> service=<service_type> action=authenticate status=timeout reason=timeout src=<source_address> srcname=N/A dst=<destination_address> dstname=N/A msg="User failed to authenticate within the allowed period"
Meaning	The user failed to get authenticated within a specified time period.

Message ID	38002
Log Type	Event Log - Firewall Authentication
Severity	Notification
FortiOS version	4.0
Messages	ipproto=<protocol> src=<source_address> dst=<destination_address> adgroup=<group_name> user=<user_name> ui={GUI CLI console} action=FSAE-auth status=failure reason=<string> msg="AD group <group_name> user <administrator_name> failed in authentication"
Meaning	The user failed to get authenticated.

Message ID	38002
Log Type	Event Log - Firewall Authentication
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} action=authenticate status=failure msg="User <administrator_name> failed in authentication"
Meaning	The specified administrator failed in authenticating the session.

38003

Message ID	38003
Log Type	Event Log - Firewall Authentication
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} action=authenticate status=lockout msg="User at <ip_address> failed authentication too many times."
Meaning	The specified administrator failed authentication and is locked out because they tried too many times.

38010

Message ID	38010
Log Type	Event Log - Authentication Event
Severity	Alert
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} action=encryption cipher=aes-128-cbc status=failed msg="EVP encryption failed"
Meaning	The EVP encryption failed.

38011

Message ID	38011
Log Type	Event Log - Authentication Event
Severity	Warning
FortiOS version	4.0
Messages	initiator=<initiator> status=failure reason=table_add_failed src=<source_address> dst=<destination_address> msg="FortiGuard Web Filtering override table is full."
Meaning	The FortiGuard Web Filtering table is full.

Message ID	38011
Log Type	Event Log - Authentication Event
Severity	Alert
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} action=decryption cipher=aes-128-cbc status=failed msg="EVP decryption failed"
Meaning	The EVP decryption failed.

38012

Message ID	38012
Log Type	Event Log - Authentication Event
Severity	Notification
FortiOS version	4.0
Messages	initiator=<user_name> status=success reason=none src=<source_address> dst=<destination_address> action=authentication scope=<override_scope> scope_data=<scope_description> rule_type=<rule_type> rule_data=<rule_data> offsite=<url_address> expiry=<override_time_message> msg="User <user_name> added webfilter override entry <entry_name> from <location>"
Meaning	A FortiGuard Web Filtering override was successfully created.

38020

Message ID	38020
Log Type	Event Log - Authentication Event
Severity	Notification
FortiOS version	4.0
Messages	ipproto=< protocol > src=< source_address > dst=< destination_address > action= deny reason= forticlient check error=< string > cookie=< cookie_name > msg=< log_message_information >
Meaning	Checking for FortiClient failed.

Event-Chassis

Event-Chassis log messages record chassis events for the FortiGate-5000 series and higher.

[99503](#)

[99504](#)

[99505](#)

[99506](#)

[99507](#)

[99508](#)

[99509](#)

99503

Message ID	99503
Log Type	Event Log - Chassis
Severity	Variable (Warning or Critical)
FortiOS version	4.0
Messages	Chassis fan anomaly: Fan <fan_integer> , <rpm_integer> RPM
Meaning	A chassis fan is operating at an RPM value outside of the normal operating range, <fan_integer> is the number of the fan tray. For the FortiGate-5140, <fan_integer> can be 0, 1 or 2. The FortiGate-5050 has only one fan tray, <rpm_integer> is the RPM value that the fan is operating at.

99504

Message ID	99504
Log Type	Event Log - Chassis
Severity	Variable (Warning or Critical)
FortiOS version	4.0
Messages	Chassis temperature anomaly: T <sensor_integer> , <temp_integer> Celsius
Meaning	A temperature sensor has reported a temperature outside of the normal operating range for this sensor. A typical operating range is between 10 and 75 degrees Celsius. <temp_integer> identifies the temperature sensor <temp_integer> is the temperature being reported by the sensor.

99505

Message ID	99505
Log Type	Event Log - Chassis
Severity	Variable (Warning or Critical)
FortiOS version	4.0
Messages	Chassis voltage anomaly: V3.3, <monitored_voltage> V Chassis voltage anomaly: V5, <monitored_voltage> V Chassis voltage anomaly: V12, <monitored_voltage> V
Meaning	A chassis voltage sensor has detected a voltage level outside of the operating range for the sensor.

99506

Message ID	99506
Log Type	Event Log - Chassis
Severity	Variable (Warning or Critical)
FortiOS version	4.0
Messages	Blade fan anomaly: Blade <rpm_integer> RPM
Meaning	A blade fan is operating at an RPM value outside of the normal operating range.

99507

Message ID	99507
Log Type	Event Log - Chassis
Severity	Variable (Warning or Critical)
FortiOS version	4.0
Messages	Blade temperature anomaly: Blade <temp_integer> Celsius
Meaning	A temperature sensor on a FortiGate-5000 or FortiSwitch-5000 series module has reported a temperature outside of the normal operating range for this sensor.

99508

Message ID	99508
Log Type	Event Log - Chassis
Severity	Variable (Warning or Critical)
FortiOS version	4.0
Messages	Blade voltage anomaly: Blade <monitored_voltage> V
Meaning	A blade voltage anomaly.

99509

Message ID	99509
Log Type	Event Log - Chassis
Severity	Variable (Warning or Critical)
FortiOS version	4.0
Messages	chassisd failed to create the cmd pipe: mkfifo(CHASSIS_CMD_PIPE_NAME) <name>
	chassisd failed to open the cmd pipe: open(CHASSIS_CMD_PIPE_NAME) <name>
	chassisd failed to create the shared memory segment: shgment(CHASSIS_STATUS_SHM_KEY) <name>
	chassisd failed to create the shared memory segment: shmat(CHASSIS_STATUS_SHM_KEY) <name>
Meaning	As indicated. Software errors may prevent proper system monitoring.
Action	Reboot the FortiGate blade

Event-IPSec negotiation

Event-IPSec negotiation log messages record IPSec activities and events.

23002

23004

23005

23007

23008

23009

23011

23011

23012

23002

Message ID	23002
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> action=negotiate init=<string> mode={aggressive main} stage=<value_ipsec_stage> dir={inbound outbound} status={success failure} msg="<log_message_information>"
Meaning	IPSec generic negotiation report.

Message ID	23002
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<string> action=negotiate user=<user_name> group=<group_name> status=<string> msg="<log_message_information>"
Meaning	IPSec generic negotiation report.

23004

Message ID	23004
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<cookie_name> action=negotiate init=<string> mode={aggressive main} stage=<value_ipsec_stage> dir={inbound outbound} status={success failure} msg="<log_message_information>"
Meaning	IPSec generic negotiation progress report.

23005

Message ID	23005
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> msg="<log_message_information>"
Meaning	IPSec generic negotiation report.

23007

Message ID	23007
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<string> action=delete_phase1_sa user=<user_name> group=<group_name> xauth_user=<user_name> xauth_group=<group_name> msg="<log_message_information>"
Meaning	IPSec generic negotiation report.

23008

Message ID	23008
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<string> action=delete_ipsec_sa enc_spi=<value> dec_spi=<value> user=<user_name> group=<group_name> xauth_user=<user_name> xauth_group=<group_name> msg="<log_message_information>"
Meaning	IPSec generic negotiation report.

23009

Message ID	23009
Log Type	Event log – IPSec Negotiation
Severity	Variable
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<string> action=error user=<user_name> group=<group_name> xauth_user=<user_name> xauth_group=<group_name> status=esp_error error_num=<value> spi=<value>08x seq=<value>08x msg="<log_message_information>"
Meaning	IPSec generic negotiation report.

23008

Message ID	23008
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<cookie_name> action=delete_phase1_sa spi=<string>1x desc_spi=<string>1x msg="delete ipsec sa"
Meaning	Deleted IPSec SA.

Message ID	23008
Log Type	Event log – IPSec Negotiation
Severity	Notification
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<cookie_name> action=delete_ipsec_sa enc_spi=<string> dec_spi=<string>1x msg=<log_message_information>
Meaning	Deleted IPSec SA.

23009

Message ID	23009
Log Type	Event log – IPSec Negotiation
Severity	Variable
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<cookie_name> action=error status=esp_error error_num=<error_number> spi=<Value_index>08x msg=<log_message_information> loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<cookie_name> action=error status=esp_error error_num=<error_number> spi=<integer>08x msg=<log_message_information>
Meaning	IPSec ESP packet error report.

Message ID	23009
Log Type	Event log – IPSec Negotiation
Severity	Variable
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<cookie_name> action=error status=esp_error error_num=<error_number> spi=<integer>08x seq=<integer>08x msg=<log_message_information>
Meaning	IPSec ESP packet error report.

Message ID	23009
Log Type	Event log – IPSec Negotiation
Severity	Variable
FortiOS version	4.0
Messages	loc_ip=<ip_address> loc_port=<port_number> rem_ip=<ip_address> rem_port=<port_number> out_if=<string> vpn_tunnel=<vpn_name> cookies=<cookie_name> action=error user=<administrator-name> group=<group_name> status=esp_error error_num=<error_number> spi=<integer>08x seq=<integer>08x msg=<log_message_information>
Meaning	IPSec ESP packet error report.

23011

Message ID	23011
Log Type	Event log – IPSec Negotiation
Severity	Variable
FortiOS version	4.0
Messages	loc_ip=< <i>ip_address</i> > loc_port=< <i>port_num</i> > rem_ip=< <i>ip_address</i> > rem_port=< <i>port_num</i> > out_if=< <i>string</i> > vpn_tunnel=< <i>vpn_name</i> > cookies=< <i>cookie_name</i> > action= <i>dpd</i> status= <i>dpd_failure</i> msg="IPSec connection failure"
Meaning	IPSec connection failure.

Message ID	23011
Log Type	Event log – IPSec Negotiation
Severity	Variable
FortiOS version	4.0
Messages	loc_ip=< <i>ip_address</i> > loc_port=< <i>port_number</i> > rem_ip=< <i>ip_address</i> > rem_port=< <i>port_number</i> > out_if=< <i>string</i> > vpn_tunnel=< <i>vpn_name</i> > cookies=< <i>cookie_name</i> > action= <i>dpd</i> user=< <i>administrator_name</i> > group=< <i>group_name</i> > status= <i>dpd_failure</i> msg="IPSec connection failure"
Meaning	IPSec connection failure.

23012

Message ID	23012
Log Type	Event log – IPSec Negotiation
Severity	Variable
FortiOS version	4.0
Messages	loc_ip=< <i>ip_address</i> > loc_port=< <i>port_number</i> > rem_ip=< <i>ip_address</i> > rem_port=< <i>port_number</i> > out_if=< <i>string</i> > vpn_tunnel=< <i>vpn_name</i> > cookies=< <i>cookie_name</i> > action= <i>tunnel</i> user=< <i>administrator_name</i> > group=< <i>group_name</i> > msg="< <i>log_message_information</i> >"
Meaning	IPSec tunnel status changed.

Event-L2TP/PPP/PPPoE

Event-L2TP/PPP/PPPoE log messages record events and activities that occur with the internet and modem protocols, L2TP, PPP, and PPPoE.

29001	30005
29002	30006
29003	30007
29004	30008
29009	30009
29011	31004
29012	31005
29013	31006
29014	31007
29015	31008
29016	31009
29022	
29024	
30004	

29001

Message ID	29001
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> local=<ip_address> remote=<ip_address> assigned=<ip_address> stat=<string> msg="<log_message_information>"
Meaning	PPPd log message.

29002

Message ID	29002
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> local=<local_ip_address> remote=<remote_ip_address> assigned=<ip_address> action=auth_success msg="User <user_name> using <auth> with authentication protocol <protocol_information>"
Meaning	PPPD authentication is a success.

29003

Message ID	29003
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> local=<local_ip_address> remote=<remote_ip_address> assigned=<ip_address> action=auth_failed msg="<user_name> is trying to connect using <auth> with authentication protocol <protocol_information>"
Meaning	PPPD authentication failed.

29004

Message ID	29004
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Warning
FortiOS version	4.0
Messages	status=failure action=connect msg="PPTP: the maximum number of connections has been reached. No more clients can connect."
Meaning	The maximum number of PPTP connections has been reached.

29009

Message ID	29009
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Notification
FortiOS version	4.0
Messages	gateway_ip=<ip_address> assigned_ip=<ip_address> mtu=<value_bytes> msg=\' PPPoE status report \'
Meaning	A PPPoE status report.

29011

Message ID	29011
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Error
FortiOS version	4.0
Messages	Can't execute <program_name>: <string>
Meaning	PPPd cannot execute the specified program.

29012

Message ID	29012
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Error
FortiOS version	4.0
Messages	<string>
Meaning	PPPd has received the specified wrong option.

29013

Message ID	29013
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Notification
FortiOS version	4.0
Messages	msg=\' pppd is started \'
Meaning	PPPd is started

29014

Message ID	29014
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Information
FortiOS version	4.0
Messages	pppd is exiting
Meaning	PPPd is exiting.

29015

Message ID	29015
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Error
FortiOS version	4.0
Messages	Peer IP is the same as an interface IP <i><string></i> . IP <i><ip_address></i>
Meaning	PPP has received bad options.

29016

Message ID	29016
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Error
FortiOS version	4.0
Messages	Local IP is the same as an interface IP <i><string></i> . IP <i><ip_address></i>
Meaning	PPP has received bad options.

29022

Message ID	29022
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Warning
FortiOS version	4.0
Messages	status= <i>failure</i> action= <i>connect</i> msg=\ <i>“PPTP: No IP addresses left to assign in virtual domain: <ip_address>”</i>
Meaning	No IP addresses are available.

29024

Message ID	29024
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Warning
FortiOS version	4.0
Messages	status= <i>failure</i> action= <i>start</i> msg=\ <i>“failed to expand pptp config list due to not enough memory”</i>
Meaning	Not enough memory.

30004

Message ID	30004
Log Type	Event log – L2TP/PPTP/PPPOE
Severity	Variable
FortiOS version	4.0
Messages	msg= <i><log_message_information></i>
Meaning	PPTP log message.

Message ID	30004
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Warning
FortiOS version	4.0
Messages	action= start status= success msg=\“ PPTPD: started successfully \”
Meaning	PPPTPD start

30005

Message ID	30005
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Error
FortiOS version	4.0
Messages	action= start status= failure reason=\“ failed to create socket \” msg=\“ PPTPD failed to start because failed to create socket \”
Meaning	PPPTPD failed to start.

30006

Message ID	30006
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Notification
FortiOS version	4.0
Messages	action= exit status= success msg=\“ PPTPD exited successfully \”
Meaning	PPPTPD exited successfully.

30007

Message ID	30007
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Error
FortiOS version	4.0
Messages	action= disconnect status= success reason=\“ PPTP setting is changed \” msg=\“ PPTPD closed all client connections in vdom <vdom_name> because PPTP setting was changed. \”
Meaning	All PPTPD connections were closed because the PPTP setting changed.

Message ID	30007
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Error
FortiOS version	4.0
Messages	action= disconnect status= success reason=\“ failed to find the interface by device index \” msg=\“ PPTPD closed all client connections in vdom <vdom_name> because failed to find the interface by device index. \”
Meaning	The PPTPD disconnected.

30008

Message ID	30008
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Information
FortiOS version	4.0
Messages	action= connect status= success msg=\“ Client <ip_address> control connection started \”
Meaning	PPTPD client connection.

30009

Message ID	30009
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Information
FortiOS version	4.0
Messages	action= disconnect status= success msg=\“ Client <client_name> control connection finished \”
Meaning	PPTPD client disconnected.

31004

Message ID	31004
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Variable
FortiOS version	3.0(MR1 and up)
Messages	msg= <log_message_information>
Meaning	L2TP log message.

31005

Message ID	31005
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Notification
FortiOS version	3.0(MR5 and up)
Messages	action= exit status= success msg=\“ L2TPD exited successfully \”
Meaning	L2TPD successfully exited.

31006

Message ID	31006
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Information/Warning
FortiOS version	3.0(MR5 and up)
Messages	action= disconnect status= success reason=\“ L2TP setting changed \” msg=\“ L2TPD closed all client connections in vdom <vdom_name> because L2TP setting was changed \”
	action= disconnect status= success reason=\“ interface not found \” msg=\“ L2TPD closed all client connections in vdom <vdom_name> because failed to find interface by device index \”
Meaning	L2TP closed all client connections in a specified vdom because L2TP setting was changed.
	L2TP closed all client connections in a specified vdom because failed to find interface by device index.

31007

Message ID	31007
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Warning
FortiOS version	3.0(MR5 and up)
Messages	action= connect status= failure reason=\“ no ip available \” msg=\“ No IP addresses left to assign in virtual domain <vdom_name> \”
Meaning	There are no more available IP addresses to assign in the VDOM.

31008

Message ID	31008
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Information
FortiOS version	3.0(MR5 and up)
Messages	action= connect status= success msg=\“ Client <client_name> control connection started (<ip_address>), assigned ip <ip_address> \”
Meaning	L2TP client connection is started.

31009

Message ID	31009
Log Type	Event log - L2TP/PPTP/PPPoE
Severity	Information
FortiOS version	3.0(MR5 and up)
Messages	action= disconnect status= success msg=\“ Client <ip_address> control connection (<ip_address>) finished \”
Meaning	L2TP client connection has finished.

Event-SSLVPN

Event SSL-VPN log messages record SSL-VPN user, administration and session events.

99601	99827
99602	99840
99603	99841
99604	99842
99703	99843
99705	99844
99706	
99707	
99709	
99805	
99806	
99807	
99808	
99809	
99810	
99811	
99812	
99820	
99825	
99826	

99601

Message ID	99601
Log Type	Event Log – SSL VPN user
Severity	Information
FortiOS version	4.0
Messages	<p>user=<administrator_name> rip=<reserved_ip_address> action=login status=success reason=none msg="User <administrator_name> login successfully from <location>"\</p> <p>user=<user_name> rip=<reserved_ip_address> action=login status=failure reason=hostcheck msg="User <user_name> login failed from <location>"</p>
Meaning	<p>An SSL-VPN web access user has logged into the system successfully.</p> <p>An SSL-VPN web access user has logged into system, but host check has failed.</p>

99602

Message ID	99602
Log Type	SSL-VPN Log – SSL VPN user
Severity	Information
FortiOS version	4.0
Messages	user=<user_name> rip=<reserved_ip_address> action=login status=failure reason=<reason> msg="User <user_name> login failed from <location>"
Meaning	An SSL-VPN web access user failed to log in too many times.

99603

Message ID	99603
Log Type	SSL-VPN Log – SSL VPN user
Severity	Information
FortiOS version	4.0
Messages	user=<user_name> rip=<reserved_ip_address> action=logout status=success reason=none msg="User <user_name> logout successfully from <location>"
Meaning	An SSL-VPN web access user has logged out of the system successfully.

99604

Message ID	99604
Log Type	SSL-VPN Log – SSL VPN user
Severity	Information
FortiOS version	4.0
Messages	user=<user_name> rip=<reserved_ip_address> action=logout status=success reason=timeout msg="SSL VPN web access session timeout from <location>"
Meaning	An SSL-VPN web access session is discarded because of inactivity.

99703

Message ID	99703
Log Type	SSL-VPN Log – SSL VPN administrator
Severity	Information
FortiOS version	4.0
Messages	action= <i>info</i> user=<administrator_name> ui=<user_interface> msg="User <administrator_name> changed SSL setting from <location>"
Meaning	The specified administrator updated the SSL configuration.

99705

Message ID	99705
Log Type	SSL-VPN Log – SSL VPN administrator
Severity	Information
FortiOS version	4.0
Messages	action= <i>info</i> user=<administrator_name> ui=<user_interface> msg="A CA certificate is loaded from <location>" action= <i>info</i> user=<administrator_name> ui=<user_interface> msg="A REMOTE certificate is loaded from <location>"
Meaning	The specified administrator loaded a CA certificate. A REMOTE certificate was loaded.

99706

Message ID	99706
Log Type	SSL-VPN Log – SSL VPN administrator
Severity	Information
FortiOS version	4.0
Messages	action= <i>info</i> user=<administrator_name> ui=<user_interface> msg="A CA certificate is removed from <location>" action= <i>info</i> user=<administrator_name> ui=<user_interface> msg="A REMOTE certificate is removed from <location>"
Meaning	The specified administrator loaded a local certificate. A REMOTE certificate was removed.

99707

Message ID	99707
Log Type	SSL-VPN Log – SSL VPN administrator
Severity	Information
FortiOS version	4.0
Messages	action= <i>info</i> user=<administrator_name> ui=<user_interface> msg="A Local Certificate is loaded from <location>"
Meaning	The specified administrator loaded a local certificate.

99708

Message ID	99708
Log Type	SSL-VPN Log – SSL VPN administrator
Severity	Information
FortiOS version	4.0
Messages	action= <i>info</i> user=<administrator_name> ui=<user_interface> msg=“ A Local Certificate is removed from <location> ”
Meaning	A local certificate was removed from a specified location by a specified user.

99709

Message ID	99709
Log Type	SSL-VPN Log – SSL VPN administrator
Severity	Information
FortiOS version	4.0
Messages	action= <i>info</i> user=<administrator_name> ui=<user_interface> msg=“ A CRL is loaded from <location> ”
Meaning	The specified administrator loaded a Certificate Revocation List (CRL).

99710

Message ID	99710
Log Type	SSL-VPN Log – SSL VPN administrator
Severity	Information
FortiOS version	4.0
Messages	action= <i>crl-update</i> status= <i>success</i> crl=<crl_name> method=<method_type> msg= “ CRL <crl_name> is updated with <string> ”
Meaning	A CRL is updated.

99805

Message ID	99805
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= <i>success</i> ui=<user_interface> status= <i>success</i> msg=“ Certificate Verified from <location> ”
Meaning	An SSL certificate has been verified.

99806

Message ID	99806
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= start ui=<user_interface> status= success msg= “New SSL VPN tunnel <location>”
Meaning	A new SSL-VPN tunnel is successfully established.

99807

Message ID	99807
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= stop ui=<user_interface> status= success msg= “Tunnel <tunnel_name> timeout from <location>”
Meaning	The SSL-VPN tunnel has timed out.

99808

Message ID	99808
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= stop ui=<user_interface> status= success msg= “STOP SSL VPN Tunnel <tunnel_name> from <location>”
Meaning	The SSL-VPN tunnel was closed.

99809

Message ID	99809
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= start ui=<user_interface> status= success msg= “New SSL web Application <app_name> from <location>”
Meaning	A new SSL web application was started.

99810

Message ID	99810
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= stop ui=<user_interface> status= success msg= “STOP SSL Web Application <app_name> from <location>”
Meaning	An SSL web application was closed.

99811

Message ID	99811
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= block ui=<user_interface> status= block msg= “SSL Web Application <app_name> from <location> Blocked”
Meaning	An SSL web application could not be used because it was blocked.

99812

Message ID	99812
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= stop ui=<user_interface> status= success msg= “Web Application <app_name> from <location> timeout”
Meaning	An SSL-VPN web application has timed out.

99820

Message ID	99820
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	msg= “Unknown TAG is read <tag_value>.”
Meaning	An unknown packet with the specified tag value was received.

99825

Message ID	99825
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	msg=“ <i>Client type <packet_type> <content></i> .”
Meaning	An unknown control packet was received with the specified type and content.

99826

Message ID	99826
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	msg=“ <i>Client Certification Validation error code <error_code></i> ”
Meaning	A “certificate validation” packet is received with returned error code.

99827

Message ID	99827
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	msg=“ <i>Client Having Antivirus <content_value></i> ”
Meaning	A “checking antivirus” control packet is received with the specified packet content value.

99840

Message ID	99840
Log Type	SSL-VPN Log – SSL VPN session
Severity	Error
FortiOS version	4.0
Messages	action= <i>alert</i> ui= <i><remote_ip></i> msg=“ <i>SSL Error Alerts from <remote_ip> <warning_type> <warning_reason></i> ”
Meaning	Two SSL peers exchanged alert messages. The peers can decide what action to follow.

99841

Message ID	99841
Log Type	SSL-VPN Log – SSL VPN session
Severity	Error
FortiOS version	4.0
Messages	action= <i>exit</i> ui=<remote_ip> msg="SSL Exit Error: from <remote_ip> <state_of_SSL_connection>"
Meaning	An error occurred in the SSL connection.

99842

Message ID	99842
Log Type	SSL-VPN Log – SSL VPN session
Severity	Error
FortiOS version	4.0
Messages	action= <i>fail</i> ui=<remote_ip> msg="SSL Fail Error: from <remote_ip> <state_of_SSL_connection>"
Meaning	A failure error occurred in the SSL connection.

99843

Message ID	99843
Log Type	SSL-VPN Log – SSL VPN session
Severity	Information
FortiOS version	4.0
Messages	action= <i>new</i> ui=<remote_ip> msg="SSL New Connection: from <remote_ip> <state_of_SSL_connection>"
Meaning	A new SSL connection was created.

99844

Message ID	99844
Log Type	SSL-VPN Log – SSL VPN session
Severity	Warning
FortiOS version	4.0
Messages	action= <i>warning</i> ui=<remote_ip> msg="SSL Warning: from <remote_ip> <warning_type> <warning_reason>"
Meaning	Two SSL peers exchanged warning messages. The peers can decide what action to follow.

Event-VIP SSL

Event-VIP SSL log messages record VIP activities.

45001
45003
45005
45007
45009
45011
45012
45013
45015
45017
45019
45023
45027
45029
45031

45001

Message ID	45001
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive expected=<handshake_type> received=<handshake_type> msg="Incorrect SSL handshake message"
Meaning	An SSL received an incorrect handshaking message. The handshake type in the expected log field can be one of the following: 0=HelloRequest 1=ClientHello 2=ServerHello 4=NewSessionTicket 11=Certificate 12=ServerKeyExchange 13=CertificateRequest 14=ServerHelloDone 15=CertificateVerify 16=ClientKeyExchange 20=Finished The received log field can be any one of the above, especially if the record is corrupted.

45003

Message ID	45003
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close handshake=<handshake_type> msg="Bad length in SSL handshake"
Meaning	An SSL handshake message has a bad length.

45005

Message ID	45005
Log Type	Event-Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg=\ <i>“RSA verification of Diffie-Hellman parameters failed”</i>
Meaning	An RSA verification of Diffie-Hellman parameters failed.

45007

Message ID	45007
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> local=<local_hash_value> remote=<remote_hash_value> action=close msg=\ <i>“Hash in SSL Finished does not match calculated hash”</i>
Meaning	A Hash in the SSL Finished does not match the calculated hash. Each hash value in the local and remote log fields are hex encoded.

45009

Message ID	45009
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close reason=<reason_id> msg=\ <i>“SSL decryption failure”</i>
Meaning	The SSL decryption failed. The reason log field contains one of the following: <ul style="list-style-type: none"> • status_bad_pad_len=1 – indicates that the received SSL Record did not comply with RFC 4336 section 6.2.3.2 on padding_length • status_bad_pad_value=2 – indicates that the received SSL Record did not comply with RFC 4346 section 6.2.3.2 on padding • status_bad_mac=3 – indicates that the MAC in the received SSL Record did not match the MAC calculated by the FortiGate for that SSL Record. • status_internal_error=4 – indicates that there was an internal error

45011

Message ID	45011
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close min-minor=<value> recv-minor=<value> msg=\ <i>“SSL minor below minimum configured value”</i>
Meaning	An SSL minor version is below the configured minimum value.

45012

Message ID	45012
Log Type	Event Log – VIP SSL
Severity	Warning
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg=\ <i>“SSL maximum connections reached”</i>
Meaning	The SSL maximum connection limit was reached.

45013

Message ID	45013
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg=\ <i>“None of the offered CipherSuites are supported”</i>
Meaning	None of the offered SSL CipherSuites are supported.

45015

Message ID	45015
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive len=<value> msg=\ <i>“Incorrect SSL handshake length”</i>
Meaning	The SSL handshake has an invalid length.

45017

Message ID	45017
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive handshake=<handshake> len=<value> max=<maximum_value> msg= “SSL Handshake too long”
Meaning	The SSL handshake was too long.

45019

Message ID	45019
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=send level=<alert_level> desc=<alert_desc> msg= “SSL Alert sent”
Meaning	<p>An SSL alert was sent. The levels are 1=warning, and 2=fatal. The desc log field contains the following:</p> <ul style="list-style-type: none"> • fts_alert_desc_close_notify=0 – notifies the recipient that the sender will not send any more messages on this connection • fts_alert_desc_unexpected_message=10 – an inappropriate message was received; this is usually fatal and should be observed closely • fts_alert_desc_bad_record_mac=20 – is returned if a record is received with an incorrect MAC • fts_alert_desc_decryption_failed=21 – may be returned if a TLSCiphertext decrypted in an invalid way; either it wasn't an even multiple of the block length or its padding values, when checked, were not correct (always fatal) • fts_alert_desc_record_overflow=22 – a TLSCiphertext record was received that had a length more than 2¹⁴+2048 bytes, or a record decrypted to a TLSCompressed record with more than 2¹⁴+1024 bytes (always fatal) • fts_alert_desc_handshake_failure=40 – indicates the sender was unable to negotiate an acceptable set of security parameters given the options available (fatal error) • fts_alert_desc_no_certificate=41 – indicates there is no available certificate • fts_alert_desc_illegal_parameter=47 – a field in the handshake was out of range or inconsistent with other fields (always fatal) • fts_alert_desc_record_error=50 – a message could not be decoded because some field was out of the specified range or the length of the message was incorrect (always fatal) • fts_alert_desc_decrypt_error=51 – a handshake cryptographic operation failed, including being unable to correctly verify a signature, decrypt a key exchange, or validate a finished message • fts_alert_desc_protocol_version=70 – the protocol version the client has attempted to negotiate is recognized but not supported (always fatal) • fts_alert_desc_internal_error=80 – an internal error unrelated to the peer or correctness of the protocol (always fatal)

45023

Message ID	45023
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive level=<level_value> desc=<value> msg=\ <i>“SSL Alert received”</i>
Meaning	An SSL alert was received.

45027

Message ID	45027
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive type=<type> msg=\ <i>“Invalid SSL ContentType”</i>
Meaning	An invalid SSL ContentType occurred.

45029

Message ID	45029
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg=\ <i>“Bad length in SSL ChangeCipherSpec”</i>
Meaning	An SSL ChangeCipherSpec has a bad length.

45031

Message ID	45031
Log Type	Event Log – VIP SSL
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_number> vip=<vip_name> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> min=<minimum_value> max=<maximum_value> received=<received_value> action=close msg=<log_message_information>
Meaning	An SSL ChangeCipherSpec has a bad length.

Event-WAN Acceleration

Event-WAN Acceleration log messages record WAN events that occur on the network.

48001	48124
48003	48127
48005	48129
48007	48131
48009	48132
48011	48200
48012	48201
48013	48205
48015	48300
48017	48301
48019	
48023	
48027	
48029	
48031	
48100	
48101	
48102	
48123	

48001

Message ID	48001
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive expected=<value> received=<value> msg=\“Incorrect SSL handshake message\”
Meaning	The SSL received an incorrect handshake message.

48003

Message ID	48003
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close handshake=<value> msg=\“Bad length in SSL handshake\”
Meaning	The SSL handshake message had a bad length.

48005

Message ID	48005
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg=\“RSA verification of Diffie-Hellman paramters failed\”
Meaning	RSA verification of Diffie-Hellman parameters failed.

48007

Message ID	48007
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> local=<local_value> remote=<value> action=close msg=\“Hash in SSL Finished does not match calculated hash\”
Meaning	Hash in SSL Finished does not match calculated hash.

48009

Message ID	48009
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close reason=<value> msg= “SSL decryption failure ”
Meaning	The SSL received an incorrect handshake message.

48011

Message ID	48011
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close min-minor=<value> recv-minor=<value> msg= “SSL minor below minimum configured value ”
Meaning	SSL minor version less than configured minimum value.

48012

Message ID	48012
Log Type	Event Log - WAN Acceleration
Severity	Warning
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg= “SSL maximum connections reached ”
Meaning	SSL maximum connection limit reached.

48013

Message ID	48013
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg= “None of the offered CipherSuites are supported ”
Meaning	The SSL CipherSuites that are offered are not supported.

48015

Message ID	48015
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive len=<value> msg=l"Incorrect SSL handshake length"
Meaning	The SSL handshake has an invalid length.

48017

Message ID	48015
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive handshake=<value> len=<value> max=<value> msg=l"SSL Handshake too long"
Meaning	The SSL handshake was too long.

48019

Message ID	48019
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=send level=<value> desc=<value> msg=l"SSL Alert sent"
Meaning	An SSL alert was sent.

48023

Message ID	48023
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive level=<value> desc=<value> msg=l"SSL Alert received"
Meaning	An SSL alert was received.

48027

Message ID	48027
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=receive type=<value> msg=\ Invalid SSL ContentType \
Meaning	An invalid SSL ContentType.

48029

Message ID	48029
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> action=close msg=\ Bad length in SSL ChangeCipherSpec \
Meaning	An SSL ChangeCipherSpec has a bad length.

48031

Message ID	48031
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> min=<value> max=<value> received=<value> action=close msg=\ <log_message_information> \
Meaning	An SSL ChangeCipherSpec has a bad length.

48100

Message ID	48100
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> msg=\ authentication failed: cert authentication failed \
Meaning	An authentication concerning certificate authentication failed.

48101

Message ID	48101
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> authgrp=<authentication_group> host=<host_name> msg=\ <i>“authentication failed: incorrect psk”</i>
Meaning	An authentication failed because of an incorrect pass keyword.

48102

Message ID	48102
Log Type	Event Log - WAN Acceleration
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> authgrp=<authentication_group> peer=<peer> msg=\ <i>“authentication failed: <reason>”</i>
Meaning	An authentication failed.

48123

Message ID	48123
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	msg=\ <i>“A wan-opt rule is changed”</i>
Meaning	A WAN-opt rule was changed.

48124

Message ID	48124
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	msg=\ <i>“A wan-opt rule is added”</i>
Meaning	A WAN-opt rule was added.

Message ID	48124
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} id=<log_identification> msg=\ <i>“User <user_name> deleted a wad rule <rule> from <location>”</i>
Meaning	A wad rule entry was deleted.

48127

Message ID	48127
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} msg=\“user <user_name> set web proxy name\”
Meaning	The specified user set the wad cache name.

Message ID	48127
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} msg=\“user <user_name> set wan accelerator host-id\”
Meaning	The specified user set the wan host name.

48129

Message ID	48129
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} msg=\“user <user_name> set wan accelerator storage\”
Meaning	The specified user set the WAN-opt storage.

Message ID	48129
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} msg=\“user <user_name> delete wan accelerator storage entry\”
Meaning	The specified user deleted the WAN-opt storage entry.

Message ID	48129
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} msg=\“user <user_name> set byte cache storage\”
Meaning	The specified user set the byte cache storage.

Message ID	48129
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0

Message ID	48129
Messages	user=<user_name> ui={GUI CLI console} msg=\“user <user_name> set web cache storage\”
Meaning	The specified user set the web cache storage.
Message ID	48129
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} msg=\“user <user_name> set wan accelerator storage\”
Meaning	The iSCSI target is set.

48131

Message ID	48131
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} name=<name> msg=\“User <user_name> added a wan accelerator ssl server setting <name> from <location> \”
Meaning	The specified user has added a wad ssl server setting.

48132

Message ID	48132
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} name=<name> msg=\“User <user_name> deleted a wan accelerator ssl server setting <name> from <location>\”
Meaning	The specified user deleted a wad ssl server setting.

48200

Message ID	48200
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} name=<name> msg=\“User <user_name> added network accelerator peer <peer_name> from <location>\”
Meaning	The specified user added a network accelerator peer.

48201

Message ID	48201
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} name=<name> msg=\ <i>“User <user_name> deleted a network accelerator peer entry <peer_name> from <location>”</i>
Meaning	The specified user deleted a network accelerator peer.

48205

Message ID	48205
Log Type	Event Log - WAN Acceleration
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI CLI console} authgrp=<authentication_group> msg=\ <i>“User <user_name> deleted a network accelerator auth-group entry <peer_name> from <location>”</i>
Meaning	The specified user deleted a network accelerator authentication group.

48300

Message ID	48300
Log Type	Event Log - WAN Acceleration
Severity	Critical
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> rule-id=<rule_identification> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> msg=\ <i>“auto detection failed: server side ftg is not properly configured”</i>
Meaning	The server side of the FortiGate unit is not properly configured.

48301

Message ID	48300
Log Type	Event Log - WAN Acceleration
Severity	Critical
FortiOS version	4.0
Messages	serial=<serial_number> policy=<policy_id> rule-id=<rule_identification> app-type=<application_type> src=<source_address> src-port=<source_port> dst=<destination_address> dst-port=<destination_port> msg=\ <i>“unexpected application type. Please report.”</i>
Meaning	There was an unexpected application type.

Event-LDB-monitor

Event-LDB-monitor log messages record VIP activities.

46000

46001

46002

46003

46004

46005

46100

46101

46000

Message ID	46000
Log Type	Event-LDB-monitor
Severity	Notification
FortiOS version	4.0
Messages	vip=<vip_name> server=<server_ip_address> port=<port_number> server-admin-status={active standby disable} action=enable msg="ldb server enabled"
Meaning	The VIP realserver is enabled.

46001

Message ID	46001
Log Type	Event-LDB-monitor
Severity	Alert
FortiOS version	4.0
Messages	vip=<vip_name> server=<server_ip_address> port=<port_number> server-admin-status={active standby disable} action=disable msg="ldb server disabled"
Meaning	The VIP realserver is disabled.

46002

Message ID	46002
Log Type	Event-LDB-monitor
Severity	Notification
FortiOS version	4.0
Messages	vip=<vip_name> server=<server_ip_address> port=<port_number> server-admin-status={active standby disable} action=up msg="ldb server is up"
Meaning	The VIP realserver is up.

46003

Message ID	46003
Log Type	Event-LDB-monitor
Severity	Alert
FortiOS version	4.0
Messages	vip=<vip_name> server=<server_ip_address> port=<port_number> server-admin-status={active standby disable} action=down msg="ldb server down"
Meaning	The VIP realserver is down.

46004

Message ID	46004
Log Type	Event-LDB-monitor
Severity	Notification
FortiOS version	4.0
Messages	vip=<vip_name> server=<server_ip_address> port=<port_number> server-admin-status={active standby disable} action=holddown msg=\“ldb server entered holddown period\” interval=<value_seconds>
Meaning	The VIP realserver started a hold down period in seconds.

46005

Message ID	46005
Log Type	Event-LDB-monitor
Severity	Alert
FortiOS version	4.0
Messages	vip=<vip_name> server=<server_ip_address> port=<port_number> server-admin-status={active standby disable} action=holddown msg=\“ldb server health checking failed during holddown period\”
Meaning	The VIP realserver failed during the hold down period.

46100

Message ID	46100
Log Type	Event-LDB-monitor
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI<ip_address> CLI console} name=<name> msg=\“User <user_name> added load balance monitor <monitor_name> from {GUI <ip_address> CLI console}\”
Meaning	A load balance server monitor was added.

46101

Message ID	46101
Log Type	Event-LDB-monitor
Severity	Notification
FortiOS version	4.0
Messages	user=<user_name> ui={GUI<ip_address> CLI console} name=<name> msg=\“User <user_name> deleted a load balance server monitor <monitor_name> from {GUI <ip_address> CLI console}\”
Meaning	A load balance server monitor was deleted.

Event-his-performance

Event-his-performance log messages record the FortiGate unit's performance statistics.

47001

Message ID	47001
Log Type	Event-his-performance
Severity	Information
FortiOS version	4.0
Messages	action= <i>perf-stats</i> cpu=<percent_cpu_number> mem=<percent_memory_number> total_session=<session_number> msg="Performance statistics"
Meaning	Performance statistics for the FortiGate unit.

Event-HA

Event-HA log messages are recorded when FortiGate units are in high availability mode.

These log messages describe changes in cluster unit status. These changes in status occur if a cluster unit fails/starts up, or if a link fails/restored. Each of these messages includes the serial number of the cluster unit reporting the message. You can use the serial number to determine which cluster unit status has changed.

35001

- A high availability activity report has been generated.
- The HA subordinate unit synchronized with the new antispam engine.
- The HA subordinate unit failed to synchronize.
- The HA subordinate unit synchronized with the extended database.
- The HA subordinate unit synchronized with the new antivirus database.
- The HA subordinate unit synchronized with the new virus database.
- The HA subordinate unit synchronized with the new IDS package.

Message ID	35001
Log Type	Event Log - HA activity
Severity	Notification
FortiOS version	4.0
Messages	ip=<ip_address> ha-prio=<ha_cluster_priority> msg="<log_message_information>"
Meaning	A high availability activity report has been generated.

Message ID	35001
Log Type	Event Log - HA activity
Severity	Notification
FortiOS version	4.0
Messages	msg="HA slave sync AS(eng:<engine> rule set:<rule_set>) package <package_name>"
Meaning	The HA subordinate unit synchronized with the new antispam engine.

Message ID	35001
Log Type	Event Log - HA activity
Severity	Notification
FortiOS version	4.0
Messages	msg="HA slave sync failed in <number> turns"
Meaning	The HA subordinate unit failed to synchronize.

Message ID	35001
Log Type	Event Log - HA activity
Severity	Notification
FortiOS version	4.0
Messages	msg="HA slave sync extdb (<version_number>) <string>"
Meaning	The HA subordinate unit synchronized with the extended database.

Message ID	35001
Log Type	Event Log - HA activity
Severity	Notification
FortiOS version	4.0
Messages	msg="HA slave sync AV (<version_number>) package <name>"
Meaning	The HA subordinate unit synchronized with the new antivirus database.

Message ID	35001
Log Type	Event Log - HA activity
Severity	Notification
FortiOS version	4.0
Messages	msg="HA slave sync virdb(<version_number>) <string>"
Meaning	The HA subordinate unit synchronized with the new virus database.

Message ID	35001
Log Type	Event Log - HA activity
Severity	Notification
FortiOS version	4.0
Messages	msg="HA slave syn ids(<version_number>) package <string>"
Meaning	The HA subordinate unit synchronized with the new IDS package.

Event-pattern

Event-pattern logs are recorded whenever an administrator updates virus, IPS, and antispam databases from the FortiGuard network.

41000

41001

41002

41000

Message ID	41000
Log Type	Event - Pattern update
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui=GUI(<ip_address>) action=update status=success msg="Virus database has been updated successfully by user <administrator_name> via GUI (<ip_address>)"
Meaning	The specified administrator updated the virus database successfully from the web-based manager.

Message ID	41000
Log Type	Event - Pattern update
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui=GUI(<ip_address>) action=update status=success msg="IPS database has been updated successfully by user <administrator_name> via GUI (<ip_address>)"
Meaning	The specified administrator updated the IPS database from the web-based manager.

Message ID	41000
Log Type	Event - Pattern update
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui=GUI(<ip_address>) action=update status=failure msg="Update virus database failed by user <administrator_name> via GUI (<ip_address>)"
Meaning	The specified administrator failed to updated the virus database from the web-based manager.

Message ID	41000
Log Type	Event - Pattern update
Severity	Notification
FortiOS version	4.0
Messages	user=<administrator_name> ui=GUI(<ip_address>) action=update status=failure msg="AntiSpam database has been updated successfully by user <administrator_name> via GUI (<ip_address>)"
Meaning	The specified administrator successfully updated the AntiSpam database from the web-based manager.

41001

Message ID	41001
Log Type	Event - Pattern update
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui=GUI(<ip_address>) action=update status=failure msg="Update IPS database failed by user <administrator_name> via GUI (<ip_address>)"
Meaning	The specified administrator failed to update the IPS database from the web-based manager.

Message ID	41001
Log Type	Event - Pattern update
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui=GUI(<ip_address>) action=update status=failure msg="Update virus database failed by user <administrator_name> via GUI (<ip_address>)"
Meaning	The specified administrator failed to update the virus database from the web-based manager.

Message ID	41001
Log Type	Event - Pattern update
Severity	Critical
FortiOS version	4.0
Messages	user=<administrator_name> ui=GUI(<ip_address>) action=update status=failure msg="Update AntiSpam database failed by user <administrator_name> via GUI (<ip_address>)"
Meaning	The specified administrator failed to update the AntiSpam database from the web-based manager.

41002

Message ID	41002
Log Type	Event - Pattern update
Severity	Critical
FortiOS version	4.0
Messages	action=update status=failure msg="One of the HA members does not have valid license"
Meaning	A HA member does not have a valid license, which was found when updating licenses.

Data Leak Prevention

Data Leak Protection (DLP) log messages are log messages that record data leaks. These logs provide additional information for administrators that can better analyze and detect data leaks.

110000

Message ID	110000
Log Type	Data Leak Prevention
Severity	Notification
FortiOS version	4.0
Messages	<p>policyid=<policy_identification_number> serial=<log_serial_number> user=<user_name> group=<group_name> src=<source_address> sport=<source_port> src_int=<source_interface> dst=<destination_address> dport=<destination_port> dst_int=<destination_interface> service=<service_type> status=detected hostname=<hostname> url=<url_address> from=<sender_email> to=<receiver_email> msg=data leak detected(Data Leak Prevention Rule matched) rulename=<dlp_rule_name> action=<log_action_type></p>
Meaning	A data leak was detected by a specified DLP sensor rule.

Application Control

Application Control log messages are log messages that record application control protocols and events.

116000

116001

116002

116003

116010

116011

116013

116020

116000

Message ID	116000
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src_int=<source_interface> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown}
Meaning	An application control instant messaging message.

116001

Message ID	116001
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src_int=<source_interface> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown} filename=<file_name> filesize=<file_size> message=<log_message_information>
Meaning	An application control instant message file transfer message.

116002

Message ID	116002
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src_int=<source_interface> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown}
Meaning	An application control instant message chat message

116003

Message ID	116003
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src_int=<source_interface> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown} reason=<reason> req=<request_type>
Meaning	An application control instant message SIP session blocked message.

116010

Message ID	116010
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src_int=<source_interface> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown}
Meaning	An application control instant message message.

116011

Message ID	116011
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src_int=<source_interface> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown} reason=<reason> req=<request_type>
Meaning	An application control VoIP-SIP session blocked message.

116013

Message ID	116013
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src_int=<source_interface> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown} phone=<phone_number> reason=<reason>
Meaning	An application control VoIP-SCCP blocked call message.

116020

Message ID	116020
Log Type	Application Control
Severity	Variable
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> kind={login chat file photo audio call register unregister call-block request response} profile=<profile_type> dir=<directory> src=<source_address> src_port=<source_port> src_int=<source_interface> dst=<destination_address> dst_int=<destination_interface> dst_port=<destination_port> dst_int=<destination_interface> src_name=<source_name> dst_name=<destination_name> proto=<protocol> service=<service> policyid=<policy_identification> serial=<serial_number> app_list=<application_control_list_name> app_type=<application_type> app=<application> action={pass block monitor kickout encrypt-kickout reject unknown} count=<count> msg=<log_message_information>
Meaning	An application control IPS message.

Antivirus

Antivirus log messages record actual viruses that are contained in an email as well as anything that appears to be similar to a virus or suspicious, such as in a file or in an email.

60000

63000

63001

63002

66000

60000

Message ID	60000
Log Type	Antivirus Log
Severity	Variable
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> filetype=<file_type> filefilter=<file_filter> service={HTTP SMTP FTP} dir=<directory> agent=<agent_name> status={passthrough blocked} from=<sender_email_address> to=<recipient_email_address> file=<file_name> checksum=<string> virus=<virus_type> url=<url_address> ref=<reference_url_address> msg="<log_message_information>"
Meaning	An email contains a file that appears to be infected. When viewing this log message in Formatted format in the web-based manager, select the reference URL for more information.

63000

Message ID	63000
Log Type	Antivirus Log
Severity	Variable
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> filetype=<file_type> filefilter=<file_filter> service={HTTP SMTP FTP} dir=<directory> agent=<agent_name> status={passthrough blocked} from=<sender_email_address> to=<recipient_email_address> file=<file_name> checksum=<string> virus=<virus_type> url=<url_address> ref=<reference_url_address> msg="<log_message_information>"
Meaning	An email containing a file has been blocked by the FortiGate unit. When viewing this log message in Formatted format in the web-based manager, select the reference URL for more information.

63001

Message ID	63001
Log Type	Antivirus Log
Severity	Variable
FortiOS version	4.0
Messages	<p>policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> filetype=<file_type> filefilter=<file_filter> service={HTTP SMTP FTP} dir=<directory> agent=<agent_name> status={passthrough blocked} from=<sender_email_address> to=<recipient_email_address> file=<file_name> checksum=<string> virus=<virus_type> url=<url_address> ref=<reference_url_address> msg="<log_message_information>"</p>
Meaning	An email containing a file has been exempted by the FortiGate unit. When viewing this log message in Formatted format in the web-based manager, select the reference URL for more information.

63002

Message ID	63002
Log Type	Antivirus Log
Severity	Variable
FortiOS version	4.0
Messages	<p>policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> filetype=<file_type> filefilter=<file_filter> service={HTTP SMTP FTP} dir=<directory> agent=<agent_name> status={passthrough blocked} from=<sender_email_address> to=<recipient_email_address> file=<file_name> checksum=<string> virus=<virus_type> url=<url_address> ref=<reference_url_address> msg="<log_message_information>"</p>
Meaning	An email containing a file has been intercepted by the FortiGate unit. When viewing this log message in Formatted format in the web-based manager, select the reference URL for more information.

66000

Message ID	66000
Log Type	Antivirus Log
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> filetype=<file_type> filefilter=<file_filter> service={HTTP SMTP FTP} dir=<directory> agent=<foscarrieronly_agent_name> status={passthrough blocked} url=<url_address> ref=<reference_url_address> msg="File exceeds size limit."
Meaning	A file exceeds the size limit. When viewing this log message in Formatted format in the web-based manager, select the reference URL for more information.

Attack

Attack log messages are recorded when attacks are made against your network. These log messages provide details about the attack, such as the severity level of the attack and a reference URL link to find more information about the specified attack in the Fortinet Attack Encyclopedia.

70000

Message ID	70000
Log Type	Attack log – Signature event
Severity	Alert
FortiOS version	4.0
Messages	<p>policyid=<policy_identification_number> serial=<serial_number> attack_id=<value_attack_id> severity=<severity_level> carrier_ep=<foscarrieronly_end-point_identification> profile=<protection_profile_name> sensor=<dlp_sensor_name> src=<source_ip_address> dst=<ip_address> src_port=<port_number> dst_port=<port_number> src_int=<interface_name> dst_int=<interface_name> status={clear_session detected dropped reset drop_session pass_session reset_client reset_server} proto=<protocol_number> service=<service_location> user=<user_name> group=<group_name> ref=<reference_url> count=<sum_attacks_detected> incident_serialno=<attack_identification_number> msg="<log_message_information>"</p>
Meaning	<p>Attack signature message providing the source and destination addressing information. Look up the attack ID in the Fortinet Attack Encyclopedia for more information about the signature.</p> <p>Note: The count field displays the number of times the attack occurred. For example, if the attack occurred three times, the count field shows the number three. The count number is also included in the message field.</p>
Action	<p>Get more information about the attack and the steps to take from the Fortinet Attack Encyclopedia in the FortiProtect Center. Analyze logs as required.</p>

73001

Message ID	73001
Log Type	Attack log – Anomaly event
Severity	Critical
FortiOS version	4.0

Message ID	73001
Messages	<p> policyid=<policy_identification_number> serial=<serial_number> attack_id=<value_attack_id> severity=<severity_level> carrier_ep=<foscarrieronly_end-point_identification> src=<source_ip_address> dst=<ip_address> src_port=<port_number> dst_port=<port_number> interface=<interface_name> src_int=<interface_name> dst_int=<interface_name> status={clear_session detected dropped reset drop_session pass_session reset_client reset_server} proto=<protocol_number> service=<network_service> user=<user_name> group=<group_name> msg="<log_message_information>" </p>
Meaning	Attack anomaly message providing the source and destination addressing information. Look up the attack ID in the Fortinet Attack Encyclopedia for more information about the anomaly.
Action	Get more information about the attack and the steps to take from the Fortinet Attack Encyclopedia in the FortiProtect Center. Analyze logs as required.

Spam filter

Spam filter log messages record email protocols SMTP, POP3 and IMAP. In this section, these log messages are grouped into their subtype, SMTP, POP3 or IMAP.

[SMTP](#)

[POP3](#)

[IMAP](#)

SMTP

80000

Message ID	80000
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="from ip is in ip blacklist (connection block ip <ip_address>)"
Meaning	The IP address was found in the IP black list.

80001

Message ID	80001
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The IP address is in the DNSBL/ORDBL list.

80002

Message ID	80000
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The SMTP HELO/EHLO domain name DNS check failed.

80003

Message ID	80003
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="from email address is in email blacklist. (no.1 pattern matched)"
Meaning	The sender's email address was found in the email black list.

80004

Message ID	80004
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The email message contains a banned header.

80005

Message ID	80004
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The return email domain name DNS check failed.

80006

Message ID	80006
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="The email contains banned word(s). (n-n)"
Meaning	The email message from the specified source was blocked because it contains a word from the banned word list. See the Fortinet Knowledge Center article, AntiSpam log message explanation, for more information on the (n-n) value.

80007

Message ID	80007
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The IP address is in the IP black list.

80008

Message ID	80008
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The email message contains a blocked URL or many blocked URLs.

80010

Message ID	80010
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The sender's email address is in the email white list.

80011

Message ID	80011
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The sender's email address is in the email white list.

80012

Message ID	80012
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The email checksum is in the checksum black list.

80014

Message ID	80014
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=smtp profile=<profile_type> status=detected from=<sender_email_address> to=<recipient_email_address> msg="<log_message_information>"
Meaning	The email message is exempt because it contains an exempt word.

80008

Message ID	80008
Log Type	Spam Filter Log – SMTP
Severity	Notification
FortiOS version	4.0
Messages	src=<source_ip_address> dst=<destination_ip_address> src_int=Antispam dst_int=<destination_interface> service=smtp status=detected from=<sender_emailaddress> to=<receiver_emailaddress> msg="The email contains FortiGuard - AntiSpam blocking URL(s).(black url <url>)"
Meaning	The email message from the specified source was blocked because it contains either one or more FortiGuard-AntiSpam blocking URLs.

POP3

83003

Message ID	83003
Log Type	Spam Filter – POP3
Severity	Notification
FortiOS version	4.0
Messages	src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=pop3 status=detected from=<sender_email_address> to=<recipient_email_address> msg="from email address is in email blacklist. (no.1 pattern match)"
Meaning	The sender's email address was found in the email black list.

83005

Message ID	83005
Log Type	Spam Filter – POP3
Severity	Notification
FortiOS version	4.0
Messages	src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=pop3 status=detected from=<sender_email_address> to=<recipient_email_address> msg="return email domain name DNS check failed.(failed to obtain DNS record for domain <domain_name>)"
Meaning	The email address was returned because the FortiGate unit failed to obtain the DNS record for the domain.

83006

Message ID	83006
Log Type	Spam Filter – POP3
Severity	Notification
FortiOS version	4.0
Messages	scr=<source_ip_address> dst=<destination_ip_address> src_int=<source_interface> dst_int=<destination_interface> service=pop3 status=detected msg="The email contains banned word(s). (no.<number> pattern matched)"
Meaning	The email message from the specified source was blocked because it contains a word from the banned word list. The (<number>) part of the message contains the corresponding banned word ID number. See the Fortinet Knowledge Center article, Antispam log message explanation, for details about (<number>).

83007

Message ID	83007
Log Type	Spam Filter – POP3
Severity	Notification
FortiOS version	4.0
Messages	scr=<source_ip_address> dst=<destination_ip_address> src_int= Hardware dst_int= external service= pop3 status= detected from=<sender_email_address> to=<receiver_email_address> msg="from ip is in FortiGuard - AntiSpam ip blacklist.(path black ip <ip_address>)"
Meaning	The sender's email address is from an IP address that is in FortiGuard-AntiSpam's black list.

83008

Message ID	83008
Log Type	Spam Filter – POP3
Severity	Notification
FortiOS version	4.0
Messages	scr=<source_ip_address> dst=<destination_ip_address> src_int= IPS dst_int= external service= pop3 status= detected from=<sender_email_address> to=<recipient_email_address> msg="The email contains FortiGuard - AntiSpam banned blocking URL(s).(black url <url>)"
Meaning	The email message from the specified source was blocked because it contains either one or more FortiGuard-AntiSpam blocking URLs.

83011

Message ID	83011
Log Type	Spam Filter – POP3
Severity	Notification
FortiOS version	4.0
Messages	scr=<source_ip_address> dst=<destination_ip_address> src_int=<source_interface> dst_int=<destination_interface> service= pop3 status= exempted from=<sender_email_address> to=<receiver_email_address> msg="from ip is in FortiGuard - AntiSpam ip whitelist(path white ip <ip_address>)"
Meaning	The sender's email address is from an IP address that is in FortiGuard-AntiSpam's white list.

IMAP

86006

Message ID	86006
Log Type	Spam Filter – IMAP
Severity	Notification
FortiOS version	4.0
Messages	src=< source_ip_address > dst=< destination_ip_address > src_int=< source_interface > dst_int=< destination_interface > service= imap status= detected msg="The email contains banned word(s). (<value-value>)"
Meaning	The email message from the specified source was blocked because it contains a word from the banned word list. See the Fortinet Knowledge Center article, AntiSpam log message explanation, for more information.

Message ID	86006
Log Type	Spam Filter – IMAP
Severity	Notification
FortiOS version	4.0
Messages	src=< source_ip_address > dst=< destination_ip_address > src_int=< source_interface > dst_int=< destination_interface > service= imap status= detected msg="The email contains banned word(s). (<banned_word>)"
Meaning	The email message from the specified source was blocked because it contains a word from the banned word list. See the Fortinet Knowledge Center article, AntiSpam log message explanation, for more information.

Webfilter

Web filter log messages record URL activity and any filters configured in the firewall policy, such as a blocked URL because it was found in the URL black list.

The following log messages include the firmware version that the log message is generated in. Log messages generated in one firmware version may not contain the exact information as in another firmware version, because of changes to existing features or new features.

90000
91005
91010
93002
93003
93006
93007
93013
99001
99501
99510
99511

90000

Message ID	90000
Log Type	Web Filter – Category Block
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> service=<service_type> status=[enable disable] from=<sender_email_address> to=<receiver_email_address> msg="<log_message_information>"
Meaning	A banned word was found.

91000

Message ID	91000
Log Type	Web Filter – Category Block
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> service=<service_type> status=blocked count=<count> req_type=<request_type> url=<url_address> msg="<log_message_information>"
Meaning	A cookie was removed.

91005

Message ID	91005
Log Type	Web Filter – Category Block
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> service=<service_type> status=blocked count=<count> req_type=<request_type> url=<url_address> msg="<log_message_information>"
Meaning	Java applet from specified host was removed.

91010

Message ID	91010
Log Type	Web Filter – Category Block
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> service=<service_type> hostname=<hostname> status=blocked count=<count> req_type=<request_type> url=<url_address> msg="<log_message_information>"
Meaning	ActiveX script from specified host was removed.

93002

Message ID	93002
Log Type	Web Filter – Category Block
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> profile=<profile_name> service=<service_type> hostname=<hostname> status=blocked count=<count> req_type=<request_type> url=<url_address> msg="URL was blocked because it is in the URL filter list"
Meaning	The specified URL was blocked because it is in the URL blacklist.

93003

Message ID	93003
Log Type	Web Filter – URL Filter
Severity	Information
FortiOS version	4.0
Messages	user=<user_id> src=<source_ip_address> srcport=<port_num> src_int=<source_interface> dst=<destination_ip_address> dstport=<destination_port> dst_int=<destination_interface> service=http hostname=<url> status=passthrough error="no rating service is found" url=<url_address> msg="Policy allows URLs when a rating error occurs"
Meaning	A rating error occurred and the policy allows URLs when a rating error occurs.

Message ID	93003
Log Type	Web Filter – URL Filter
Severity	Information
FortiOS version	4.0

Message ID	93003
Messages	policyid=<policy_identification_number> serial=<serial_number> user=<user_name> group=<group_name> src=<source_ip_address> srcport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dstport=<destination_port> dst_int=<destination_interface> service=<service_type> hostname=<url_address> profile=<protection_profile_name> status=<exempted> req_type=<[referral direct]> url=<url_address> url=<url_address> msg="URL was exempted because it is in the URL filter list"
Meaning	The URL is exempted in the URL filter list.
Message ID	93003
Log Type	Web Filter – URL Filter
Severity	Information
FortiOS version	4.0
Messages	serial=<serial_number> user=<user_name> group=<user_group> src=<source_ip_address> srcport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dstport=<destination_port> dst_int=<destination_interface> service=<service_type> hostname=<url> profile=<profile_name> status=<allowed> req_type=<request_type> url=<url_address> error= "no rating service is found" url=<url_address> msg="URL was exempted because it is in the URL filter list"
Meaning	The URL is allowed in the URL filter list.

93004

Message ID	93004
Log Type	Web Filter – URL Filter
Severity	Notification
FortiOS version	4.0
Messages	policyid=<policy_identification_number> user=<user_name> group=<user_group> profile=<protection_profile> src=<source_ip_address> sport=<source_port> dst=<destination_ip_address> service=https status=filtered req_type=<[direct request]> msg="The certificate for the HTTPS session contained an invalid domain name. The session has been filtered by IP only."
Meaning	The service's certificate for the HTTPS session contained an invalid domain name and was filtered by IP address.

93006

Message ID	93006
Log Type	Web Filter – URL Filter
Severity	Critical
FortiOS version	4.0
Messages	hostname=<url> msg="gethostbyname() failed: <hostname>"
Meaning	Cannot resolve the name of the FortiGuard server
Action	Check settings.

93007

Message ID	93007
Log Type	Web Filter – URL Filter
Severity	Critical
FortiOS version	4.0
Messages	msg="calloc() failed: <hostname>"
Meaning	Insufficient resources.
Action	Delete logs to free some memory.

93013

Message ID	93013
Log Type	Web Filter – Category Block
Severity	Critical
FortiOS version	4.0
Messages	FortiGuard is enabled in the protection profile but the FortiGuard service is not enabled
Meaning	FortiGuard is enabled in the protection profile but the FortiGuard service is not enabled.
Action	Enable the FortiGuard service.

99001

Message ID	99001
Log Type	Web Filter – Category Block
Severity	Error
FortiOS version	4.0
Messages	serial=<serial_id> user=<administrator_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=http hostname=<domain_name> url=<url_address> status=passthrough error=<error_type> req_type=<request_type> url=<url_address> msg="Policy <policy_action> URLs when a rating error occurs"
Meaning	All pending requests are flushed when the FortiGuard server list needs to be reloaded. These requests are flushed to ensure a clean update of the list. The list only reloads as a result of one of the following: <ul style="list-style-type: none"> • System time zone changed • The FortiGuard hostname or port changed • The FortiGuard server override list has been enabled or disabled • The FortiGuard server override list is enabled and the list was modified One log message is generated for each request that was flushed as a result of the update.

99501

Message ID	99501
Log Type	Web Filter – Category Block
Severity	Notification
FortiOS version	4.0
Messages	serial=<serial_id> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=<service_type> method=<method_type> hostname=<domain_name> status=blocked req_type=<request_type> url=<url_address> msg="URL belongs to a denied category in policy."
Meaning	A URL belongs to a denied category in policy.

99510

Message ID	99510
Log Type	Web Filter – FortiGuard
Severity	Notification
FortiOS version	4.0
Messages	serial=<serial_id> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_interface> service=<service_type> method=<method_type> hostname=<name> status=passthrough req_type=<request_type> url=<url_address> msg="URL belongs to an allowed category in policy"
Meaning	The URL was logged because it was rated in a category that is allowed in the policy.

99511

Message ID	99511
Log Type	Web Filter – FortiGuard
Severity	Variable
FortiOS version	4.0
Messages	serial=<serial_id> user=<user_name> group=<group_name> src=<source_ip_address> sport=<source_port> src_int=<source_interface> dst=<destination_ip_address> dport=<destination_port> dst_int=<destination_source> service=<service_type> method=<method_type> mode=<mode_type> rule_type=<rule_type> rule_data=<rule_data> hostname=<name> status=passthrough req_type=<request_type> url=<url_address> msg="URL belongs to an override rule"
Meaning	The URL was allowed because it belongs to an override rule.

DLP archives

DLP archive log messages are log messages that are sent to the FortiAnalyzer unit (or FortiGuard Analysis server) that include email, FTP activities, IM events, VoIP events, and web filter events. You can configure your FortiGate unit to send content archives to a FortiGuard Analysis server if you have subscribe to the FortiGuard Analysis and Management Service.

40000

60000

70000

80000

40000

Message ID	40000
Log Type	DLP Archive – Web
Severity	Information
FortiOS version	4.0
Messages	SN=<log_serial_number> user=<user_name> group=<group_name> carrier_ep=<foscarrieronly_end-point_identification> cat=<web site_category_number> cat_desc=<web site_category_name> <contentlogversion_integer>:<time_stamp>:<serial_number>:<client_ipaddress> <-> <server_ipaddress>:[clean infected heuristic banned_word blocked exempt oversized]: <number of bytes from client>:<number of bytes from server>:[POST GET] <url_address>
Meaning	A HTTP web site was archived to the FortiAnalyzer unit or FortiGuard Analysis server.

60000

Message ID	60000
Log Type	DLP Archive – Email
Severity	Information
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end- point_identification> <contentlogversion_integer>:<session_integer>:<client_ipaddress> <-> <server_ipaddress>:<infectionstatus>:<size_sent>:<from_emailaddress/to_email address>:<attachments> <subject>
Meaning	An email that used SMTP protocol was archived to the FortiAnalyzer unit or FortiGuard Analysis server.

70000

Message ID	70000
Log Type	DLP Archive – Email
Severity	Information
FortiOS version	4.0
Messages	SN=<log_serial_number> user=<user_name> group=<group_name> carrier_ep=<foscarrieronly_end-point_identification> <contentlogversion_integer>:<session_integer>:<client_ipaddress> <-> <server_ipaddress>:<infectionstatus>:<size_sent>:ft=<from_emailaddress/to_em ailaddress>:<number_attachments> <subject>
Meaning	An email that used POP3 protocol was archived to the FortiAnalyzer unit.

80000

Message ID	80000
Log Type	DLP Archive – FTP
Severity	Information
FortiOS version	4.0
Messages	user=<user_name> group=<usergroup_name> carrier_ep=<foscarrieronly_end-point_identification> <contentlogversion_integer>:<session_integer>:<client_ipaddress> <-> <server_ipaddress>:<infectionstatus>:<number of bytes sent by client/ number of bytes sent by server>:{RETR PASS USER} {filename password} username}
Meaning	A user accessed an FTP server. RETR is when the user retrieves a file and is followed with the filename he or she retrieved. PASS is when the user entered their password to access the FTP server. USER is when the user name is accepted to access the FTP server.

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com