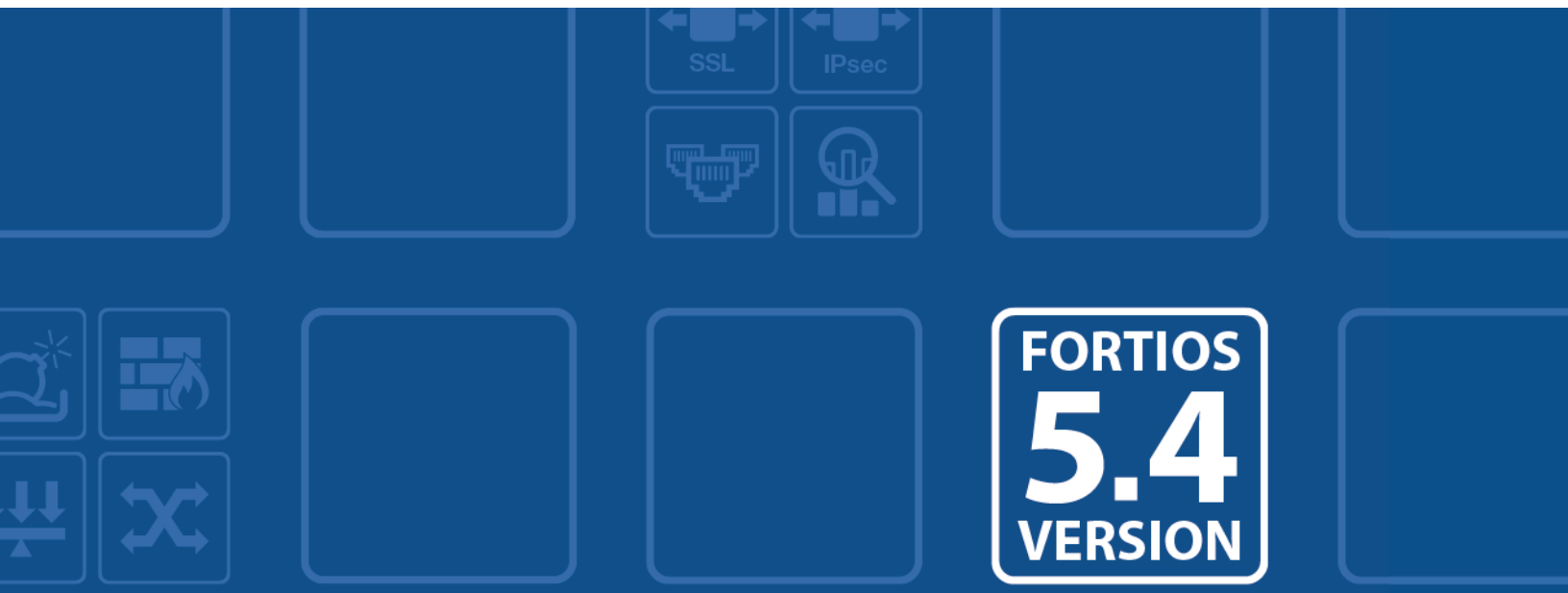
FORTINET
High Performance Network Security

FortiOS - FortiOS Log Reference

VERSION 5.4.0



FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

January 27, 2017

FortiOS 5.4.0 FortiOS Log Reference

01-540-299610-20170127

TABLE OF CONTENTS

Change Log **7**
Introduction **8**
Before You Begin 8
Overview 8
What's New 8
FortiOS 5.4.0 8
Log Types and Sub Types **10**
Type 10
Subtype 11
Priority Level 11
Message IDs 11
Log Message Format 12
Log Field Format 12
Log Schema Structure **13**
Header and Body Fields 13
Log ID Numbers 15
Log ID Definitions 16
FortiOS 5.4.0 Log Messages **19**
Anomaly 19
Anomaly Log Messages 20
App 21
App Log Messages 22
AV 23
AV Log Messages 25
DLP 27
DLP Log Messages 29
Email 30
Email Log Messages 31
Event 33
COMPLIANCE-CHECK 33
ENDPOINT 34
HA 36
ROUTER 39
SYSTEM 41

USER 67
VPN 70
WAD 76
WIRELESS 79
GTP 85
GTP Log Messages 88
IPS 89
IPS Log Messages 91
Traffic 91
Traffic Log Messages 95
VoIP 96
VoIP Log Messages 98
WAF 99
WAF Log Messages 100
Web 101
Web Log Messages 103
Appendix A: Log Field Diff Between 5.2.0 and 5.4.0 106
Content 106
Event 109
Compliance-Check 109
Endpoint 110
GTP 111
HA 113
Router 114
System 114
User 116
VPN 117
WAD 117
Wireless 117
GTP 118
Security (UTM) 120
Anomaly 121
App 122
AV 123
DLP 123
Email 124
IPS 124
Web 124
Traffic 125
WAF 126
Other logs 127
Netscan 127

VOIP 129
Appendix B: Log Field Diff for 5.2.9 and 5.4.0 131
Traffic 131
Event 131
Compliance-Check 132
Endpoint 132
Router 133
System 133
Security (UTM) 133
Anomaly 133
IPS 134
Web 134
GTP 134
WAF 137
Netscan 138
VOIP 141
Appendix C: Log ID Diff for 5.2.0 and 5.4.0 142
Event 142
COMPLIANCE-CHECK 142
Endpoint 142
GTP 143
HA 144
Router 144
System 144
User 150
VPN 150
WAD 153
Wireless 153
GTP 156
Security 157
Anomaly 157
AntiVirus 157
IPS 157
Web Filter 158
Traffic 158
WAF 158
Other Logs 159
Netscan 159
VOIP 160
Appendix D: Log ID Diff for 5.2.9 and 5.4.0 161
Traffic 161
Event 161

Compliance-Check 161
Endpoint 161
HA 162
Router 162
System 162
VPN 164
WAD 164
Wireless 164
Security (UTM) 164
Web 164
Email 165
GTP 167
WAF 168
Other 168
Netscan 168

Change Log

Date	Change Description
2015-12-18	Updated for version 5.4.0.
2016-01-29	Updated the Log Types and Sub Types section to indicate the new GTP and WAF log types. Previously GTP was a log sub type of the Event log type.
2016-11-03	Added a What's New section and an appendix of a log field diff for 5.2.0 and 5.4.0.
2016-11-10	Updated Appendix B: Log ID Diff for 5.2.9 and 5.4.0. Added Appendix D: Log ID Diff for 5.2.9 and 5.4.0.
2017-01-27	Removed the `encrypt-kickout` value from the *Log Field Format* section.

Introduction

This document provides information about all the log messages applicable to the FortiGate devices running FortiOS version 5.2.0 or higher. The logs are intended for administrators to be used as reference for more information about a specific log entry and message that is generated.

Before You Begin

Before you begin using this reference, read the following notes:

- The information in this document applies to all FortiGate units currently running FortiGate 5.2.0 or higher.
- Ensure that you have enabled logging for FortiGate unit. For more information, see the *Logging and Reporting* chapter in the *FortiGate Handbook*.
- Each log message is displayed in RAW format in the Log View of the web-based manager.
- Each log message is documented similar to how it appears in the log viewer table based on the RAW format. For more information, see the *Logging and Reporting* chapter in the *FortiGate Handbook*.

This reference contains detailed information for each log type and sub type; however, this reference contains only information gathered at publication and, as a result, not every log message field contains detailed information.

Overview

The log types described in this document report traffic, security, and event log information useful for system administrators when recording, monitoring, and tracing the operation of a FortiGate device running FortiOS. The logs provide information regarding the following:

- Firewall attacks
- Configuration changes
- Successful and unsuccessful system operations

What's New

This section identifies major changes in the FortiOS Log Reference from version 5.4.0 and later.

FortiOS 5.4.0

Content

- Content log type was removed from FortiOS 5.4.0.

Event

- Compliance-check log subtype was added to Event log type.
- GTP log subtype was removed from Event log type.
- Router log subtype was added to Event log type.

GTP

- GTP was added as a new log type with a category of 14. Previously GTP was a log subtype of the Event log type.

WAF

- WAF was added as a new log type with a category of 12.

Log Types and Sub Types

FortiGate devices can record the following types and sub types of log entry information:

Type	Description	Sub Type
Traffic	Records traffic flow information, such as an HTTP/HTTPS request and its response, if any.	• Local • Forward • Multicast • Sniffer
Security (UTM)	Records virus attack and intrusion attempts.	• AntiVirus • Anomaly • Application Control • Data Leak Prevention (DLP) • Intrusion Prevention (IPS) • Email Filter • Web Filter
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	• Compliance-check • Endpoint Control • High Availability • Router • System • User • Virtual Private Network (VPN) • WAD • Wireless
GTP	Records GPRS Tunneling Protocol (GTP) traffic for FortiCarrier devices.	
WAF	Records web application firewall information for FortiWeb appliances and virtual appliances	

Type

Each log entry contains a Type (type) field that indicates its log type, and in which log file it is stored.

Subtype

Each log entry might also contain a Sub Type (subtype) field within a log type, based on the feature associated with the cause of the log entry.

For example:

- In event logs, some log entries have a subtype of user, system, or other sub types.
- In security (UTM) logs, some log entries have a subtype of DLP, Web Filter, Email or other sub types.
- In traffic logs, the sub types are: local, forward, multicast, and sniffer.

Priority Level

Each log entry contains a Level (pri) field that indicates the estimated severity of the event that caused the log entry, such as pri=warning, and therefore how high a priority it is likely to be. Level (pri) associations with the descriptions below are not always uniform. They also may not correspond with your own definitions of how severe each event is. If you require notification when a specific event occurs, either configure SNMP traps or alert email by administrator-defined Severity Level (severity_level) or ID (log_id), not by Level (pri).

Level (0 is highest)	Name	Description
0	Emergency	The system is unusable or not responding.
1	Alert	Immediate action required. Used in security logs.
2	Critical	Functionality is affected.
3	Error	An error exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notification	Information about normal events.
6	Information	General information about system operations. Used in event logs to record configuration changes.

For each location where the FortiGate device can store log files (disk, memory, Syslog or FortiAnalyzer), you can define a severity threshold. The FortiGate stores all log messages equal to or exceeding the log severity level selected. For example, if you select Error, FortiGate will store log messages whose log severity level is Error, Critical, Alert, and Emergency.

Message IDs

The MSG ID (msg_id) field is a 10-digit number located in the header, incremented with each individual log message generated by FortiGate. It is used only for numbering each entry in the database, and does not necessarily reflect its cause.

Each msg_id number is a unique identifier for that specific log entry. No other log messages, regardless of cause, share the same msg_id.

LOG ID field	10-digit number
MSG-ID(msg_id)	Last 6 digits at the end of the LOG ID field.

Log Message Format

For documentation purposes, all log types and sub types follow this generic table format to present the log message entry and severity information.

Message ID	Message	Severity
2	LOG_ID_TRAFFIC_ALLOW	Notice

Log Field Format

The following table describes the standard format in which each log type is described in this document. For documentation purposes, all log types and sub types follow this generic table format to present the log entry information.

Log Field	Log Field Description	Data Type	Length	Value(s)
appact	The security action from app control	ENUM	16	• block • monitor • pass • reject • reset

Log Schema Structure

This section describes the schema of the FortiGate log messages.

Header and Body Fields

Each log message consists of several fields and values. In the web-based manager, the logs are displayed in a **Formatted** table view or **Raw** format. You can download the logs in the raw format for further analysis.

- Header - Contains the date and time the log originated, log identifier, message identifier, administrative domain (ADOM), the log category, severity level, and where the log originated. These fields are common to all log categories.
- Body - Describes the reason why the log was created and actions taken by the FortiGate device to address it. These fields vary by log category.

Following is an example of traffic log message in raw format. The body fields are highlighted in bold.

```
date=2014-07-04 time=14:26:59 logid=0001000014 type=traffic subtype=local
level=notice vd=vdom1 srcip=10.6.30.254 srcport=54705 srcintf="mgmt1"
dstip=10.6.30.1 dstport=80 dstintf="vdom1" sessionid=350696 status=close
policyid=0 dstcountry="Reserved" srccountry="Reserved" trandisp=noop
service=HTTP proto=6 app="Web Management" duration=13 sentbyte=1948
rcvdbyte=3553 sentpkt=9 rcvdpkt=9 devtype="Fortinet Device"
osname="Fortinet OS" mastersrcmac=00:09:0f:67:6c:31
srcmac=00:09:0f:67:6c:31
```

The following table provides an example of the log field information that is contained in the header and body fields, according to its name as it appears in the **Formatted** or **Raw** view.

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (raw format)
		Traffic	Event	Security	
Header					
Date (date)	The day, month, and year when the log message was reported.	✓	✓	✓	`date=2014-07-04`
Time (time)	The hour clock when the log message was recorded.	✓	✓	✓	`time=14:26:59`
ID (log_id)	See Log ID	✓	✓	✓	`logid=0001000014`
MSG (msg)	See Message IDs	✓	✓	✓	`msg=000100000012`
Type (type)	See Type	✓	✓	✓	`type=traffic`

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (raw format)
		Traffic	Event	Security	
Sub Type (subtype)	See Sub Type	✓	✓	✓	`subtype=local`
VDOM (vd)	The virtual domain in which the log message was recorded.	✓	✓	✓	`vd=vdom1`
Level (pri)	Priority level	✓	✓	✓	`level=notice`
Body					
Protocol (proto)	tcp: The protocol used by web traffic (tcp by default)	✓	✓	✓	`proto=6`
Source IP (srcip)	The IP address of the traffic's origin. The source varies by the direction: • In HTTP requests, this is the web browser or other client. • In HTTP responses, this is the physical server.	✓	✓	✓	`srcip=10.6.30.254`
Source Port (srcport)	The port number of the traffic's origin.	✓	✓	✓	`srcport=54705`
Source Interface (srcintf)	The interface of the traffic's origin.	✓	✓	✓	`srcintf="mgmt1"`
Destination IP (dstip)	The destination IP address for the web.	✓	✓	✓	`dstip=10.6.30.1`
Destination Port (dstport)	The port number of the traffic's destination.	✓	✓	✓	`dstport=80`
Destination Interface (dstintf)	The interface of the traffic's destination.	✓	✓	✓	`dstintf="vdom1"`
Session ID (sessionid)	The session number for the traffic connection	✓	✓	✓	`sessionid=350696`
Status (status)	The status of the session	✓	✓	✓	`status=close`

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (raw format)
		Traffic	Event	Security	
Policy (policyid)	The name of the server policy governing the traffic which caused the log message.	✓	✓	✓	`policyid=0`
Service (service)	http or https The name of the application-layer protocol used by the traffic. By definition, for FortiWeb, this is always HTTP or HTTPS.	✓	✓	✓	`service=HTTP`
User (user)	The daemon or name of the administrator account that performed the action that caused the log message.	✓	✓	✓	`user=admin`

Log ID Numbers

The ID (log_id) is a 10-digit field located in the header, immediately following the time and date fields. It is a unique identifier for that specific log and includes the following information about the log entry.

Log ID number components	Description	Examples
Log Type	Represented by the first two digits of the log ID.	• Traffic log IDs begin with "`00`". • Event log IDs begin with "`01`".
Sub Type or Event Type	Represented by the second two digits of the log ID.	• VPN log subtype is represented with "`01`" which belongs to the Event log type that is represented with "`01`". Therefore, all VPN related Event log IDs will begin with the `0101` log ID series.
Message ID	The last six digits of the log ID represent the message ID.	• An administrator account always has the log ID `0000003401`.

The log_id field is a number assigned to all permutations of the same message. It classifies a log entry by the nature of the cause of the log message, such as administrator authentication failures or traffic. Other log messages that share the same cause will share the same log_id.

Log ID Definitions

Following are the definitions for the log type IDs and sub type IDs applicable to FortiOS version 5.2.1 and later.

Log Type IDs	Sub Type IDs
traffic:0	• forward:0 • local:1 • multicast:2 • sniffer:4
event:1	• system:0 • vpn:1 • user:2 • router:3 • wireless:4 • wad:5 • endpoint:7 • ha:8 • compliance-check: 9
antivirus: 2	• virus:2 • suspicious:0 • analytics:1 • botnet:2 • infected:11 • filename:12 • oversize:13 • scanerror:62 • switchproto:63

Log Type IDs	Sub Type IDs
webfilter:3	• content:14 • urlfilter:15 • ftgd_blk:16 • ftgd_allow:17 • ftgd_err:18 • activexfilter:35 • cookiefilter:36 • appletfilter:37 • ftgd_quota_counting:38 • ftgd_quota_expired:39 • ftgd_quota:40 • scriptfilter:41 • webfilter_command_block:43
ips:4	• signature:19
spam: 5	• msn-hotmail:5 • yahoo-mail:6 • gmail:7 • smtp:8 • pop3:9 • imap:10 • mapi:11 • carrier-endpoint-filter: • 47 mass-mms:52

Log Type IDs	Sub Type IDs
contentlog: 6	• HTTP:24 • FTP:25 • SMTP:26 • POP3:27 • IMAP:28 • HTTPS:30 • im-all:31 • NNTP:39 • VOIP:40 • SMTPS:55 • POP3S:56 • IMAPS:57 • MM1:48 • MM3:49 • MM4:50 • MM7:51
anomaly: 7	• anomaly: 20
voip: 8	• viop: 14
dlp: 9	• dlp:54 • dlp-docsource:55
app-ctrl-all: 10	• app-ctrl-all:59
netscan: 11	• discovery:0 • vulnerability:1
WAF: 12	
GTP: 14	
UTM	• virus:2 • webfilter:3 • ips:4 • spam:5 • contentlog:6 • voip:8 • dlp:9 • app-ctrl:10

FortiOS 5.4.0 Log Messages

The following tables list the FortiOS 5.4.0 log messages.

Anomaly

Log Field Name	Description	Data Type	Length
action	Action	string	16
attack	Attack	string	256
attackid	Attack ID	uint32	10
count	Count	uint32	10
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
dstintf	Destination Interface	string	64
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtype	Event Type	string	32
group	User Group Name	string	64
icmpcode	ICMP code	string	6
icmpid	ICMP ID	string	8
icmptype	ICMP Type	string	6
level	Log Level	string	11
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
msg	Log Message	string	518
policyid	Policy ID	uint32	10
policytype		string	24
proto	Protocol	uint8	3
ref	Reference	string	
service	Name of Service	string	36
sessionid	Session ID	uint32	10
severity	Severity	string	8
srccountry		string	64
srcintf	Source Interface	string	64
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
user	User	string	256
vd	Virtual Domain Name	string	32

Anomaly Log Messages

The following table describes the log message IDs and messages of the Anomaly log.

Message ID	Message	Severity
18432	LOGID_ATTCK_ANOMALY_TCP_UDP	Alert
18433	LOGID_ATTCK_ANOMALY_ICMP	Alert
18434	LOGID_ATTCK_ANOMALY_OTHERS	Alert

App

Log Field Name	Description	Data Type	Length
action	Security action performed by App Control	string	16
app	Application name	string	96
appcat	Application category name	string	64
appid	Application ID	uint32	10
applist	Application Control profile name	string	64
apprisk	Application risk level	string	16
cloudaction	Action performed by cloud application	string	32
clouduser	User login ID detected by the Deep Application Control feature	string	256
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstip	Destination IP	ip	39
dstname	Destination Name	string	64
dstport	Destination Port	uint16	5
eventtype	App Control Event Type	string	32
filename	File name	string	256
filesize	File size in bytes	uint64	10
group	User group name	string	64
hostname	The host name of a URL	string	256

Log Field Name	Description	Data Type	Length
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile Name	string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
rcvdbyte	Received Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcintf	Source Interface	string	64
srcip	Source IP	ip	39
srcname	Source Name	string	64
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32

App Log Messages

The following table describes the log message IDs and messages of the App log.

Message ID	Message	Severity
28672	LOGID_APP_CTRL_IM_BASIC	Information
28673	LOGID_APP_CTRL_IM_BASIC_WITH_STATUS	Information
28674	LOGID_APP_CTRL_IM_BASIC_WITH_COUNT	Information
28675	LOGID_APP_CTRL_IM_FILE	Information
28676	LOGID_APP_CTRL_IM_CHAT	Information
28677	LOGID_APP_CTRL_IM_CHAT_BLOCK	Information
28678	LOGID_APP_CTRL_IM_BLOCK	Information
28704	LOGID_APP_CTRL_IPS_PASS	Information
28705	LOGID_APP_CTRL_IPS_BLOCK	Warning
28706	LOGID_APP_CTRL_IPS_RESET	Warning
28720	LOGID_APP_CTRL_SSH_PASS	Information
28721	LOGID_APP_CTRL_SSH_BLOCK	Warning

AV

Log Field Name	Description	Data Type	Length
action	The security action performed by AV	string	11
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
checksum	The checksum of the scanned file	string	16
command	FTP Command info	string	16
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid	Device serial number	string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtype	Event type of AV	string	32
filefilter	The filter used to identify the affected file	string	12
filename	File name	string	256
filetype	File type	string	16
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5

Log Field Name	Description	Data Type	Length
sessionid	Session ID	uint32	10
srcintf	Source Interface	string	32
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	subtype of the virus log	string	20
switchproto	Protocol change information	string	128
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
url	The url address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10

AV Log Messages

The following table describes the log message IDs and messages of the AV log.

Message ID	Message	Severity
8192	MESGID_INFECT_WARNING	Warning
8193	MESGID_INFECT_NOTIF	Notice
8194	MESGID_INFECT_MIME_WARNING	Warning
8195	MESGID_INFECT_MIME_NOTIF	Notice
8196	MESGID_WORM_WARNING	Warning
8197	MESGID_WORM_NOTIF	Notice

Message ID	Message	Severity
8198	MESGID_WORM_MIME_WARNING	Warning
8199	MESGID_WORM_MIME_NOTIF	Notice
8448	MESGID_BLOCK_WARNING	Warning
8449	MESGID_BLOCK_NOTIF	Notice
8450	MESGID_BLOCK_MIME_WARNING	Warning
8451	MESGID_BLOCK_MIME_NOTIF	Notice
8452	MESGID_BLOCK_COMMAND	Warning
8453	MESGID_INTERCEPT	Notice
8454	MESGID_INTERCEPT_MIME	Notice
8455	MESGID_EXEMPT	Notice
8456	MESGID_EXEMPT_MIME	Notice
8457	MESGID_MMS_CHECKSUM	Warning
8458	MESGID_MMS_CHECKSUM_NOTIF	Notice
8704	MESGID_OVERSIZE_WARNING	Warning
8705	MESGID_OVERSIZE_NOTIF	Notice
8706	MESGID_OVERSIZE_MIME_WARNING	Warning
8707	MESGID_OVERSIZE_MIME_NOTIF	Notice
8720	MESGID_SWITCH_PROTO_WARNING	Warning
8721	MESGID_SWITCH_PROTO_NOTIF	Notice
8960	MESGID_SCAN_UNCOMPSIZELIMIT_WARNING	Warning
8961	MESGID_SCAN_UNCOMPSIZELIMIT_NOTIF	Notice
8962	MESGID_SCAN_ARCHIVE_ENCRYPTED_WARNING	Warning
8963	MESGID_SCAN_ARCHIVE_ENCRYPTED_NOTIF	Notice
8964	MESGID_SCAN_ARCHIVE_CORRUPTED_WARNING	Warning

Message ID	Message	Severity
8965	MESGID_SCAN_ARCHIVE_CORRUPTED_NOTIF	Notice
8966	MESGID_SCAN_ARCHIVE_MULTIPART_WARNING	Warning
8967	MESGID_SCAN_ARCHIVE_MULTIPART_NOTIF	Notice
8968	MESGID_SCAN_ARCHIVE_NESTED_WARNING	Warning
8969	MESGID_SCAN_ARCHIVE_NESTED_NOTIF	Notice
8970	MESGID_SCAN_ARCHIVE_OVERSIZE_WARNING	Warning
8971	MESGID_SCAN_ARCHIVE_OVERSIZE_NOTIF	Notice
8972	MESGID_SCAN_ARCHIVE_UNHANDLED_WARNING	Warning
8973	MESGID_SCAN_ARCHIVE_UNHANDLED_NOTIF	Notice
9233	MESGID_ANALYTICS_SUBMITTED	Notice
9238	MESGID_ANALYTICS_FSA_RESULT	Notice
9248	MESGID_BOTNET_WARNING	Warning
9249	MESGID_BOTNET_NOTIF	Notice

DLP

Log Field Name	Description	Data Type	Length
action	Security action performed by DLP	string	20
agent	User agent - eg. agent="Mozilla/5.0"	string	64
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of packets	string	8
dlpextra	DLP extra information	string	256
docsource	DLP fingerprint document source	string	515
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
epoch	Epoch used for locating file	uint32	10
eventid	The serial number of the dlparchive file in the same epoch	uint32	10
eventtype	DLP event type	string	32
filename	File name	string	256
filesize	File size in bytes	uint64	10
filetype	File type	string	23
filtercat	DLP filter category	string	8
filteridx	DLP filter ID	uint32	10
filtername	DLP rule name	string	128
filtertype	DLP filter type	string	23
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
mmsdir	MMS Directory	string	3
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	DLP profile name	string	64
proto	Protocol number	uint8	3
rcvdbyte	Received bytes	uint64	20

Log Field Name	Description	Data Type	Length
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
sensitivity	Sensitivity for document fingerprint	string	36
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
severity	Severity level of a DLP rule	string	8
srcintf	Source Interface	string	32
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	128
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32

DLP Log Messages

The following table describes the log message IDs and messages of the DLP log.

Message ID	Message	Severity
24576	LOG_ID_DLP_WARN	Warning
24577	LOG_ID_DLP_NOTIF	Notice

Message ID	Message	Severity
24578	LOG_ID_DLP_DOC_SOURCE	Notice
24579	LOG_ID_DLP_DOC_SOURCE_ERROR	Warning

Email

Log Field Name	Description	Data Type	Length
action	Security action of the email filter	string	8
agent	User agent - eg. agent="Mozilla/5.0"	string	64
attachment	The flag for email attachement	string	3
banword	Banned word	string	128
cc	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of packets	string	8
dstintf	Destination Interface	string	64
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtype	Email Filter event type	string	32
from	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	512
policyid	Policy ID	uint32	10

Log Field Name	Description	Data Type	Length
profile	Email Filter profile name	string	64
proto	Protocol number	uint8	3
rcvdbyte	Received Bytes	uint64	20
recipient	Email addresses from the SMTP envelope	string	512
sender	Email addresses from the SMTP envelope	string	128
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
size	Email size in Bytes?	string	16
srcintf	Source Interface	string	64
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
user	User name	string	256
vd	Virtual domain name	string	12

Email Log Messages

The following table describes the log message IDs and messages of the Email log.

Message ID	Message	Severity
20480	LOGID_ANTISPAM_EMAIL_SMTP_NOTIF	Notice

Message ID	Message	Severity
20481	LOGID_ANTISPAM_EMAIL_SMTP_BWORD_NOTIF	Notice
20482	LOGID_ANTISPAM_EMAIL_POP3_NOTIF	Notice
20483	LOGID_ANTISPAM_EMAIL_POP3_BWORD_NOTIF	Notice
20484	LOGID_ANTISPAM_EMAIL_IMAP_NOTIF	Notice
20485	LOGID_ANTISPAM_ENDPOINT_FILTER_WARNING	Warning
20486	LOGID_ANTISPAM_ENDPOINT_FILTER_NOTIF	Notice
20487	LOGID_ANTISPAM_ENDPOINT_MM7_WARNING	Warning
20488	LOGID_ANTISPAM_ENDPOINT_MM7_NOTIF	Notice
20489	LOGID_ANTISPAM_ENDPOINT_MM1_WARNING	Warning
20490	LOGID_ANTISPAM_ENDPOINT_MM1_NOTIF	Notice
20491	LOGID_ANTISPAM_EMAIL_IMAP_BWORD_NOTIF	Notice
20492	LOGID_ANTISPAM_MM1_FLOOD_WARNING	Warning
20493	LOGID_ANTISPAM_MM1_FLOOD_NOTIF	Notice
20494	LOGID_ANTISPAM_MM4_FLOOD_WARNING	Warning
20495	LOGID_ANTISPAM_MM4_FLOOD_NOTIF	Notice
20496	LOGID_ANTISPAM_MM1_DUPE_WARNING	Warning
20497	LOGID_ANTISPAM_MM1_DUPE_NOTIF	Notice
20498	LOGID_ANTISPAM_MM4_DUPE_WARNING	Warning
20499	LOGID_ANTISPAM_MM4_DUPE_NOTIF	Notice
20500	LOGID_ANTISPAM_EMAIL_MSN_NOTIF	Information
20501	LOGID_ANTISPAM_EMAIL_YAHOO_NOTIF	Information
20502	LOGID_ANTISPAM_EMAIL_GOOGLE_NOTIF	Information
20503	LOGID_EMAIL_SMTP_GENERAL_NOTIF	Information
20504	LOGID_EMAIL_POP3_GENERAL_NOTIF	Information

Message ID	Message	Severity
20505	LOGID_EMAIL_IMAP_GENERAL_NOTIF	Information
20506	LOGID_EMAIL_MAPI_GENERAL_NOTIF	Information
20507	LOGID_ANTISPAM_EMAIL_MAPI_BWORD_NOTIF	Notice
20508	LOGID_ANTISPAM_EMAIL_MAPI_NOTIF	Notice
20509	LOGID_ANTISPAM_FTGD_ERR	Information

Event

COMPLIANCE-CHECK

Log Field Name	Description	Data Type	Length
action	Action	string	32
date	Date	string	10
devid	Device ID	string	16
level	Log Level	string	11
logdesc	Log Description	string	
logid	Log ID	string	10
module	Module	string	32
msg	Log Message	string	
reason	Reason	string	256
result	Result	string	31
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
vd	Virtual Domain Name	string	32

COMPLIANCE-CHECK Log Messages

The following table describes the log message IDs and messages of the COMPLIANCE-CHECK log.

Message ID	Message	Severity
45151	LOG_ID_EVENT_DSSCC_FAIL	Unknown
45152	LOG_ID_EVENT_DSSCC_PASS	Unknown

ENDPOINT

Log Field Name	Description	Data Type	Length
action	EndPoint Action	string	32
connection_type	FortiClient Connection Type	string	6
count	Count of EndPoint Connections	uint32	10
cveid		string	1024
date	Date	string	10
devid	Device ID	string	16
devtype		string	32
fctuid		string	32
forticlient_id	Unique FortiClient ID	string	33
hostname	Endpoint Hostname	string	128
interface	Interface	string	32
ip	Source IP	ip	39
level	Log Level	string	11
license_limit	Maximum Number of FortiClients for the License	string	32
license_used	use 'used'?	uint16	5
logdesc	Log Description	string	
logid	Log ID	string	10
msg	Log Message	string	

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
reason	Reason	string	256
repeat	Number of Times Repeated for the Action	uint16	5
scantime		uint64	20
severity		string	10
srcname		string	64
status	Status	string	23
subtype	Log subtype	string	20
time	Time	string	8
type	Log Type	string	16
ui	User Interface	string	64
used_for_type	Connection for the type	uint16	5
user	User Name	string	256
vd	Virtual Domain Name	string	32
vendorurl		string	256
vulncat		string	32
vulnid		uint32	10
vulnname		string	128

ENDPOINT Log Messages

The following table describes the log message IDs and messages of the ENDPOINT log.

Message ID	Message	Severity
45057	LOG_ID_FCC_ADD	Information
45058	LOG_ID_FCC_CLOSE	Information
45061	LOG_ID_FCC_CLOSE_BY_TYPE	Information

Message ID	Message	Severity
45071	LOG_ID_FCC_VULN_SCAN	Notice
45100	LOG_ID_EC_REG_FAIL_LIMIT	Warning
45101	LOG_ID_EC_REG_SUCCEED	Notice
45102	LOG_ID_EC_REG_RENEWED	Notice
45103	LOG_ID_EC_REG_BLOCK	Notice
45104	LOG_ID_EC_REG_UNBLOCK	Notice
45105	LOG_ID_EC_REG_DEREG	Notice
45106	LOG_ID_EC_REG_LIC_UPGRADED	Notice
45107	LOG_ID_EC_CONF_DISTRIBUTED	Notice
45108	LOG_ID_EC_FTCL_UNREG	Notice
45109	LOG_ID_EC_FTCL_LOGOFF	Notice
45110	LOG_ID_EC_FTCL_ENABLE_NOTSYNC	Notice
45111	LOG_ID_EC_REG_SYNC_FAIL	Warning
45112	LOG_ID_EC_REG_FAIL_KEY	Warning
45113	LOG_ID_EC_REG_FAIL_BLOCKED	Warning
45114	LOG_ID_EC_REG_QUARANTINE	Notice
45115	LOG_ID_EC_REG_UNQUARANTINE	Notice
45116	LOG_ID_EC_REG_UNQUARANTINE_ALL	Notice
45117	LOG_ID_EC_REG_FAIL_VER	Warning

HA

Log Field Name	Description	Data Type	Length
activity	HA activity message	string	128
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
devintfname	HA device Interface Name	string	32
from_vcluster	source virtual cluster number	uint32	10
ha-prio	HA Priority	uint8	3
ha_group	HA Group Number - can be 1 - 256	uint8	3
ha_role	The HA role in the cluster	string	6
hbdn_reason	heartbeat down reason	string	18
ip		ip	39
level	Log Level	string	11
logdesc	Log Description	string	
logid	Log ID	string	10
msg	Log Message	string	
sn	Serial Number	string	64
subtype	Log Subtype	string	20
sync_status	The sync status with the master	string	11
sync_type	The sync type with the master	string	14
time	Time	string	8
to_vcluster	destination virtual cluster number	uint32	10
type	Log Type	string	16
vcluster	virtual cluster id	uint32	10
vcluster_member	virtual cluster member id	uint32	10
vcluster_state	virtual cluster state	string	7
vd	Virtual Domain Name	string	32
vdname	vdom name	string	16

HA Log Messages

The following table describes the log message IDs and messages of the HA log.

Message ID	Message	Severity
35001	LOG_ID_HA_SYNC_VIRDB	Notice
35002	LOG_ID_HA_SYNC_ETDB	Notice
35003	LOG_ID_HA_SYNC_EXDB	Notice
35004	LOG_ID_HA_SYNC_FLDB	Notice
35005	LOG_ID_HA_SYNC_IPS	Notice
35007	LOG_ID_HA_SYNC_AV	Notice
35009	LOG_ID_HA_SYNC_CID	Notice
35010	LOG_ID_HA_SYNC_UWDB	Notice
35011	LOG_ID_HA_SYNC_FAIL	Error
35012	LOG_ID_CONF_SYNC_FAIL	Error
37888	MESGID_HA_GROUP_DELETE	Notice
37889	MESGID_VC_DELETE	Notice
37890	MESGID_VC_MOVE_VDOM	Notice
37891	MESGID_VC_ADD_VDOM	Notice
37892	MESGID_VC_MOVE_MEMB_STATE	Notice
37893	MESGID_VC_DETECT_MEMB_DEAD	Critical
37894	MESGID_VC_DETECT_MEMB_JOIN	Critical
37895	MESGID_VC_ADD_HADEV	Notice
37896	MESGID_VC_DEL_HADEV	Notice
37897	MESGID_HADEV_READY	Notice
37898	MESGID_HADEV_FAIL	Warning
37899	MESGID_HADEV_PEERINFO	Notice

Message ID	Message	Severity
37900	MESGID_HBDEV_DELETE	Notice
37901	MESGID_HBDEV_DOWN	Critical
37902	MESGID_HBDEV_UP	Information
37903	MESGID_SYNC_STATUS	Information
37904	MESGID_HA_ACTIVITY	Notice
37905	MESGID_HA_ENABLE_SET_AS_MASTER	Notice
37906	MESGID_HA_DISABLE_SET_AS_MASTER	Notice
37907	MESGID_VLAN_HB_UP	Information
37908	MESGID_VLAN_HB_DOWN	Error
37909	MESGID_VLAN_HB_DOWN_SUM	Error

ROUTER

Log Field Name	Description	Data Type	Length
action	Action	string	32
date	Date	string	10
ddnsserver	DDNS Server	ip	39
devid	Device ID	string	16
dhcp_msg	DHCP Message	string	
dns_ip	DNS IP	ip	39
dns_name	DNS Name	string	64
dst_int	Destination Interface	string	64
duid		string	128
iaid		uint32	10
interface	Interface	string	32

Log Field Name	Description	Data Type	Length
lease		uint32	10
level	Log Level	string	11
logdesc	Log Description	string	
logid	Log ID	string	10
mac	Mac Address	string	17
msg	Message	string	
service	Name of Service	string	64
src_int	Source Interface	string	64
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
vd	Virtual Domain Name	string	32

ROUTER Log Messages

The following table describes the log message IDs and messages of the ROUTER log.

Message ID	Message	Severity
20300	LOG_ID_BGP_NB_STAT_CHG	Unknown
20301	LOG_ID_VZ_LOG	Information
20302	LOG_ID_OSPF_NB_STAT_CHG	Unknown
20303	LOG_ID_OSPF6_NB_STAT_CHG	Unknown
20401	LOG_ID_ROUTER_CLEAR	Notice
27001	LOG_ID_VRRP_STATE_CHG	Information
51000	51000	Information

SYSTEM

Log Field Name	Description	Data Type	Length
acktime	Alarm Acknowledge Time	string	24
act		string	16
action	Action	string	32
addr	IP Address	string	80
alarmid	Alarm ID	uint32	10
assigned	Assigned IP Address	ip	39
bandwidth	Bandwidth	string	42
banned_rule	NAC quarantine Banned Rule Name	string	36
banned_src	NAC quarantine Banned Source IP	string	16
blocked	Blocked MMS	uint32	10
cert	Certificate	string	36
cfgattr	configuration attribute	string	
cfgobj	configuration object	string	256
cfgpath	configuration path	string	128
cfgtid	config transaction id	uint32	10
chassisid	Chassis ID	uint8	
checksum	for MMS Statistics	uint32	10
cipher	Encryption Type	uint16	
community	Community	string	36
conserve	Flag for Conserve Mode	string	32
count	Count	uint32	10
cpu	CPU Usage	uint8	3
created	Sessions Created	string	64

Log Field Name	Description	Data Type	Length
crl		string	
daddr	Destination IP Address	string	80
daemon	Daemon Name	string	32
datarange	data range for reports	string	50
date	Date	string	10
ddnsserver	DDNS Server	ip	39
desc	Description	string	128
devid	Device ID	string	16
dhcp_msg	DHCP Message	string	
dintf	Destination Interface	string	36
disk	Disk Usage	uint8	3
disklograte	Disk Log Rate	uint64	20
dns_ip	DNS IP Address	ip	39
dns_name	DNS Name	string	64
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
dst_int	Destination Interface	string	64
duid		string	128
duration	Duration	uint32	10
entermargin	Conserve Mode Enter Margin	uint32	10
error	Error Reason for Log Upload to Forticloud	string	256
exitmargin	Conserve Mode Exit Margin	uint32	10
expectedhandshake	Expected Handshake	string	
expectedsignature	Expected Signature	uint8	

Log Field Name	Description	Data Type	Length
fams_pause	Fortinet Analysis and Management Service Pause	uint32	10
fazlograte	FortiAnalyzer Logging Rate	uint64	20
field		string	32
file	File Name for Generated Report?	string	256
filesize	Report File Size in Bytes	uint32	
free		string	32
from	Sender Email Address for Notification	string	128
gateway	gateway ip address for PPPoE status report	ip	39
green		string	32
group	User group Name	string	64
groupid	User Group ID	uint32	10
handshake	Handshake	string	32
hash	Hash Value of Downloaded File	string	32
hostname	Hostname	string	128
iaid		uint32	10
identidx	use 'id' ?	uint32	10
infected	Infected MMS	uint32	10
informationsource	Information Source	string	
intercepted	Intercepted MMS	uint32	10
interface	Interface	string	32
intf	Interface	string	16
ip		ip	39
iptype	IP Protocol Type	string	16
lease	DHCP Lease	uint32	10

Log Field Name	Description	Data Type	Length
len	SSL Handshake Message Length	uint32	10
level	Log Level	string	11
limit	Virtual Domain Resource Limit	uint32	10
local	Local IP for a PPPD Connection	ip	39
log	Log Name for Log Rotation	string	32
logdesc	Log Description	string	
logid	Log ID	string	10
mac	Mac Address	string	17
major	Major Version	uint8	
max	Max Value	uint8	
maxminor		uint8	
mem	Memory Usage	uint8	3
member		uint8	
min	Minimum Value	uint8	
minminor		uint8	
minor	SSL Minor Version	uint8	
mode	Mode	string	12
module	Configuration Module Name	string	32
monitor-name	Health Monitor Type	string	35
monitor-type	Health Monitor Name	string	32
msg	Message Text	string	
msgproto	Message Protocol Number	string	16
mtu	Max Transmission Unit Value	uint32	10
name	Name	string	128

Log Field Name	Description	Data Type	Length
nat	NAT IP Address	ip	39
newchannel	New Channel Number	uint8	
newchassisid	New Chassis ID	uint8	
newslot	New Slot Number	uint8	
new_status	New Status	string	512
new_value	New Virtual Domain Name	string	128
nf_type	Notification Type	string	14
oldchannel	Original Channel Number	uint8	
oldchassisid	Original Chassis Number	uint8	
oldslot	Original Slot Number	uint8	
old_status	Original Status	string	512
old_value	Original Virtual Domain name	string	128
passwd	Password	string	20
pid	Process ID	uint32	10
policyid	Policy ID	uint32	10
poolname	IP Pool Name	string	36
port	Port Number	uint16	5
portbegin	Port Number to Begin	uint16	5
portend	Port Number to End	uint16	5
probeproto	Link Monitor Probe Protocol	string	16
process	Process	string	
processtime	process time for reports	uint32	
profile	Profile Name	string	64
profilegroup	Profile Group Name	string	4

Log Field Name	Description	Data Type	Length
profiletype	Profile Type	string	64
profile_vd	Virtual Domain Name	string	64
proto	Protocol Number	uint8	3
reason	Reason	string	256
received	Received Packet	uint8	
receivedhandshake	Received Handshake	string	
receivedsignature	Received Signature	uint8	
recvminor		uint8	
red		string	32
remote	Remote IP Address	ip	39
reporttype	Report Type	string	20
saddr	Source Address IP	string	80
scanned	Number of Scanned MMSs	uint32	10
sensor	NAC Sensor Name	string	36
serial	Serial Number	uint32	10
serialno	Serial Number	string	16
server	Server IP Address	string	64
service	Name of Service	string	64
session_id	Session ID	uint32	10
sess_duration	Session Duration	uint32	10
setuprate	Session Setup Rate	uint64	20
slot	Slot Number	uint8	
sn	Serial Number	string	64
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
src_int	Source Interface	string	64
ssl2		uint8	
state	State	string	64
status	Status	string	23
submodule	Configuration Sub-Module Name	string	32
subtype	Log Subtype	string	20
suspicious	Number of Suspicious MMSs	uint32	10
sysconserve	On/Off Flag for Server Conserve Mode	string	32
time	Time	string	8
to	Recipient Email Addresses for Notification	string	512
total	Total	uint32	10
totalsession	Total Number of Sessions	uint32	10
trace_id	ID for Tracing	string	32
type	Log Type	string	16
ui	User Interface	string	64
unit	Unit	uint32	10
url	URL	string	512
used	Number of Used IPs	uint32	10
user	User Name	string	256
vd	Virtual Domain Name	string	32
version	Version	string	64
vip	Virtual IP	string	64
virus	Virus Name	string	128

SYSTEM Log Messages

The following table describes the log message IDs and messages of the SYSTEM log.

Message ID	Message	Severity
20001	LOG_ID_CLIENT_DISASSOCIATED	Information
20002	LOG_ID_DOMAIN_UNRESOLVABLE	Notice
20003	LOG_ID_MAIL_SENT_FAIL	Notice
20004	LOG_ID_POLICY_TOO_BIG	Unknown
20005	LOG_ID_PPP_LINK_UP	Information
20006	LOG_ID_PPP_LINK_DOWN	Information
20007	20007	Critical
20008	LOG_ID_POLICY6_TOO_BIG	Unknown
20010	LOG_ID_KERNEL_ERROR	Critical
20011	LOG_ID_CLIENT_NEW_ASSOCIATION	Information
20012	LOG_ID_CLIENT_WPA_1X	Information
20013	LOG_ID_CLIENT_WPA_SSN	Information
20015	LOG_ID_IEEE802_NEW_STATION	Information
20016	LOG_ID_MODEM_EXCEED_REDIAL_COUNT	Information
20017	LOG_ID_MODEM_FAIL_TO_OPEN	Information
20020	LOG_ID_MODEM_USB_DETECTED	Warning
20021	LOG_ID_MAIL_RESENT	Information
20022	LOG_ID_MODEM_USB_REMOVED	Warning
20023	LOG_ID_MODEM_USBLTE_DETECTED	Information
20024	LOG_ID_MODEM_USBLTE_REMOVED	Information
20025	LOG_ID_REPORTD_REPORT_SUCCESS	Notice
20026	LOG_ID_REPORTD_REPORT_FAILURE	Error

Message ID	Message	Severity
20027	LOG_ID_REPORT_DEL_OLD_REC	Information
20028	LOG_ID_REPORT_RECREATE_DB	Warning
20031	LOG_ID_RAD_OUT_OF_MEM	Critical
20032	LOG_ID_RAD_NOT_FOUND	Critical
20033	LOG_ID_RAD_MOBILE_IPV6	Information
20034	LOG_ID_RAD_IPV6_OUT_OF_RANGE	Critical
20035	LOG_ID_RAD_MIN_OUT_OF_RANGE	Critical
20036	LOG_ID_RAD_MAX_OUT_OF_RANGE	Critical
20037	LOG_ID_RAD_MAX_ADV_OUT_OF_RANGE	Critical
20038	LOG_ID_RAD_MTU_OUT_OF_RANGE	Critical
20039	LOG_ID_RAD_MTU_TOO_SMALL	Critical
20040	LOG_ID_RAD_TIME_TOO_SMALL	Critical
20041	LOG_ID_RAD_HOP_OUT_OF_RANGE	Critical
20042	LOG_ID_RAD_DFT_HOP_OUT_OF_RANGE	Critical
20043	LOG_ID_RAD_AGENT_OUT_OF_RANGE	Critical
20044	LOG_ID_RAD_AGENT_FLAG_NOT_SET	Critical
20045	LOG_ID_RAD_PREFIX_TOO_LONG	Critical
20046	LOG_ID_RAD_PREF_TIME_TOO_SMALL	Critical
20047	LOG_ID_RAD_FAIL_IPV6_SOCKET	Critical
20048	LOG_ID_RAD_FAIL_OPT_IPV6_PKTINFO	Critical
20049	LOG_ID_RAD_FAIL_OPT_IPV6_CHECKSUM	Critical
20050	LOG_ID_RAD_FAIL_OPT_IPV6_UNICAST_HOPS	Critical
20051	LOG_ID_RAD_FAIL_OPT_IPV6_MULTICAST_HOPS	Critical
20052	LOG_ID_RAD_FAIL_OPT_IPV6_HOPLIMIT	Critical

Message ID	Message	Severity
20053	LOG_ID_RAD_FAIL_OPT_IPPROTO_ICMPV6	Critical
20054	LOG_ID_RAD_EXIT_BY_SIGNAL	Information
20055	LOG_ID_RAD_FAIL_CMDB_QUERY	Critical
20056	LOG_ID_RAD_FAIL_CMDB_FOR_EACH	Critical
20057	LOG_ID_RAD_FAIL_FIND_VIRT_INTF	Critical
20058	LOG_ID_RAD_UNLOAD_INTF	Information
20059	LOG_ID_RAD_NO_PKT_INFO	Warning
20060	LOG_ID_RAD_INV_ICMPV6_LEN	Warning
20061	LOG_ID_RAD_INV_ICMPV6_TYPE	Critical
20062	LOG_ID_RAD_INV_ICMPV6_RA_LEN	Warning
20063	LOG_ID_RAD_ICMPV6_NO_SRC_ADDR	Warning
20064	LOG_ID_RAD_INV_ICMPV6_RS_LEN	Warning
20065	LOG_ID_RAD_INV_ICMPV6_CODE	Warning
20066	LOG_ID_RAD_INV_ICMPV6_HOP	Warning
20067	LOG_ID_RAD_MISMATCH_HOP	Warning
20068	LOG_ID_RAD_MISMATCH_MGR_FLAG	Warning
20069	LOG_ID_RAD_MISMATCH_OTH_FLAG	Warning
20070	LOG_ID_RAD_MISMATCH_TIME	Warning
20071	LOG_ID_RAD_MISMATCH_TIMER	Warning
20072	LOG_ID_RAD_EXTRA_DATA	Critical
20073	LOG_ID_RAD_NO_OPT_DATA	Critical
20074	LOG_ID_RAD_INV_OPT_LEN	Critical
20075	LOG_ID_RAD_MISMATCH_MTU	Warning
20077	LOG_ID_RAD_MISMATCH_PREF_TIME	Warning

Message ID	Message	Severity
20078	LOG_ID_RAD_INV_OPT	Critical
20079	LOG_ID_RAD_READY	Information
20080	LOG_ID_RAD_FAIL_TO_RCV	Critical
20081	LOG_ID_RAD_INV_HOP	Critical
20082	LOG_ID_RAD_INV_PKTINFO	Critical
20083	LOG_ID_RAD_FAIL_TO_CHECK	Warning
20084	LOG_ID_RAD_FAIL_TO_SEND	Warning
20085	20085	Information
20086	20086	Unknown
20090	LOG_ID_INTF_LINK_STA_CHG	Notice
20099	LOG_ID_INTF_STA_CHG	Warning
20100	LOG_ID_WEB_CAT_UPDATED	Critical
20101	LOG_ID_WEB_LIC_EXPIRE	Warning
20102	LOG_ID_SPAM_LIC_EXPIRE	Warning
20103	LOG_ID_AV_LIC_EXPIRE	Warning
20104	LOG_ID_IPS_LIC_EXPIRE	Warning
20105	LOG_ID_LOG_UPLOAD_SKIP	Warning
20107	LOG_ID_LOG_UPLOAD_ERR	Warning
20108	LOG_ID_LOG_UPLOAD_DONE	Notice
20109	LOG_ID_WEB_LIC_EXPIRED	Critical
20110	LOG_ID_HPAPI_ESPD_START	Notice
20111	LOG_ID_HPAPI_ESPD_RESET	Warning
20113	LOG_ID_IPSA_DOWNLOAD_FAIL	Error
20114	LOG_ID_IPSA_SELFTEST_FAIL	Error

Message ID	Message	Severity
20115	LOG_ID_IPSA_STATUSUPD_FAIL	Error
20116	LOG_ID_SPAM_LIC_EXPIRED	Critical
20118	LOG_ID_WEBF_STATUS_REACH	Warning
20119	LOG_ID_WEBF_STATUS_UNREACH	Warning
20200	LOG_ID_FIPS_SELF_TEST	Notice
20201	LOG_ID_FIPS_SELF_ALL_TEST	Notice
20202	LOG_ID_DISK_FORMAT_ERROR	Warning
20203	LOG_ID_DAEMON_SHUTDOWN	Information
20204	LOG_ID_DAEMON_START	Information
20205	LOG_ID_DISK_FORMAT_REQ	Critical
20206	LOG_ID_DISK_SCAN_REQ	Warning
20207	LOG_ID_RAD_MISMATCH_VALID_TIME	Warning
20208	LOG_ID_ZOMBIE_DAEMON_CLEANUP	Information
20209	LOG_ID_DISK_UNAVAIL	Critical
20220	20220	Information
20221	20221	Information
22000	LOG_ID_INV_PKT_LEN	Warning
22001	LOG_ID_UNSUPPORTED_PROT_VER	Warning
22002	LOG_ID_INV_REQ_TYPE	Warning
22003	LOG_ID_FAIL_SET_SIG_HANDLER	Warning
22004	LOG_ID_FAIL_CREATE_SOCKET	Warning
22005	LOG_ID_FAIL_CREATE_SOCKET_RETRY	Warning
22006	LOG_ID_FAIL_REG_CMDB_EVENT	Warning
22009	LOG_ID_FAIL_FIND_AV_PROFILE	Warning

Message ID	Message	Severity
22010	LOG_ID_SENDTO_FAIL	Error
22011	22011	Unknown
22012	22012	Unknown
22013	22013	Alert
22014	22014	Alert
22015	22015	Notice
22016	22016	Notice
22017	LOG_ID_EXCEED_GLOB_RES_LIMIT	Notice
22018	LOG_ID_EXCEED_VD_RES_LIMIT	Notice
22020	LOG_ID_FAIL_CREATE_HA_SOCKET	Warning
22021	LOG_ID_FAIL_CREATE_HA_SOCKET_RETRY	Warning
22100	LOG_ID_QUAR_DROP_TRAN_JOB	Warning
22101	LOG_ID_QUAR_DROP_TLL_JOB	Warning
22102	LOG_ID_LOG_DISK_FAILURE	Critical
22103	LOG_ID_QUAR_DAILY_LIMIT_REACHED	Warning
22104	LOG_ID_POWER_RESTORE	Critical
22105	LOG_ID_POWER_FAILURE	Critical
22106	LOG_ID_POWER_OPTIONAL_NOT_DETECTED	Warning
22107	LOG_ID_VOLT_ANOM	Warning
22108	LOG_ID_FAN_ANOM	Warning
22109	LOG_ID_TEMP_TOO_HIGH	Warning
22110	LOG_ID_SPARE_BLOCK_LOW	Critical
22150	LOG_ID_VOLT_NOM	Notice
22151	LOG_ID_FAN_NOM	Notice

Message ID	Message	Severity
22152	LOG_ID_TEMP_TOO_LOW	Warning
22153	LOG_ID_TEMP_NORM	Notice
22200	LOG_ID_AUTO_UPT_CERT	Warning
22201	LOG_ID_AUTO_GEN_CERT	Warning
22203	LOG_ID_AUTO_GEN_CERT_FAIL	Error
22204	LOG_ID_AUTO_GEN_CERT_PENDING	Information
22205	LOG_ID_AUTO_GEN_CERT_SUCC	Information
22206	LOG_ID_CRL_EXPIRED	Warning
22700	LOG_ID_IPS_FAIL_OPEN	Critical
22701	LOG_ID_IPS_FAIL_OPEN_END	Critical
22800	LOG_ID_SCAN_SERV_FAIL	Critical
22801	LOG_ID_SCAN_LEAVE_CONSERVE_MODE	Critical
22802	LOG_ID_SYS_ENTER_CONSERVE_MODE	Critical
22803	LOG_ID_SYS_LEAVE_CONSERVE_MODE	Critical
22804	LOG_ID_LIC_STATUS_CHG	Critical
22805	LOG_ID_FAIL_TO_VALIDATE_LIC	Warning
22806	LOG_ID_DUP_LIC	Warning
22810	LOG_ID_SCAN_ENTER_CONSERVE_MODE	Critical
22891	LOG_ID_FLCFGD	Error
22900	LOG_ID_CAPUTP_SESSION	Error
22901	LOG_ID_FAZ_CON	Notice
22902	LOG_ID_FAZ_DISCON	Notice
22903	LOG_ID_FAZ_CON_ERR	Critical
22913	LOG_ID_FDS_SRV_DISCON	Notice

Message ID	Message	Severity
22914	LOG_ID_FDS_SRV_CHG	Notice
22915	LOG_ID_FDS_SRV_CON	Notice
22916	LOG_ID_FDS_STATUS	Notice
22917	LOG_ID_FDS_SMS_QUOTA	Notice
22918	LOG_ID_FDS_CTRL_STATUS	Notice
22921	LOG_ID_EVENT_ROUTE_INFO_CHANGED	Critical
22922	LOG_ID_EVENT_LINK_MONITOR_STATUS	Notice
22923	LOG_ID_EVENT_VWL_LQTY_STATUS	Notice
22924	LOG_ID_EVENT_VWL_VOLUME_STATUS	Notice
26001	LOG_ID_DHCP_ACK	Information
26002	LOG_ID_DHCP_RELEASE	Information
26003	LOG_ID_DHCP_STAT	Information
26004	LOG_ID_DHCP_CLIENT_LEASE	Information
26005	LOG_ID_DHCP_LEASE_USAGE_HIGH	Warning
26006	LOG_ID_DHCP_LEASE_USAGE_FULL	Warning
26007	LOG_ID_DHCP_BLOCKED_MAC	Information
26008	LOG_ID_DHCP_DDNS_ADD	Information
26009	LOG_ID_DHCP_DDNS_DELETE	Information
26010	LOG_ID_DHCP_DDNS_COMPLETED	Information
26011	LOG_ID_DHCPV6_REPLY	Information
26012	LOG_ID_DHCPV6_RELEASE	Information
29001	LOG_ID_PPPD_MSG	Unknown
29002	LOG_ID_PPPD_AUTH_SUC	Notice
29003	LOG_ID_PPPD_AUTH_FAIL	Notice

Message ID	Message	Severity
29009	LOG_ID_PPPOE_STATUS_REPORT	Notice
29011	LOG_ID_PPPD_FAIL_TO_EXEC	Error
29012	LOG_ID_PPP_OPT_ERR	Unknown
29013	LOG_ID_PPPD_START	Notice
29014	LOG_ID_PPPD_EXIT	Information
29015	LOG_ID_PPP_RCV_BAD_PEER_IP	Error
29016	LOG_ID_PPP_RCV_BAD_LOCAL_IP	Error
29017	LOG_ID_PPP_OPT_NOTIF	Unknown
29020	LOG_ID_WIRELESS_SET_FAIL	Notice
29021	LOG_ID_EVENT_AUTH_SNMP_QUERY_FAILED	Warning
29022	LOG_ID_DDNS_UPDATE_FAIL	Error
32001	LOG_ID_ADMIN_LOGIN_SUCC	Unknown
32002	LOG_ID_ADMIN_LOGIN_FAIL	Alert
32003	LOG_ID_ADMIN_LOGOUT	Unknown
32005	LOG_ID_ADMIN_OVERIDE_VDOM	Information
32006	LOG_ID_ADMIN_ENTER_VDOM	Information
32007	LOG_ID_ADMIN_LEFT_VDOM	Information
32008	LOG_ID_VIEW_DISK_LOG_FAIL	Warning
32009	LOG_ID_SYSTEM_START	Information
32010	LOG_ID_DISK_LOG_FULL	Warning
32011	LOG_ID_LOG_ROLL	Notice
32012	LOG_ID_FIPS_LEAVE_ERR_MOD	Information
32014	LOG_ID_CS_LIC_EXPIRE	Warning
32015	LOG_ID_DISK_LOG_USAGE	Warning

Message ID	Message	Severity
32016	LOG_ID_FDS_QUOTA_WARN	Emergency
32017	LOG_ID_FDS_DAILY_QUOTA_FULL	Alert
32018	LOG_ID_FIPS_ENTER_ERR_MOD	Emergency
32019	LOG_ID_CC_ENTER_ERR_MOD	Emergency
32020	LOG_ID_SSH_CORRPUT_MAC	Warning
32021	LOG_ID_ADMIN_LOGIN_DISABLE	Alert
32022	LOG_ID_VDOM_ENABLED	Notice
32023	LOG_ID_MEM_LOG_FIRST_FULL	Information
32024	LOG_ID_ADMIN_PASSWD_EXPIRE	Notice
32027	LOG_ID_VIEW_DISK_LOG_SUCC	Notice
32028	LOG_ID_LOG_DEL_DIR	Information
32029	LOG_ID_LOG_DEL_FILE	Warning
32030	LOG_ID_SEND_FDS_STAT	Notice
32031	LOG_ID_VIEW_MEM_LOG_FAIL	Warning
32032	LOG_ID_DISK_DLP_ARCH_FULL	Emergency
32033	LOG_ID_DISK_QUAR_FULL	Emergency
32034	LOG_ID_DISK_REPORT_FULL	Emergency
32035	LOG_ID_VDOM_DISABLED	Notice
32036	LOG_ID_DISK_IPS_ARCH_FULL	Emergency
32037	LOG_ID_DISK_LOG_FIRST_FULL	Information
32038	LOG_ID_LOG_ROLL_FORTICRON	Notice
32039	LOG_ID_VIEW_MEM_LOG_SUCC	Notice
32040	LOG_ID_REPORT_DELETED	Information
32041	LOG_ID_REPORT_DELETED_GUI	Information

Message ID	Message	Severity
32042	LOG_ID_MEM_LOG_SECOND_FULL	Warning
32043	LOG_ID_MEM_LOG_FINAL_FULL	Warning
32044	LOG_ID_LOG_DELETE	Notice
32045	LOG_ID_MGR_LIC_EXPIRE	Warning
32046	LOG_ID_SSL_CORRPUT_MAC	Warning
32048	LOG_ID_SCHEDULE_EXPIRE	Warning
32049	LOG_ID_FC_EXPIRE	Warning
32051	LOG_ID_LOG_UPLOAD	Notice
32086	LOG_ID_ENTER_TRANSPARENT	Warning
32087	LOG_ID_ENTER_NAT	Warning
32095	LOG_ID_GUI_CHG_SUB_MODULE	Warning
32096	LOG_ID_GUI_DOWNLOAD_LOG	Warning
32100	LOG_ID_FORTI_TOKEN_SYNC	Warning
32101	LOG_ID_LCD_CHG_CONF	Notice
32102	LOG_ID_CHG_CONFIG	Unknown
32103	LOG_ID_NEW_FIRMWARE	Notice
32104	LOG_ID_CHG_CONFIG_GUI	Unknown
32105	LOG_ID_NTP_SVR_STAUS_CHG_REACHABLE	Notice
32106	LOG_ID_NTP_SVR_STAUS_CHG_RESOLVABLE	Notice
32107	LOG_ID_NTP_SVR_STAUS_CHG_UNRESOLVABLE	Notice
32108	LOG_ID_NTP_SVR_STAUS_CHG_UNREACHABLE	Notice
32109	LOG_ID_UPD_SIGN_AV_DB	Critical
32110	LOG_ID_UPD_SIGN_IPS_DB	Critical
32111	LOG_ID_UPD_SIGN_AVIPS_DB	Critical

Message ID	Message	Severity
32113	LOG_ID_UPD_SIGN_SRCVIS_DB	Critical
32114	LOG_ID_UPD_SIGN_GEOIP_DB	Critical
32115	LOG_ID_UPD_SIGN_SERVER_LIST	Critical
32116	LOG_ID_UPD_SIGN_AVPKG_FAILURE	Warning
32117	LOG_ID_UPD_SIGN_AVPKG_SUCCESS	Warning
32118	LOG_ID_UPD_ADMIN_AV_DB	Notice
32119	LOG_ID_UPD_SCANUNIT_AV_DB	Critical
32120	LOG_ID_RPT_ADD_DATASET	Notice
32122	LOG_ID_RPT_DEL_DATASET	Notice
32125	LOG_ID_RPT_ADD_CHART	Notice
32126	LOG_ID_RPT_DEL_CHART	Notice
32129	LOG_ID_ADD_GUEST	Notice
32130	LOG_ID_CHG_USER	Notice
32131	LOG_ID_DEL_GUEST	Notice
32132	LOG_ID_ADD_USER	Notice
32138	LOG_ID_REBOOT	Critical
32140	LOG_ID_TIME_USER_SETTING_CHG	Notice
32141	LOG_ID_TIME_NTP_SETTING_CHG	Notice
32142	LOG_ID_BACKUP_CONF	Alert
32143	LOG_ID_BACKUP_CONF_BY_SCP	Warning
32148	LOG_ID_GET_CRL	Notice
32149	LOG_ID_COMMAND_FAIL	Notice
32151	LOG_ID_ADD_IP6_LOCAL_POL	Notice
32152	LOG_ID_CHG_IP6_LOCAL_POL	Notice

Message ID	Message	Severity
32153	LOG_ID_DEL_IP6_LOCAL_POL	Notice
32155	LOG_ID_ACT_FTOKEN_REQ	Notice
32156	LOG_ID_ACT_FTOKEN_SUCC	Notice
32157	LOG_ID_SYNC_FTOKEN_SUCC	Notice
32158	LOG_ID_SYNC_FTOKEN_FAIL	Notice
32159	LOG_ID_ACT_FTOKEN_FAIL	Notice
32168	LOG_ID_REACH_VDOM_LIMIT	Notice
32169	LOG_ID_ALARM_DLP_DB	Alert
32170	LOG_ID_ALARM_MSG	Alert
32171	LOG_ID_ALARM_ACK	Alert
32172	LOG_ID_ADD_IP4_LOCAL_POL	Notice
32173	LOG_ID_CHG_IP4_LOCAL_POL	Notice
32174	LOG_ID_DEL_IP4_LOCAL_POL	Notice
32190	LOG_ID_UPT_INVALID_IMG	Critical
32191	LOG_ID_UPT_INVALID_IMG_CC	Critical
32192	LOG_ID_UPT_INVALID_IMG_RSA	Critical
32193	LOG_ID_UPT_IMG_RSA	Critical
32194	LOG_ID_UPT_IMG_FAIL	Critical
32199	LOG_ID_RESTORE_IMG_USB	Critical
32200	LOG_ID_SHUTDOWN	Critical
32201	LOG_ID_LOAD_IMG_SUCC	Critical
32202	LOG_ID_RESTORE_IMG	Critical
32203	LOG_ID_RESTORE_CONF	Critical
32204	LOG_ID_RESTORE_FGD_SVR	Critical

Message ID	Message	Severity
32205	LOG_ID_RESTORE_VDOM_LIC	Critical
32206	LOG_ID_RESTORE_SCRIPT	Warning
32207	LOG_ID_RETRIEVE_CONF_LIST	Warning
32208	LOG_ID_IMP_PKCS12_CERT	Critical
32209	LOG_ID_RESTORE_USR_DEF_IPS	Critical
32210	LOG_ID_BACKUP_IMG_SUCC	Notice
32211	LOG_ID_UPLOAD_REVISION	Notice
32212	LOG_ID_DEL_REVISION	Notice
32213	LOG_ID_RESTORE_TEMPLATE	Warning
32214	LOG_ID_RESTORE_FILE	Warning
32215	LOG_ID_UPT_IMG	Critical
32217	LOG_ID_UPD_IPS	Notice
32218	LOG_ID_UPD_DLP	Warning
32219	LOG_ID_BACKUP_OUTPUT	Warning
32220	LOG_ID_BACKUP_COMMAND	Warning
32221	LOG_ID_UPD_VDOM_LIC	Warning
32222	LOG_ID_GLB_SETTING_CHG	Notice
32223	LOG_ID_BACKUP_USER_DEF_IPS	Notice
32224	LOG_ID_BACKUP_DISK_LOG	Notice
32225	LOG_ID_DEL_ALL_REVISION	Notice
32226	LOG_ID_LOAD_IMG_FAIL	Critical
32227	LOG_ID_UPD_DLP_FAIL	Warning
32228	LOG_ID_LOAD_IMG_FAIL_WRONG_IMG	Critical
32229	LOG_ID_LOAD_IMG_FAIL_NO_RSA	Critical

Message ID	Message	Severity
32230	LOG_ID_LOAD_IMG_FAIL_INVALID_RSA	Critical
32231	LOG_ID_RESTORE_FGD_SVR_FAIL	Notice
32232	LOG_ID_RESTORE_VDOM_LIC_FAIL	Notice
32233	LOG_ID_BACKUP_IMG_FAIL	Notice
32234	LOG_ID_RESTORE_IMG_INVALID_CC	Critical
32235	LOG_ID_RESTORE_IMG_FORTIGUARD	Critical
32236	LOG_ID_BACKUP_MEM_LOG	Notice
32237	LOG_ID_BACKUP_MEM_LOG_FAIL	Notice
32238	LOG_ID_BACKUP_DISK_LOG_FAIL	Notice
32239	LOG_ID_BACKUP_DISK_LOG_USB	Notice
32240	LOG_ID_SYS_USB_MODE	Critical
32241	LOG_ID_BACKUP_DISK_LOG_USB_FAIL	Notice
32242	LOG_ID_UPD_VDOM_LIC_FAIL	Warning
32243	LOG_ID_UPD_IPS_SCP	Warning
32244	LOG_ID_UPD_IPS_SCP_FAIL	Warning
32245	LOG_ID_BACKUP_USER_DEF_IPS_FAIL	Error
32252	LOG_ID_FACTORY_RESET	Critical
32253	LOG_ID_FORMAT_RAID	Critical
32254	LOG_ID_ENABLE_RAID	Critical
32255	LOG_ID_DISABLE_RAID	Critical
32300	LOG_ID_UPLOAD_RPT_IMG	Notice
32301	LOG_ID_ADD_VDOM	Notice
32302	LOG_ID_DEL_VDOM	Notice
32400	LOG_ID_CONF_CHG	Alert

Message ID	Message	Severity
32545	LOG_ID_SYS_RESTART	Critical
32546	LOG_ID_APPLICATION_CRASH	Warning
32547	LOG_ID_AUTOSCRIPT_START	Information
32548	LOG_ID_AUTOSCRIPT_STOP	Information
32561	LOG_ID_ADMIN_LOGOUT_DISCONNECT	Unknown
32562	LOG_ID_STORE_CONF_FAIL_SPACE	Critical
32564	LOG_ID_RESTORE_CONF_FAIL	Warning
32565	LOG_ID_RESTORE_CONF_BY_MGMT	Warning
32566	LOG_ID_RESTORE_CONF_BY_SCP	Critical
32567	LOG_ID_RESTORE_CONF_BY_USB	Critical
32568	LOG_ID_DEL_REVISION_DB	Notice
32569	LOG_ID_FSW_SWITCH_LOG_EVENT	Unknown
36880	LOG_ID_EVENT_SYSTEM_MAC_HOST_STORE_LIMIT	Warning
38400	LOGID_EVENT_NOTIF_SEND_SUCC	Notice
38401	LOGID_EVENT_NOTIF_SEND_FAIL	Warning
38402	LOGID_EVENT_NOTIF_DNS_FAIL	Notice
38403	LOGID_EVENT_NOTIF_INSUFFICIENT_RESOURCE	Critical
38404	LOGID_EVENT_NOTIF_HOSTNAME_ERROR	Error
38405	LOGID_NOTIF_CODE_SENDTO_SMS_PHONE	Notice
38406	LOGID_NOTIF_CODE_SENDTO_SMS_TO	Notice
38407	LOGID_NOTIF_CODE_SENDTO_EMAIL	Notice
38408	LOGID_EVENT_OFTP_SSL_CONNECTED	Information
38409	LOGID_EVENT_OFTP_SSL_DISCONNECTED	Information
38410	LOGID_EVENT_OFTP_SSL_FAILED	Information

Message ID	Message	Severity
38411	LOGID_EVENT_TWO_F_AUTH_CODE_SENDTO	Notice
38412	LOGID_EVENT_TOKEN_CODE_SENDTO	Notice
40704	LOG_ID_EVENT_SYS_PERF	Notice
41000	LOG_ID_UPD_FGT_SUCC	Notice
41001	LOG_ID_UPD_FGT_FAIL	Critical
41002	LOG_ID_UPD_SRC_VIS	Notice
41003	LOG_ID_INVALID_UPD_LIC	Critical
42201	LOG_ID_NETX_VMX_ATTACH	Notice
42203	LOG_ID_NETX_VMX_DENIED	Notice
43264	LOGID_MMS_STATS	Information
43776	LOG_ID_EVENT_NAC_QUARANTINE	Notice
43777	LOG_ID_EVENT_NAC_ANOMALY_QUARANTINE	Notice
43800	LOG_ID_EVENT_ELBC_BLADE_JOIN	Critical
43801	LOG_ID_EVENT_ELBC_BLADE_LEAVE	Critical
43802	LOG_ID_EVENT_ELBC_MASTER_BLADE_FOUND	Critical
43803	LOG_ID_EVENT_ELBC_MASTER_BLADE_LOST	Critical
43804	LOG_ID_EVENT_ELBC_MASTER_BLADE_CHANGE	Critical
43805	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_FOUND	Critical
43806	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_LOST	Critical
43807	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_CHANGE	Critical
43808	LOG_ID_EVENT_ELBC_CHASSIS_ACTIVE	Critical
43809	LOG_ID_EVENT_ELBC_CHASSIS_INACTIVE	Critical
44544	LOGID_EVENT_CONFIG_PATH	Unknown
44545	LOGID_EVENT_CONFIG_OBJ	Unknown

Message ID	Message	Severity
44546	LOGID_EVENT_CONFIG_ATTR	Unknown
44547	LOGID_EVENT_CONFIG_OBJATTR	Unknown
44548	LOGID_EVENT_CONFIG_EXEC	Information
45000	LOG_ID_VSD_SSL_RCV_HS	Debug
45001	LOG_ID_VSD_SSL_RCV_WRG_HS	Error
45002	LOG_ID_VSD_SSL_SENT_HS	Debug
45003	LOG_ID_VSD_SSL_WRG_HS_LEN	Error
45004	LOG_ID_VSD_SSL_RCV_CCS	Debug
45005	LOG_ID_VSD_SSL_RSA_DH_FAIL	Error
45006	LOG_ID_VSD_SSL_SENT_CCS	Debug
45007	LOG_ID_VSD_SSL_BAD_HASH	Error
45009	LOG_ID_VSD_SSL_DECRY_FAIL	Error
45010	LOG_ID_VSD_SSL_SESSION_CLOSED	Debug
45011	LOG_ID_VSD_SSL_LESS_MINOR	Error
45012	LOG_ID_VSD_SSL_REACH_MAX_CON	Warning
45013	LOG_ID_VSD_SSL_NOT_SUPPORT_CS	Error
45016	LOG_ID_VSD_SSL_HS_FIN	Debug
45017	LOG_ID_VSD_SSL_HS_TOO_LONG	Error
45018	LOG_ID_VSD_SSL_MORE_MINOR	Debug
45019	LOG_ID_VSD_SSL_SENT_ALERT_ERR	Error
45020	LOG_ID_VSD_SSL_SESSION_EXPIRE	Debug
45021	LOG_ID_VSD_SSL_SENT_ALERT	Debug
45022	LOG_ID_VSD_SSL_RCV_CH	Debug
45023	LOG_ID_VSD_SSL_RCV_SH	Debug

Message ID	Message	Severity
45024	LOG_ID_VSD_SSL_SENT_SH	Debug
45025	LOG_ID_VSD_SSL_RCV_ALERT	Error
45027	LOG_ID_VSD_SSL_INVALID_CONT_TYPE	Error
45029	LOG_ID_VSD_SSL_BAD_CCS_LEN	Error
45031	LOG_ID_VSD_SSL_BAD_DH	Error
45032	LOG_ID_VSD_SSL_PUB_KEY_TOO_BIG	Error
45033	LOG_ID_VSD_SSL_NOT_SUPPORT_CM	Error
45034	LOG_ID_VSD_SSL_SERVER_KEY_HASH_ALGORITHM_ MISMATCH	Error
45035	LOG_ID_VSD_SSL_SERVER_KEY_SIGNATURE_ ALGORITHM_MISMATCH	Error
45161	LOG_ID_EVENT_DSSCC_EXEC	Information
46000	LOG_ID_VIP_REAL_SVR_ENA	Notice
46001	LOG_ID_VIP_REAL_SVR_DISA	Alert
46002	LOG_ID_VIP_REAL_SVR_UP	Notice
46003	LOG_ID_VIP_REAL_SVR_DOWN	Alert
46004	LOG_ID_VIP_REAL_SVR_ENT_HOLDDOWN	Notice
46005	LOG_ID_VIP_REAL_SVR_FAIL_HOLDDOWN	Alert
46006	LOG_ID_VIP_REAL_SVR_FAIL	Debug
46400	LOG_ID_EVENT_EXT_SYS	Unknown
46401	LOG_ID_EVENT_EXT_LOCAL	Unknown
46402	LOG_ID_EVENT_EXT_REMOTE	Unknown
47201	LOG_ID_AMC_ENTER_BYPASS	Emergency
47202	LOG_ID_AMC_EXIT_BYPASS	Emergency
47203	LOG_ID_ENTER_BYPASS	Emergency
47204	LOG_ID_EXIT_BYPASS	Emergency

USER

Log Field Name	Description	Data Type	Length
acct_stat	Accounting state (RADIUS)	string	14
action	Action	string	32
adgroup	AD Group Name	string	128
authproto	The protocol that initiated the authentication	string	64
carrier_ep	The FortiOS Carrier end-point identification	string	64
category	Category	uint32	10
count	Number of Packets	uint32	10
date	Date	string	10
devid	Device ID	string	16
dstip	Destination IP	ip	39
duration	Duration	uint32	10
expiry	FortiGuard override expiry timestamp	string	64
group	User name group	string	64
initiator	Original login user name for Fortiguard override	string	64
level	Log Level	string	11
logdesc	Log Description	string	
logid	Log ID	string	10
msg	Message	string	
oldwprof	Old Web Filter Profile	string	64
policyid	Policy ID	uint32	10
poolname	IP Pool Name	string	36
portbegin	Port Begin	uint16	5
portend	Port End	uint16	5

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
reason	Reason	string	256
rsso_key	RADIUS SSO attribute value	string	64
scope	FortiGuard Override Scope	string	16
server	AD server FQDN or IP	string	64
srcip	Source IP	ip	39
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
ui	User Interface	string	64
user	User Name	string	256
vd	Virtual Domain Name	string	32

USER Log Messages

The following table describes the log message IDs and messages of the USER log.

Message ID	Message	Severity
38010	LOG_ID_FIPS_ENCRY_FAIL	Alert
38011	LOG_ID_FIPS_DECRY_FAIL	Alert
38012	LOG_ID_ENTROPY_TOKEN	Notice
38031	LOG_ID_FSSO_LOGON	Notice
38032	LOG_ID_FSSO_LOGOFF	Notice
38033	LOG_ID_FSSO_SVR_STATUS	Notice
38656	LOGID_EVENT_RAD_RPT_PROTO_ERROR	Notice
38657	LOGID_EVENT_RAD_RPT_PROF_NOT_FOUND	Notice

Message ID	Message	Severity
38658	LOGID_EVENT_RAD_RPT_CTX_NOT_FOUND	Notice
38659	LOGID_EVENT_RAD_RPT_ACCT_STOP_MISSED	Notice
38660	LOGID_EVENT_RAD_RPT_ACCT_EVENT	Notice
38661	LOGID_EVENT_RAD_RPT_OTHER	Notice
38662	LOGID_EVENT_RAD_STAT_PROTO_ERROR	Notice
38663	LOGID_EVENT_RAD_STAT_PROF_NOT_FOUND	Notice
38665	LOGID_EVENT_RAD_STAT_ACCT_STOP_MISSED	Notice
38666	LOGID_EVENT_RAD_STAT_ACCT_EVENT	Notice
38667	LOGID_EVENT_RAD_STAT_OTHER	Notice
38668	LOGID_EVENT_RAD_STAT_EP_BLK	Notice
43008	LOG_ID_EVENT_AUTH_SUCCESS	Unknown
43009	LOG_ID_EVENT_AUTH_FAILED	Unknown
43010	LOG_ID_EVENT_AUTH_LOCKOUT	Unknown
43011	LOG_ID_EVENT_AUTH_TIME_OUT	Notice
43012	LOG_ID_EVENT_AUTH_FSAE_AUTH_SUCCESS	Notice
43013	LOG_ID_EVENT_AUTH_FSAE_AUTH_FAIL	Notice
43014	LOG_ID_EVENT_AUTH_FSAE_LOGON	Notice
43015	LOG_ID_EVENT_AUTH_FSAE_LOGOFF	Notice
43016	LOG_ID_EVENT_AUTH_NTLM_AUTH_SUCCESS	Notice
43017	LOG_ID_EVENT_AUTH_NTLM_AUTH_FAIL	Notice
43018	LOG_ID_EVENT_AUTH_FGOVRD_FAIL	Warning
43020	LOG_ID_EVENT_AUTH_FGOVRD_SUCCESS	Notice
43025	LOG_ID_EVENT_AUTH_PROXY_SUCCESS	Notice
43026	LOG_ID_EVENT_AUTH_PROXY_FAILED	Notice

Message ID	Message	Severity
43027	LOG_ID_EVENT_AUTH_PROXY_TIME_OUT	Notice
43028	LOG_ID_EVENT_AUTH_PROXY_AUTHORIZATION_FAILED	Notice
43029	LOG_ID_EVENT_AUTH_WARNING_SUCCESS	Notice
43030	LOG_ID_EVENT_AUTH_WARNING_TBL_FULL	Warning
43040	LOG_ID_EVENT_AUTH_LOGOUT	Notice
43041	LOG_ID_EVENT_AUTH_DISCLAIMER_ACCEPT	Unknown
43042	LOG_ID_EVENT_AUTH_DISCLAIMER_DECLINE	Unknown
43043	LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_SUCCESS	Unknown
43044	LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_FAIL	Unknown

VPN

Log Field Name	Description	Data Type	Length
action	Action	string	32
assignip	Assigned IP Address	ip	39
cert-type	Certification type	string	6
cookies	Cookie	string	64
date	Date	string	10
devid	Device ID	string	16
dir	Direction	string	8
dst_host	Destination Hostname	string	64
duration	Duration	uint32	10
error_num	Error Number	string	53
espauth	ESP Authentication	string	17
esptransform	ESP Transform	string	11

Log Field Name	Description	Data Type	Length
exch	In SPI	string	14
group	User Name Group	string	64
init		string	6
in_spi		string	16
level	Log Level	string	11
locip	Local IP	ip	39
locport	Local Port	uint16	5
logdesc	Log Description	string	
logid	Log ID	string	10
method	Method	string	64
mode	Mode	string	12
msg	Message	string	
name	Name	string	128
nextstat	Time interval in seconds for the next statistics	uint32	10
outintf	Out interface	string	32
out_spi	Out SPI	string	16
peer_notif	Peer Notification	string	25
phase2_name	Phase 2 Name	string	128
rcvdbyte	Received Bytes	uint64	20
reason	Reason	string	256
remip	Remote IP	ip	39
remport	Remote Port	uint16	5
result	Result	string	31
role	Role	string	9

Log Field Name	Description	Data Type	Length
sentbyte	Bytes Sent	uint64	20
seq	Sequence	string	16
spi		string	16
stage		uint8	3
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
tunnelid	Tunnel ID	uint32	10
tunnelip	Tunnel IP	ip	39
tunneltype	Tunnel Type	string	64
type	Log Type	string	16
ui	User Interface	string	64
user	User Name	string	256
vd	Virtual Domain Name	string	32
vpntunnel	IPsec Vpn Tunnel Name	string	128
xauthgroup	XAuth Group Name	string	128
xauthuser	XAuth User Name	string	128

VPN Log Messages

The following table describes the log message IDs and messages of the VPN log.

Message ID	Message	Severity
37120	MESGID_NEG_GENERIC_P1_NOTIF	Unknown
37121	MESGID_NEG_GENERIC_P1_ERROR	Unknown
37122	MESGID_NEG_GENERIC_P2_NOTIF	Unknown
37123	MESGID_NEG_GENERIC_P2_ERROR	Unknown

Message ID	Message	Severity
37124	MESGID_NEG_I_P1_ERROR	Error
37125	MESGID_NEG_I_P2_ERROR	Error
37126	MESGID_NEG_NO_STATE_ERROR	Error
37127	MESGID_NEG_PROGRESS_P1_NOTIF	Unknown
37128	MESGID_NEG_PROGRESS_P1_ERROR	Unknown
37129	MESGID_NEG_PROGRESS_P2_NOTIF	Unknown
37130	MESGID_NEG_PROGRESS_P2_ERROR	Unknown
37131	MESGID_ESP_ERROR	Unknown
37132	MESGID_ESP_CRITICAL	Unknown
37133	MESGID_INSTALL_SA	Notice
37134	MESGID_DELETE_P1_SA	Notice
37135	MESGID_DELETE_P2_SA	Notice
37136	MESGID_DPD_FAILURE	Error
37137	MESGID_CONN_FAILURE	Error
37138	MESGID_CONN_UPDOWN	Notice
37139	MESGID_P2_UPDOWN	Notice
37141	MESGID_CONN_STATS	Notice
37184	MESGID_NEG_GENERIC_P1_NOTIF_IKEV2	Unknown
37185	MESGID_NEG_GENERIC_P1_ERROR_IKEV2	Unknown
37186	MESGID_NEG_GENERIC_P2_NOTIF_IKEV2	Unknown
37187	MESGID_NEG_GENERIC_P2_ERROR_IKEV2	Unknown
37188	MESGID_NEG_I_P1_ERROR_IKEV2	Error
37189	MESGID_NEG_I_P2_ERROR_IKEV2	Error
37190	MESGID_NEG_NO_STATE_ERROR_IKEV2	Error

Message ID	Message	Severity
37191	MESGID_NEG_PROGRESS_P1_NOTIF_IKEV2	Unknown
37192	MESGID_NEG_PROGRESS_P1_ERROR_IKEV2	Unknown
37193	MESGID_NEG_PROGRESS_P2_NOTIF_IKEV2	Unknown
37194	MESGID_NEG_PROGRESS_P2_ERROR_IKEV2	Unknown
37195	MESGID_ESP_ERROR_IKEV2	Unknown
37196	MESGID_ESP_CRITICAL_IKEV2	Unknown
37197	MESGID_INSTALL_SA_IKEV2	Notice
37198	MESGID_DELETE_P1_SA_IKEV2	Notice
37199	MESGID_DELETE_P2_SA_IKEV2	Notice
37200	MESGID_DPD_FAILURE_IKEV2	Error
37201	MESGID_CONN_FAILURE_IKEV2	Error
37202	MESGID_CONN_UPDOWN_IKEV2	Notice
37203	MESGID_P2_UPDOWN_IKEV2	Notice
37204	MESGID_CONN_STATS_IKEV2	Notice
39424	LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_UP	Unknown
39425	LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_DOWN	Unknown
39426	LOG_ID_EVENT_SSL_VPN_USER_SSL_LOGIN_FAIL	Unknown
39936	LOG_ID_EVENT_SSL_VPN_SESSION_WEB_TUNNEL_ STATS	Unknown
39937	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_DENY	Unknown
39938	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_PASS	Unknown
39939	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_TIMEOUT	Unknown
39940	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_CLOSE	Unknown
39941	LOG_ID_EVENT_SSL_VPN_SESSION_SYS_BUSY	Unknown
39942	LOG_ID_EVENT_SSL_VPN_SESSION_CERT_OK	Unknown

Message ID	Message	Severity
39943	LOG_ID_EVENT_SSL_VPN_SESSION_NEW_CON	Unknown
39944	LOG_ID_EVENT_SSL_VPN_SESSION_ALERT	Unknown
39945	LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_FAIL	Unknown
39946	LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_ERR	Unknown
39947	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UP	Unknown
39948	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_DOWN	Unknown
39949	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_STATS	Unknown
39950	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ UNKNOWNTAG	Unknown
39951	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ERROR	Unknown
39952	LOG_ID_EVENT_SSL_VPN_SESSION_ENTER_CONSERVE_ MODE	Unknown
39953	LOG_ID_EVENT_SSL_VPN_SESSION_LEAVE_CONSERVE_ MODE	Unknown
40001	LOG_ID_PPTP_TUNNEL_UP	Unknown
40002	LOG_ID_PPTP_TUNNEL_DOWN	Unknown
40003	LOG_ID_PPTP_TUNNEL_STAT	Unknown
40014	LOG_ID_PPTP_REACH_MAX_CON	Warning
40017	LOG_ID_L2TPD_CLIENT_CON_FAIL	Warning
40019	LOG_ID_L2TPD_CLIENT_DISCON	Information
40021	LOG_ID_PPTP_NOT_CONIG	Debug
40022	LOG_ID_PPTP_NO_IP_AVAIL	Warning
40024	LOG_ID_PPTP_OUT_MEM	Warning
40034	LOG_ID_PPTP_START	Notice
40035	LOG_ID_PPTP_START_FAIL	Error
40036	LOG_ID_PPTP_EXIT	Notice

Message ID	Message	Severity
40037	LOG_ID_PPTPD_SVR_DISCON	Information
40038	LOG_ID_PPTPD_CLIENT_CON	Information
40039	LOG_ID_PPTPD_CLIENT_DISCON	Information
40101	LOG_ID_L2TP_TUNNEL_UP	Unknown
40102	LOG_ID_L2TP_TUNNEL_DOWN	Unknown
40103	LOG_ID_L2TP_TUNNEL_STAT	Unknown
40114	LOG_ID_L2TPD_START	Notice
40115	LOG_ID_L2TPD_EXIT	Notice
40118	LOG_ID_L2TPD_CLIENT_CON	Information
41984	LOG_ID_EVENT_VPN_CERT_LOAD	Information
41985	LOG_ID_EVENT_VPN_CERT_REMOVAL	Information
41986	LOG_ID_EVENT_VPN_CERT_REGEN	Information
41987	LOG_ID_EVENT_VPN_CERT_UPDATE	Information
41988	LOG_ID_EVENT_SSL_VPN_SETTING_UPDATE	Information
41989	LOG_ID_EVENT_VPN_CERT_ERR	Information
41990	LOG_ID_EVENT_VPN_CERT_UPDATE_FAILED	Information
41991	LOG_ID_EVENT_VPN_CERT_EXPORT	Information

WAD

Log Field Name	Description	Data Type	Length
action	Action	string	32
addr_type	Address Type	string	4
alert	Alert	string	256
app-type	Address Type	string	64

Log Field Name	Description	Data Type	Length
authgrp	Authorization Group	string	36
date	Date	string	10
desc	Description	string	128
devid	Device ID	string	16
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
fqdn	Fully Qualified Domain Name	string	256
fwserver_name		string	32
handshake	Handshake	string	32
host	Host Name	string	256
ip		ip	39
level	Log Level	string	11
local		ip	39
logdesc	Log Description	string	
logid	Log ID	string	10
msg	Log Message	string	
peer		string	36
policyid	Policy ID	uint32	10
port	Port Number	uint16	5
reason	Reason	string	256
remote		ip	39
serial	Serial Number	uint32	10
session_id	Session ID	uint32	10
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
vd	Virtual Domain Name	string	32

WAD Log Messages

The following table describes the log message IDs and messages of the WAD log.

Message ID	Message	Severity
40960	LOGID_EVENT_WAD_WEBPROXY_FWD_SRV_ERROR	Notice
48000	LOG_ID_WAD_SSL_RCV_HS	Debug
48001	LOG_ID_WAD_SSL_RCV_WRG_HS	Error
48002	LOG_ID_WAD_SSL_SENT_HS	Debug
48003	LOG_ID_WAD_SSL_WRG_HS_LEN	Error
48004	LOG_ID_WAD_SSL_RCV_CCS	Debug
48005	LOG_ID_WAD_SSL_RSA_DH_FAIL	Error
48006	LOG_ID_WAD_SSL_SENT_CCS	Debug
48007	LOG_ID_WAD_SSL_BAD_HASH	Error
48009	LOG_ID_WAD_SSL_DECRY_FAIL	Error
48011	LOG_ID_WAD_SSL_LESS_MINOR	Error
48013	LOG_ID_WAD_SSL_NOT_SUPPORT_CS	Error
48016	LOG_ID_WAD_SSL_HS_FIN	Debug
48017	LOG_ID_WAD_SSL_HS_TOO_LONG	Error
48019	LOG_ID_WAD_SSL_SENT_ALERT	Debug
48023	LOG_ID_WAD_SSL_RCV_ALERT	Debug

Message ID	Message	Severity
48027	LOG_ID_WAD_SSL_INVALID_CONT_TYPE	Error
48029	LOG_ID_WAD_SSL_BAD_CCS_LEN	Error
48030	LOG_ID_WAD_SSL_CLIENT_CERT_REQUEST	Error
48031	LOG_ID_WAD_SSL_BAD_DH	Error
48032	LOG_ID_WAD_SSL_PUB_KEY_TOO_BIG	Error
48038	LOG_ID_WAD_SSL_RCV_FATAL_ALERT	Error
48039	LOG_ID_WAD_SSL_SENT_FATAL_ALERT	Error
48100	LOG_ID_WAD_AUTH_FAIL_CERT	Error
48101	LOG_ID_WAD_AUTH_FAIL_PSK	Error
48102	LOG_ID_WAD_AUTH_FAIL_OTH	Error
48300	LOG_ID_WRG_SVR_FGT_CONF	Critical
48301	LOG_ID_UNEXP_APP_TYPE	Critical

WIRELESS

Log Field Name	Description	Data Type	Length
action	Action	string	32
age	time in seconds - time passed since last seen	uint32	10
ap		string	36
apscan	The name of the AP, which scanned and detected the rogue AP	string	36
apstatus		uint8	3
aptype	AP Type	uint8	3
bandwidth	Bandwidth	string	42
bssid	Service Set ID	string	17
cfgtxpower	Config TX power	uint32	10

Log Field Name	Description	Data Type	Length
channel	Channel	uint8	3
configcountry	Config Country	string	4
date	Date	string	10
detectionmethod	Detection Method	string	21
devid	Device ID	string	16
ds	direction with distribution system	string	8
duration	Duration of the last threatening packed captured from TA	uint32	10
eapolcnt	EAPOL packet count	uint32	10
eapoltype	EAPOL packet type	string	16
encrypt	whether the packet is encrypted or not	uint8	3
encryption	Encryption Method	string	12
frametype	Frame Type	string	32
group	User Group Name	string	64
invalidmac	the MAC address with invalid OUI	string	17
ip		ip	39
level	Log Level	string	11
live	time in seconds	uint32	10
logdesc	Log Description	string	
logid	Log ID	string	10
mac	Mac Address	string	17
manuf	Manufacturer name	string	20
meshmode	Mesh mode	string	19
mgmtcnt	The number of unauthorized client flooding man-agemet frames	uint32	10

Log Field Name	Description	Data Type	Length
msg	Log Message	string	
noise		int8	4
onwire	A flag to indicate if the AP is onwire or not	string	3
opercountry	Operating Country	string	4
opertxpower	Operating TX power	uint32	10
profile	Profile Name	string	64
radioband	Radio Band	string	64
radioid	Radio ID	uint8	3
radioidclosest	Radio ID on the AP closest the rogue AP	uint8	3
radioiddetected	Radio ID on the AP which detected the rogue AP	uint8	3
rate		uint8	4
reason	Reason	string	256
rssi	Received signal strength indicator	uint8	3
security	Security	string	40
securitymode	Security Mode	string	40
seq	Sequence	string	16
signal	Signal	int8	4
sn	Serial Number	string	64
snclosest	SN of the AP closest to the rogue AP	string	36
sndetected	SN of the AP which detected the rogue AP	string	36
snmeshparent	SN of the mesh parent	string	36
srcip	Source IP	ip	39
ssid	Base Service Set ID	string	33
stacount	Number of stations/clients	uint32	10

Log Field Name	Description	Data Type	Length
stamac	Station/Client MAC address	string	17
subtype	Log Subtype	string	20
tamac	the MAC address of Transmitter, if none, then Receiver	string	17
threattype	WIDS threat type	string	64
time	Time	string	8
type	Log Type	string	16
user	User Name	string	256
vap		string	36
vd	Virtual Domain Name	string	32
weakwepiv	Weak Wep Initiation Vector	string	8

WIRELESS Log Messages

The following table describes the log message IDs and messages of the WIRELESS log.

Message ID	Message	Severity
43521	LOG_ID_EVENT_WIRELESS_ROGUE	Unknown
43525	LOG_ID_EVENT_WIRELESS_ONWIRE	Unknown
43528	LOG_ID_EVENT_WIRELESS_WTPR_ERROR	Unknown
43530	LOG_ID_EVENT_WIRELESS_WIDS_WL_BRIDGE	Notice
43531	LOG_ID_EVENT_WIRELESS_WIDS_BR_DEAUTH	Notice
43532	LOG_ID_EVENT_WIRELESS_WIDS_NL_PBRESP	Notice
43533	LOG_ID_EVENT_WIRELESS_WIDS_MAC_OUI	Notice
43534	LOG_ID_EVENT_WIRELESS_WIDS_LONG_DUR	Notice
43535	LOG_ID_EVENT_WIRELESS_WIDS_WEP_IV	Notice
43542	LOG_ID_EVENT_WIRELESS_WIDS_EAPOL_FLOOD	Notice
43544	LOG_ID_EVENT_WIRELESS_WIDS_MGMT_FLOOD	Notice

Message ID	Message	Severity
43546	LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH	Notice
43548	LOG_ID_EVENT_WIRELESS_WIDS_ASLEAP	Notice
43550	LOG_ID_EVENT_WIRELESS_STA_LOCATE	Notice
43551	LOG_ID_EVENT_WIRELESS_WTP_JOIN	Unknown
43552	LOG_ID_EVENT_WIRELESS_WTP_LEAVE	Unknown
43553	LOG_ID_EVENT_WIRELESS_WTP_FAIL	Notice
43554	LOG_ID_EVENT_WIRELESS_WTP_UPDATE	Unknown
43555	LOG_ID_EVENT_WIRELESS_WTP_RESET	Unknown
43556	LOG_ID_EVENT_WIRELESS_WTP_KICK	Unknown
43557	LOG_ID_EVENT_WIRELESS_WTP_ADD_FAILURE	Notice
43558	LOG_ID_EVENT_WIRELESS_WTP_CFG_ERR	Notice
43559	LOG_ID_EVENT_WIRELESS_WTP_SN_MISMATCH	Warning
43560	LOG_ID_EVENT_WIRELESS_SYS_AC_RESTARTED	Notice
43561	LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_UP	Notice
43562	LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_DOWN	Notice
43563	LOG_ID_EVENT_WIRELESS_ROGUE_DETECT	Unknown
43564	LOG_ID_EVENT_WIRELESS_ROGUE_OFFAIR	Unknown
43565	LOG_ID_EVENT_WIRELESS_ROGUE_ONAIR	Unknown
43566	LOG_ID_EVENT_WIRELESS_ROGUE_OFFWIRE	Unknown
43567	LOG_ID_EVENT_WIRELESS_FAKEAP_DETECT	Unknown
43568	LOG_ID_EVENT_WIRELESS_FAKEAP_ONAIR	Unknown
43569	LOG_ID_EVENT_WIRELESS_ROGUE_SUPPRESSED	Unknown
43570	LOG_ID_EVENT_WIRELESS_ROGUE_UNSUPPRESSED	Unknown
43571	LOG_ID_EVENT_WIRELESS_ROGUE_DETECT_CHG	Unknown

Message ID	Message	Severity
43572	LOG_ID_EVENT_WIRELESS_STA_ASSO	Notice
43573	LOG_ID_EVENT_WIRELESS_STA_AUTH	Notice
43574	LOG_ID_EVENT_WIRELESS_STA_DASS	Notice
43575	LOG_ID_EVENT_WIRELESS_STA_DAUT	Notice
43576	LOG_ID_EVENT_WIRELESS_STA_IDLE	Notice
43577	LOG_ID_EVENT_WIRELESS_STA_DENY	Notice
43578	LOG_ID_EVENT_WIRELESS_STA_KICK	Notice
43579	LOG_ID_EVENT_WIRELESS_STA_IP	Notice
43580	LOG_ID_EVENT_WIRELESS_STA_LEAVE_WTP	Notice
43581	LOG_ID_EVENT_WIRELESS_STA_WTP_DISCONN	Notice
43582	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_UNCLASSIFIED	Notice
43583	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ACCEPTED	Notice
43584	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ROGUE	Notice
43585	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_SUPPRESSED	Notice
43586	LOG_ID_EVENT_WIRELESS_WTPR_DARRP_CHAN	Unknown
43587	LOG_ID_EVENT_WIRELESS_WTPR_DARRP_START	Unknown
43588	LOG_ID_EVENT_WIRELESS_WTPR_OPER_CHAN	Unknown
43589	LOG_ID_EVENT_WIRELESS_WTPR_RADAR	Unknown
43590	LOG_ID_EVENT_WIRELESS_WTPR_NOL	Unknown
43591	LOG_ID_EVENT_WIRELESS_WTPR_COUNTRY_CFG_ SUCCESS	Unknown
43592	LOG_ID_EVENT_WIRELESS_WTPR_OPER_COUNTRY	Unknown
43593	LOG_ID_EVENT_WIRELESS_WTPR_CFG_TXPOWER	Unknown
43594	LOG_ID_EVENT_WIRELESS_WTPR_OPER_TXPOWER	Unknown
43595	LOG_ID_EVENT_WIRELESS_CLB_DENY	Notice

Message ID	Message	Severity
43596	LOG_ID_EVENT_WIRELESS_CLB_RETRY	Notice
43597	LOG_ID_EVENT_WIRELESS_WTP_ADD	Notice
43598	LOG_ID_EVENT_WIRELESS_WTP_ADD_XSS	Unknown
43599	LOG_ID_EVENT_WIRELESS_WTP_DEL	Notice
43600	LOG_ID_EVENT_WIRELESS_WTPR_DARRP_STOP	Unknown
43601	LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON	Notice
43602	LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_SUCCESS	Notice
43603	LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_FAILURE	Notice
43604	LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_REQUEST	Notice
43605	LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_SUCCESS	Notice
43606	LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_FAILURE	Notice
43607	LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_ CHECK	Notice
43608	LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_ DECLINE	Notice
43609	LOG_ID_EVENT_WIRELESS_SYS_AC_DARRP_START	Notice
43610	LOG_ID_EVENT_WIRELESS_SYS_AC_DARRP_STOP	Notice
43611	LOG_ID_EVENT_WIRELESS_SYS_AC_UP	Notice
43612	LOG_ID_EVENT_WIRELESS_SYS_AC_CFG_LOADED	Notice
43613	LOG_ID_EVENT_WIRELESS_WTP_ERR	Notice
43614	LOG_ID_EVENT_WIRELESS_DHCP_STAVATION	Notice

GTP

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128

Log Field Name	Description	Data Type	Length
c-bytes	Control Plane Data Bytes	uint64	20
c-ggsn	Control Plane GGSN IP Address	ip	39
c-ggsn-teid	Control Plane GGSN Tunnel Endpoint Identifier	uint32	10
c-gsn	Control Plane GSN	ip	39
c-pkts	Control Plane Packets	uint64	20
c-sgsn	Control Plane SGSN IP Address	ip	39
c-sgsn-teid	Control Plane SGSN Tunnel Endpoint Identifier	uint32	10
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
cpdladdr	Control Plane Downlink IP Address	ip	39
cpdlisraddr	Control Plane ISR Downlink IP Address	ip	39
cpdlisrteid	control plane ISR downlink tunnel endpoint identifier	uint32	10
cpdlteid	control plane downlink tunnel endpoint identifier	uint32	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
cpuladdr	control plane uplink IP address	ip	39
cpulteid	control plane uplink teid	uint32	10
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
duration	tunnel duration	uint32	10
end-usr-address	End user IP Address	ip	39
from	From	string	128
headerteid	Tunnel Endpoint ID Header	uint32	10

Log Field Name	Description	Data Type	Length
ietype	Malformed GTP IE number	uint8	3
imei-sv		string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
nsapi	Netscape Server Application Programming Interface	uint8	3
profile	Profile Name	string	64
rai		string	32
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	string	512
tunnel-idx	tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
u-bytes	User Plane Data Bytes	uint64	20

Log Field Name	Description	Data Type	Length
u-ggsn	user plane ggsn IP address	ip	39
u-ggsn-teid	user plane ggsn teid	uint32	10
u-gsn	User Plane GSN	ip	39
u-pkts	User Plane Packets	uint64	20
u-sgsn	user plane sgsn IP address	ip	39
u-sgsn-teid	user plane sgsn tunnel endpoint identifier	uint32	10
uli		string	32
user_data	user traffic content inside gtp-u tunnel	string	256
vd	Virtual Domain Name	string	32
version	Version	string	64

GTP Log Messages

The following table describes the log message IDs and messages of the GTP log.

Message ID	Message	Severity
41216	LOGID_GTP_FORWARD	Information
41217	LOGID_GTP_DENY	Information
41218	LOGID_GTP_RATE_LIMIT	Information
41219	LOGID_GTP_STATE_INVALID	Information
41220	LOGID_GTP_TUNNEL_LIMIT	Information
41221	LOGID_GTP_TRAFFIC_COUNT	Information
41222	LOGID_GTP_USER_DATA	Information
41223	LOGID_GTPV2_FORWARD	Information
41224	LOGID_GTPV2_DENY	Information
41225	LOGID_GTPV2_RATE_LIMIT	Information
41226	LOGID_GTPV2_STATE_INVALID	Information

Message ID	Message	Severity
41227	LOGID_GTPV2_TUNNEL_LIMIT	Information
41228	LOGID_GTPV2_TRAFFIC_COUNT	Information
41229	LOGID_GTPU_FORWARD	Information
41230	LOGID_GTPU_DENY	Information

IPS

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	66
attack	Attack Name	string	256
attackcontext	the trigger patterns and the packetdata with base64 encoding	string	2040
attackcontextid	attack context id / total	string	10
attackid	Attack ID	uint32	10
count	Repeat count for an attack event	uint32	10
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of packets	string	8
dstintf	Destination Interface	string	64
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
eventtype	IPS Event Type	string	32
group	User group name	string	64
hostname	Host Name	string	256
icmpcode	Destination Port of the ICMP message	string	6
icmpid	Source port of the ICMP message	string	8
icmptype	The type of ICMP message	string	6
incidentserialno	Incident serial number	uint32	10
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message for the attack	string	518
policyid	Policy ID	uint32	10
profile	Profile name for IPS	string	64
profile	Profile name for IPS	string	64
profiletype	Profile Type	string	64
proto	Protocol number	uint8	3
ref	URL of the FortiGuard IPS database entry for the attack.	string	
service	Service name	string	36
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
srccountry		string	64
srcintf	Source Interface	string	64
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
type	Log type	string	16
url	URL	string	512
user	User name	string	256
vd	Virtual domain name	string	32

IPS Log Messages

The following table describes the log message IDs and messages of the IPS log.

Message ID	Message	Severity
16384	LOGID_ATTCK_SIGNATURE_TCP_UDP	Alert
16385	LOGID_ATTCK_SIGNATURE_ICMP	Alert
16386	LOGID_ATTCK_SIGNATURE_OTHERS	Alert

Traffic

Log Field Name	Description	Data Type	Length
action	status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	16
ap		string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64

Log Field Name	Description	Data Type	Length
apprisk	Application Risk Level	string	16
apsn		string	36
centralnatid	Central NAT ID	uint32	10
channel	Channel	uint32	10
collectedemail	Email address from Email Collection Captive Portal	string	66
countapp	Number of App Ctrl logs associated with the session	uint32	10
countav	Number of AV logs associated with the session	uint32	10
countdlp	Number of the DLP logs associated with the session	uint32	10
countemail	Number of the email logs associated with the session	uint32	10
countips	Number of the IPS logs associated with the session	uint32	10
countwaf		uint32	10
countweb	Number of the Web Filter logs associated with the session	uint32	10
craction	Action performed by Client Reputation	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation score	uint32	10
custom	Custom field	custom	
date	Date	string	10
devid	Device serial number	string	16
devtype	Device type	string	32
dstcountry	Country name for the destination IP	string	64
dstintf	Destination Interface	string	32
dstip	Destination IP Address	ip	39
dstname	The destination name.	string	66

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dstssid	Destination SSID	string	33
dstuuid	UUID of the Destination IP address	string	37
duration	Duration of the session	uint32	10
group	User group name	string	64
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
osversion	OS version of the device	string	66
policyid	Firewall Policy ID	uint32	10
policymode		string	8
policytype		string	24
poluuid	UUID of the Firewall Policy	string	37
proto	protocol number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of service	string	63

Log Field Name	Description	Data Type	Length
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid		uint32	10
srccountry	Country name for Source IP	string	64
srcintf	Source interface name	string	32
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source port number	uint16	5
srcssid	Source SSID	string	33
srcuuid	UUID of the Source IP Address	string	37
sslexempt		string	11
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Port	uint16	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vwpvlanid		uint32	10
wanin	WAN incoming traffic in bytes	uint32	10
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint32	10

Traffic Log Messages

The following table describes the log message IDs and messages of the Traffic log.

Message ID	Message	Severity
2	LOG_ID_TRAFFIC_ALLOW	Notice
3	LOG_ID_TRAFFIC_DENY	Warning
4	LOG_ID_TRAFFIC_OTHER_START	Notice
5	LOG_ID_TRAFFIC_OTHER_ICMP_ALLOW	Notice
6	LOG_ID_TRAFFIC_OTHER_ICMP_DENY	Warning
7	LOG_ID_TRAFFIC_OTHER_INVALID	Warning
8	LOG_ID_TRAFFIC_WANOPT	Notice
9	LOG_ID_TRAFFIC_WEBCACHE	Notice

Message ID	Message	Severity
10	LOG_ID_TRAFFIC_EXPLICIT_PROXY	Notice
11	LOG_ID_TRAFFIC_FAIL_CONN	Warning
12	LOG_ID_TRAFFIC_MULTICAST	Notice
13	LOG_ID_TRAFFIC_END_FORWARD	Notice
14	LOG_ID_TRAFFIC_END_LOCAL	Notice
15	LOG_ID_TRAFFIC_START_FORWARD	Notice
16	LOG_ID_TRAFFIC_START_LOCAL	Notice
17	LOG_ID_TRAFFIC_SNIFFER	Notice
19	LOG_ID_TRAFFIC_BROADCAST	Notice

VoIP

Log Field Name	Description	Data Type	Length
action	Action	string	15
call_id	Call ID	string	64
column		uint32	10
count	Count	uint32	10
date	Date	string	10
devid	Device ID	string	16
dir	Direction	string	8
dstip	Destination IP	ip	39
dst_int	Destination Interface	string	16
dst_port	Destination Port	uint16	5
duration	Duration	uint32	10
endpoint	Endpoint	string	128

Log Field Name	Description	Data Type	Length
epoch		uint32	10
eventtype	Event Type	string	32
event_id	Event ID	uint32	10
from	From	string	128
group	User Group Name	string	64
kind		string	10
level	Log Level	string	11
line		string	128
locip	Local IP	ip	39
locport	Local Port	uint16	5
logid	Log ID	string	10
malform_data	Malformed data	uint32	10
malform_desc	Malformed data Description	string	47
message_type	Message Type	string	16
phone		string	64
policy_id	Policy ID	uint32	10
profile	Profile Name	string	64
profile_group	Profile Group Name	string	64
profile_type	Profile Type	string	64
proto	Protocol	uint8	3
reason	Reason	string	128
remip	Remote IP	ip	39
remport	Remote Port	uint16	5
request_name	Request Name	string	64

Log Field Name	Description	Data Type	Length
session_id	Session ID	uint32	10
srcip	Source IP	ip	39
src_int	Source Interface	string	16
src_port	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to		string	512
type	Log Type	string	16
user	User	string	256
vd	Virtual Domain Name	string	32
voip_proto	VoIP Protocol	string	4

VoIP Log Messages

The following table describes the log message IDs and messages of the VoIP log.

Message ID	Message	Severity
44032	LOGID_EVENT_VOIP_SIP	Information
44033	LOGID_EVENT_VOIP_SIP_BLOCK	Notice
44034	LOGID_EVENT_VOIP_SIP_FUZZING	Information
44035	LOGID_EVENT_VOIP_SCCP_REGISTER	Information
44036	LOGID_EVENT_VOIP_SCCP_UNREGISTER	Information
44037	LOGID_EVENT_VOIP_SCCP_CALL_BLOCK	Information
44038	LOGID_EVENT_VOIP_SCCP_CALL_INFO	Information

WAF

Log Field Name	Description	Data Type	Length
action	status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
constraint	WAF http protocol restrictions	string	
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	
dstintf	Destination Interface	string	32
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtype	Event Type	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Http Method	string	
msg	Log Message	string	
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3

Log Field Name	Description	Data Type	Length
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcintf	Source Interface	string	32
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

WAF Log Messages

The following table describes the log message IDs and messages of the WAF log.

Message ID	Message	Severity
30248	LOGID_WAF_SIGNATURE_BLOCK	Warning
30249	LOGID_WAF_SIGNATURE_PASS	Warning
30250	LOGID_WAF_SIGNATURE_ERASE	Warning
30251	LOGID_WAF_CUSTOM_SIGNATURE_BLOCK	Warning
30252	LOGID_WAF_CUSTOM_SIGNATURE_PASS	Warning
30253	LOGID_WAF_METHOD_BLOCK	Warning
30255	LOGID_WAF_ADDRESS_LIST_BLOCK	Warning
30257	LOGID_WAF_CONSTRAINTS_BLOCK	Warning
30258	LOGID_WAF_CONSTRAINTS_PASS	Warning

Message ID	Message	Severity
30259	LOGID_WAF_URL_ACCESS_PERMIT	Warning
30260	LOGID_WAF_URL_ACCESS_BYPASS	Warning
30261	LOGID_WAF_URL_ACCESS_BLOCK	Warning

Web

Log Field Name	Description	Data Type	Length
action	Security action performed by WF	string	11
agent	User agent - eg. agent="Mozilla/5.0"	string	64
banword	Banned word	string	128
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
contenttype	Content Type from HTTP header	string	64
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	URL rating error message	string	256
eventtype	Web Filter event type	string	32
filtertype	The script filter type	string	10
from	MMS-only - From/To headers from the email	string	128

Log Field Name	Description	Data Type	Length
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
keyword	Keyword used for search	string	512
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address.	string	6
mode	Rating override mode	string	32
msg	Log message	string	512
ovrdid	URL rating override ID	uint32	10
ovrdtbl	Rating override table	string	128
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
quotaexceeded	Quota has been exceeded	string	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based).	uint64	20
rcvdbyte	Received Bytes	uint64	20
referralurl	Referral URL	string	512
reqtype	Request type	string	8
ruledata	Rule data	string	512
ruletype	Rule type	string	9

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcintf	Source Interface	string	32
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
to	MMS-only - From/To headers from the email	string	512
type	Log type	string	16
url	The URL address	string	512
urlfilteridx	URL filter ID	uint32	10
urlfilterlist	URL filter list	string	64
urltype	URL filter type	string	8
user	User name	string	256
vd	Virtual domain name	string	32

Web Log Messages

The following table describes the log message IDs and messages of the Web log.

Message ID	Message	Severity
12288	LOG_ID_WEB_CONTENT_BANWORD	Warning
12289	LOG_ID_WEB_CONTENT_MMS_BANWORD	Warning
12290	LOG_ID_WEB_CONTENT_EXEMPTWORD	Notice
12291	LOG_ID_WEB_CONTENT_MMS_EXEMPTWORD	Notice
12292	LOG_ID_WEB_CONTENT_KEYWORD	Notice

Message ID	Message	Severity
12293	LOG_ID_WEB_CONTENT_SEARCH	Notice
12305	LOG_ID_WEB_CONTENT_BANWORD_NOTIF	Notice
12544	LOG_ID_URL_FILTER_BLOCK	Warning
12545	LOG_ID_URL_FILTER_EXEMPT	Information
12546	LOG_ID_URL_FILTER_ALLOW	Information
12547	LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_BLK	Notice
12548	LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_BLK	Notice
12549	LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_PASS	Information
12550	LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_PASS	Information
12551	LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_BLK	Notice
12552	LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_PASS	Information
12553	LOG_ID_URL_FILTER_INVALID_CERT	Notice
12554	LOG_ID_URL_FILTER_INVALID_SESSION	Notice
12555	LOG_ID_URL_FILTER_SRV_CERT_ERR_BLK	Notice
12556	LOG_ID_URL_FILTER_SRV_CERT_ERR_PASS	Notice
12557	LOG_ID_URL_FILTER_FAMS_NOT_ACTIVE	Critical
12558	LOG_ID_URL_FILTER_RATING_ERR	Information
12559	LOG_ID_URL_FILTER_PASS	Information
12560	LOG_ID_URL_WISP_BLOCK	Warning
12561	LOG_ID_URL_WISP_REDIR	Warning
12562	LOG_ID_URL_WISP_ALLOW	Information
12800	LOG_ID_WEB_FTGD_ERR	Error
12801	LOG_ID_WEB_FTGD_WARNING	Warning
12802	LOG_ID_WEB_FTGD_QUOTA	Information

Message ID	Message	Severity
13056	LOG_ID_WEB_FTGD_CAT_BLK	Warning
13057	LOG_ID_WEB_FTGD_CAT_WARN	Warning
13312	LOG_ID_WEB_FTGD_CAT_ALLOW	Notice
13313	LOG_ID_WEB_FTGD_RULE_ALLOW	Notice
13314	LOG_ID_WEB_FTGD_OFF_SITE_ALLOW	Information
13315	LOG_ID_WEB_FTGD_QUOTA_COUNTING	Notice
13316	LOG_ID_WEB_FTGD_QUOTA_EXPIRED	Warning
13317	LOG_ID_WEB_URL	Notice
13568	LOG_ID_WEB_SCRIPTFILTER_ACTIVEX	Notice
13573	LOG_ID_WEB_SCRIPTFILTER_COOKIE	Notice
13584	LOG_ID_WEB_SCRIPTFILTER_APPLET	Notice
13600	LOG_ID_WEB_SCRIPTFILTER_OTHER	Notice
13601	LOG_ID_WEB_WF_COOKIE	Notice
13602	LOG_ID_WEB_WF_REFERER	Notice
13603	LOG_ID_WEB_WF_COMMAND_BLOCK	Warning
13616	LOG_ID_CONTENT_TYPE_BLOCK	Warning

Appendix A: Log Field Diff Between 5.2.0 and 5.4.0

Refer to the *FortiOS 5.2.0 Log Reference* and *FortiOS 5.4.0 Log Reference* for a complete list of log field details related to those versions. This section covers changes applicable to the 5.4.0 version only. It is recommended that you keep both the 5.2.0 and 5.4.0 *FortiOS Log Reference* documents available for a comparison of log field delta between the versions.

For all reference purposes, in the tables provided below (see tables) , the term **Removed** indicates that a log field was removed in version 5.4.0 but exists in version 5.2.0. Similarly, the term **Added** indicates that a log file was added in version 5.4.0 but does not exist in version 5.2.0.

Content

The following table provide a list of log fields that were added newly or removed from the content log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
action	Removed
agent	Removed
attachment	Removed
cat	Removed
cat_desc	Removed
client	Removed
clogver	Removed
column	Removed
connmode	Removed
content	Removed
cstatus	Removed
custom	Removed
date	Removed

Log Field Name	Description
devid	Removed
direction	Removed
dlpsensor	Removed
dstintf	Removed
dstip	Removed
dstname	Removed
dstport	Removed
duration	Removed
enddate	Removed
epoch	Removed
eventid	Removed
file	Removed
filename	Removed
filesize	Removed
from	Removed
ftpcmd	Removed
group	Removed
heuristic	Removed
hostname	Removed
infection	Removed
kind	Removed
laddr	Removed
level	Removed
line	Removed

Log Field Name	Description
local	Removed
logid	Removed
malformdata	Removed
malformdesc	Removed
messages	Removed
messagetype	Removed
method	Removed
msg	Removed
phone	Removed
policyid	Removed
profile	Removed
profilegroup	Removed
profiletype	Removed
proto	Removed
raddr	Removed
rcvdbyte	Removed
reason	Removed
remote	Removed
requestname	Removed
sentbyte	Removed
serial	Removed
server	Removed
sessionid	Removed
srcintf	Removed

Log Field Name	Description
srcip	Removed
srcname	Removed
srcport	Removed
startdate	Removed
status	Removed
subject	Removed
subtype	Removed
time	Removed
to	Removed
type	Removed
url	Removed
user	Removed
vd	Removed
virus	Removed

Event

The following tables provide a list of log fields that were added newly or removed between from the event log subtypes in FortiOS version 5.4.0.

Compliance-Check

Log Field Name	Description
action	Added
date	Added
devid	Added
level	Added

Log Field Name	Description
logdesc	Added
logid	Added
module	Added
msg	Added
reason	Added
result	Added
status	Added
subtype	Added
time	Added
type	Added
vd	Added

Endpoint

Log Field Name	Description
cveid	Added
devtype	Added
fctuid	Added
scantime	Added
severity	Added
srcname	Added
vendorurl	Added
vulncat	Added
vulnid	Added
vulnname	Added

GTP

Log Field Name	Description
apn	Removed
c-bytes	Removed
c-ggsn	Removed
c-ggsn-teid	Removed
c-gsn	Removed
c-pkts	Removed
c-sgsn	Removed
c-sgsn-teid	Removed
cpaddr	Removed
cpdladdr	Removed
cpdlisraddr	Removed
cpdlisrteid	Removed
cpdlteid	Removed
cpteid	Removed
cpuladdr	Removed
cpulteid	Removed
date	Removed
deny_cause	Removed
devid	Removed
dstport	Removed
dtlexp	Removed
duration	Removed
end-usr-address	Removed

Log Field Name	Description
from	Removed
headerteid	Removed
ietype	Removed
imei-sv	Removed
imsi	Removed
level	Removed
linked-nsapi	Removed
logdesc	Removed
logid	Removed
msg	Removed
msg-type	Removed
msisdn	Removed
nsapi	Removed
profile	Removed
rai	Removed
rat-type	Removed
selection	Removed
seqnum	Removed
snetwork	Removed
srcport	Removed
status	Removed
subtype	Removed
time	Removed
to	Removed

Log Field Name	Description
tunnel-idx	Removed
type	Removed
u-bytes	Removed
u-ggsn	Removed
u-ggsn-teid	Removed
u-gsn	Removed
u-pkts	Removed
u-sgsn	Removed
u-sgsn-teid	Removed
uli	Removed
user_data	Removed
vd	Removed
version	Removed

HA

Log Field Name	Description
date	Added
devid	Added
ip	Added
level	Added
logdesc	Added
logid	Added
msg	Added
subtype	Added

Log Field Name	Description
time	Added
type	Added
vd	Added

Router

Log Field Name	Description
action	Added
ddnsserver	Added
dhcp_msg	Added
dns_ip	Added
dns_name	Added
dst_init	Added
duid	Added
iaid	Added
lease	Added
logdesc	Added
mac	Added
service	Added
src_int	Added

System

Log Field Name	Description
community	Added
ddnsserver	Added
disklograte	Added

Log Field Name	Description
dport	Removed
dst	Removed
dst_port	Removed
dstip	Added
dstport	Added
duid	Added
expected	Removed
expectedhandshake	Added
expectedsignature	Added
fazlograte	Added
group	Added
iaid	Added
id	Removed
ip	Added
logdesc	Added
mac	Added
max-minor	Removed
maxminor	Added
member	Added
min-minor	Removed
minminor	Added
mode	Added
policy	Removed
probeid	Removed

Log Field Name	Description
profile	Added
receivedhandshake	Added
receivedsignature	Added
recv-minor	Removed
recvminor	Added
sn	Added
src	Removed
src-vis	Removed
src_port	Removed
srcip	Added
srcport	Added
state	Added
vcm	Removed
version	Added

User

Log Field Name	Description
category	Added
logdesc	Added
poolname	Added
portbegin	Added
portend	Added
profile	Removed
ui	Added

VPN

Log Field Name	Description
action	Added
error_num	Added
error_reason	Removed
name	Added
role	Added
status	Added
ui	Added
user	Added
version	Removed

WAD

Log Field Name	Description
dst	Removed
dstip	Added
logdesc	Added
reason	Added
src	Removed
srcip	Added

Wireless

Log Field Name	Description
bandwidth	Added
encryption	Added

Log Field Name	Description
group	Added
logdesc	Added
mac	Added
seq	Added
sn	Added
srcip	Added
status	Removed
user	Added

GTP

Log Field Name	Description
apn	Added
c-bytes	Added
c-ggsn	Added
c-ggsn-teid	Added
c-gsn	Added
c-pkts	Added
c-sgsn	Added
c-sgsn-teid	Added
cpaddr	Added
cpdladdr	Added
cpdlisraddr	Added
cpdlisrteid	Added
cpdlteid	Added

Log Field Name	Description
cpteid	Added
cpuladdr	Added
cpulteid	Added
date	Added
deny_cause	Added
devid	Added
dstport	Added
dtlexp	Added
duration	Added
end-usr-address	Added
from	Added
headerteid	Added
ietype	Added
imei-sv	Added
imsi	Added
level	Added
linked-nsapi	Added
log-id	Added
msg-type	Added
msisdn	Added
nsapi	Added
profile	Added
rai	Added
rat-type	Added

Log Field Name	Description
selection	Added
seqnum	Added
snetwork	Added
srcport	Added
status	Added
subtype	Added
time	Added
to	Added
tunnel-idx	Added
type	Added
u-bytes	Added
u-ggsn	Added
u-ggsn-teid	Added
u-gsn	Added
u-pkts	Added
u-sgsn	Added
u-sgsn-teid	Added
uli	Added
user_data	Added
vd	Added
version	Added

Security (UTM)

The following tables provide a list of log fields that were added newly or removed from the security (UTM) log subtypes in FortiOS version 5.4.0.

Anomaly

The following table provide a list of log fields that were added newly or removed from the security log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
action	Added
attack	Added
attackid	Added
count	Added
craction	Added
crlevel	Added
crscore	Added
date	Added
devid	Added
dstintf	Added
dstip	Added
dstport	Added
eventtype	Added
group	Added
icmpcode	Added
icmpid	Added
icmptype	Added
level	Added
logid	Added
msg	Added
policyid	Added

Log Field Name	Description
policytype	Added
proto	Added
ref	Added
service	Added
sessionid	Added
severity	Added
srccountry	Added
srcintf	Added
srcip	Added
srcport	Added
subtype	Added
time	Added
type	Added
user	Added
vd	Added

App

The following table provide a list of log fields that were added newly or removed from the security log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
crlevel	Added
crscore	Added
dstintf	Added
dstname	Added
policyid	Added

Log Field Name	Description
profile	Added
profiletype	Added
srcintf	Added
srcname	Added

AV

The following table provide a list of log fields that were added newly or removed from the security log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
crlevel	Added
crscore	Added
dstintf	Added
policyid	Added
profiletype	Removed
rcvdbyte	Removed
sentbyte	Removed
srcintf	Added

DLP

The following table provide a list of log fields that were added newly or removed from the security log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
dstintf	Added
mmsdir	Added
policyid	Added
profiletype	Removed
srcintf	Added

Email

The following table provide a list of log fields that were added newly or removed from the security log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
dstintf	Added
policyid	Added
profiletype	Removed
srcintf	Added

IPS

The following table provide a list of log fields that were added newly or removed from the security log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
craction	Added
crlevel	Added
crscore	Added
dstintf	Added
hostname	Added
policyid	Added
rcvdbyte	Removed
sentbyte	Removed
srccountry	Added
srcintf	Added
url	Added

Web

The following table provide a list of log fields that were added newly or removed from the security log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
crlevel	Added
crscore	Added
dstintf	Added
policyid	Added
profiletype	Removed
referralurl	Added
srcintf	Added

Traffic

The following table provide a list of log fields that were added newly or removed from the traffic log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
ap	Added
apsn	Added
centralnatid	Added
channel	Added
countwaf	Added
crlevel	Added
hostname	Removed
policymode	Added
policytype	Added
radioband	Added
shapingpolicyid	Added
sslexempt	Added
vwpvlanid	Added

WAF

Log Field Name	Description
action	Added
constraint	Added
date	Added
devid	Added
direction	Added
dstintf	Added
dstip	Added
dstport	Added
eventid	Added
eventtype	Added
group	Added
level	Added
logid	Added
method	Added
msg	Added
name	Added
policyid	Added
profile	Added
proto	Added
service	Added
sessionid	Added
severity	Added

Log Field Name	Description
srcintf	Added
srcip	Added
srcport	Added
subtype	Added
time	Added
type	Added
url	Added
user	Added
vd	Added

Other logs

The following tables provide a list of log fields that were added newly or removed between the from the other log types in FortiOS version 5.4.0.

Netscan

Log Field Name	Description
action	Removed
agent	Removed
assetid	Removed
assetname	Removed
custom	Removed
date	Removed
devid	Removed
direction	Removed
dstintf	Removed

Log Field Name	Description
dstip	Removed
dstname	Removed
dstport	Removed
end	Removed
engine	Removed
eventtype	Removed
group	Removed
level	Removed
logid	Removed
method	Removed
msg	Removed
os	Removed
osfamily	Removed
osgen	Removed
osvendor	Removed
plugin	Removed
policyid	Removed
profile	Removed
profilegroup	Removed
proto	Removed
serial	Removed
service	Removed
severity	Removed
srcintf	Removed

Log Field Name	Description
srcip	Removed
srcname	Removed
srcport	Removed
start	Removed
status	Removed
subtype	Removed
time	Removed
type	Removed
user	Removed
vd	Removed
vuln	Removed
vulncat	Removed
vulncnt	Removed
vulnid	Removed
vulnref	Removed
vulnscore	Removed

VOIP

Log Field Name	Description
dst	Removed
dstip	Added
locip	Added
locport	Added
remip	Added

Log Field Name	Description
remport	Added
src	Removed
srcip	Added

Appendix B: Log Field Diff for 5.2.9 and 5.4.0

Refer to the *FortiOS 5.2.9 Log Reference* for a complete list of log field details related to version 5.2.9. This section covers changes applicable to the 5.4.0 version only. It is recommended that you keep both the 5.2.9 and 5.4.0 *FortiOS Log Reference* available for a comparison of log field delta between the versions.

For all reference purposes, in the tables provided below (see tables) , the term **Removed** indicates that a log field was removed in version 5.4.0 but exists in version 5.2.9. Similarly, the term **Added** indicates that a log file was added in version 5.4.0 but does not exist in version 5.2.9.

Traffic

The following table provide a list of log fields that were added newly or removed from the traffic log subtypes in FortiOS version 5.4.0.

Log Field Name	Description
ap	Added
apsn	Added
centralnatid	Added
channel	Added
countwaf	Added
policymode	Added
policytype	Added
radioband	Added
shapingpolicyid	Added
sslexempt	Added
vwpvlanid	Added

Event

The following tables provide a list of log fields that were added newly or removed between from the event log subtypes in FortiOS version 5.4.0.

Compliance-Check

Log Field Name	Description
action	Added
date	Added
devid	Added
level	Added
logdesc	Added
logid	Added
module	Added
msg	Added
reason	Added
result	Added
status	Added
subtype	Added
time	Added
type	Added
vd	Added

Endpoint

Log Field Name	Description
cveid	Added
devtype	Added
fctuid	Added
scantime	Added
severity	Added

Log Field Name	Description
srcname	Added
vendorurl	Added
vulncat	Added
vulnid	Added
vulnname	Added

Router

Log Field Name	Description
ddnsserver	Added
duid	Added
iaid	Added

System

Log Field Name	Description
ddnsserver	Added
dir	Removed
duid	Added
iaid	Added

Security (UTM)

The following tables provide a list of log fields that were added newly or removed from the security (UTM) log subtypes in FortiOS version 5.4.0.

Anomaly

Log Field Name	Description
agent	Removed

Log Field Name	Description
attackcontext	Removed
attackcontextid	Removed
direction	Removed
hostname	Removed
incidentserialno	Removed
policytype	Added
profile	Removed
profiletype	Removed
sniffer	Removed

IPS

Log Field Name	Description
sniffer	Removed
url	Added

Web

Log Field Name	Description
referralurl	Added

GTP

Log Field Name	Description
apn	Added
c-bytes	Added
c-ggsn	Added

Log Field Name	Description
c-ggsn-teid	Added
c-gsn	Added
c-pkts	Added
c-sgsn	Added
c-sgsn-teid	Added
cpaddr	Added
cpdladdr	Added
cpdlisraddr	Added
cpdlisrteid	Added
cpdlteid	Added
cpteid	Added
cpuladdr	Added
cpulteid	Added
date	Added
deny_cause	Added
devid	Added
dstport	Added
dtlexp	Added
duration	Added
end-usr-address	Added
from	Added
headerteid	Added
ietype	Added
imei-sv	Added

Log Field Name	Description
imsi	Added
level	Added
linked-nsapi	Added
logid	Added
msg-type	Added
msisdn	Added
nsapi	Added
profile	Added
rai	Added
rat-type	Added
selection	Added
seqnum	Added
snetwork	Added
srcport	Added
status	Added
subtype	Added
time	Added
to	Added
tunnel-idx	Added
type	Added
u-bytes	Added
u-ggsn	Added
u-ggsn-teid	Added
u-gsn	Added

Log Field Name	Description
u-pkts	Added
u-sgsn	Added
u-sgsn-teid	Added
uli	Added
user_data	Added
vd	Added
version	Added

WAF

Log Field Name	Description
action	Added
agent	Added
constraint	Added
date	Added
devid	Added
direction	Added
dstintf	Added
dstip	Added
dstport	Added
eventid	Added
eventtype	Added
group	Added
level	Added
logid	Added

Log Field Name	Description
method	Added
msg	Added
name	Added
policyid	Added
profile	Added
proto	Added
service	Added
sessionid	Added
severity	Added
srcintf	Added
srcip	Added
srcport	Added
subtype	Added
time	Added
type	Added
url	Added
user	Added
vd	Added

Netscan

Log Field Name	Description
action	Removed
agent	Removed
assetid	Removed

Log Field Name	Description
assetname	Removed
date	Removed
devid	Removed
direction	Removed
dstintf	Removed
dstip	Removed
dstname	Removed
dstport	Removed
end	Removed
engine	Removed
eventtype	Removed
group	Removed
level	Removed
logid	Removed
method	Removed
msg	Removed
os	Removed
osfamily	Removed
osgen	Removed
osvendor	Removed
plugin	Removed
policyid	Removed
profile	Removed
profilegroup	Removed

Log Field Name	Description
proto	Removed
serial	Removed
service	Removed
severity	Removed
srcintf	Removed
srcip	Removed
srcname	Removed
srcport	Removed
start	Removed
status	Removed
subtype	Removed
time	Removed
type	Removed
user	Removed
vd	Removed
vuln	Removed
vulncat	Removed
vulncnt	Removed
vulnid	Removed
vulnref	Removed
vulnscore	Removed

VOIP

Log Field Name	Description
locip	Added
locport	Added
remip	Added
remport	Added

Appendix C: Log ID Diff for 5.2.0 and 5.4.0

Refer to the *FortiOS 5.2.0 Log Reference* and *FortiOS 5.4.0 Log Reference* for a complete list of log ID details related to those versions. This section covers changes applicable to the 5.4.0 version only. It is recommended that you keep both the 5.2.0 and 5.4.0 *FortiOS Log Reference* documents available for a comparison of log ID delta between the versions.

For all reference purposes, in the tables provided below (see tables) , the term **Removed** indicates that a log ID was removed in version 5.4.0 but exists in version 5.2.0. Similarly, the term **Added** indicates that a log ID was added in version 5.4.0 but does not exist in version 5.2.0.

Event

The following tables provide a list of log IDs that were added newly or removed between from the event log subtypes in FortiOS version 5.4.0.

COMPLIANCE-CHECK

Log ID	Message	Description
45151	LOG_ID_EVENT_DSSCC_FAIL	Added
45152	LLOG_ID_EVENT_DSSCC_PASS	Added

Endpoint

Log ID	Message	Description
45056	LOG_ID_FCC_EXCEED	Removed
45059	LOG_ID_FCC_UPGRADE_SUCC	Removed
45060	LOG_ID_FCC_UPGRADE_FAIL	Removed
45061	LOG_ID_FCC_CLOSE_BY_TYPE	Added
45071	LOG_ID_FCC_VULN_SCAN	Added
45112	LOG_ID_EC_REG_FAIL_KEY	Added
45113	LOG_ID_EC_REG_FAIL_BLOCKED	Added

Log ID	Message	Description
45114	LOG_ID_EC_REG_QUARANTINE	Added
45115	LOG_ID_EC_REG_UNQUARANTINE	Added
45116	LOG_ID_EC_REG_UNQUARANTINE_ALL	Added
45117	LOG_ID_EC_REG_FAIL_VER	Added

GTP

Log ID	Message	Description
41216	LOGID_GTP_FORWARD	Removed
41217	LOGID_GTP_DENY	Removed
41218	LOGID_GTP_RATE_LIMIT	Removed
41219	LOGID_GTP_STATE_INVALID	Removed
41220	LOGID_GTP_TUNNEL_LIMIT	Removed
41221	LOGID_GTP_TRAFFIC_COUNT	Removed
41222	LOGID_GTP_USER_DATA	Removed
41223	LOGID_GTPV2_FORWARD	Removed
41224	LOGID_GTPV2_DENY	Removed
41225	LOGID_GTPV2_RATE_LIMIT	Removed
41226	LOGID_GTPV2_STATE_INVALID	Removed
41227	LOGID_GTPV2_TUNNEL_LIMIT	Removed
41228	LOGID_GTPV2_TRAFFIC_COUNT	Removed
41229	LOGID_GTPU_FORWARD	Removed
41230	LOGID_GTPU_DENY	Removed

HA

Log ID	Message	Description
35004	LOG_ID_HA_SYNC_FLDB	Added
35008	LOG_ID_HA_SYNC_VCM	Removed
35011	LOG_ID_HA_SYNC_FAIL	Added
35012	LOG_ID_CONF_SYNC_FAIL	Added
37905	MESGID_HA_ENABLE_SET_AS_MASTER	Added
37906	MESGID_HA_DISABLE_SET_AS_MASTER	Added
37907	MESGID_VLAN_HB_UP	Added
37908	MESGID_VLAN_HB_DOWN	Added
37909	MESGID_VLAN_HB_DOWN_SUM	Added

Router

Log ID	Message	Description
20301	LOG_ID_VZ_LOG	Added
20302	LOG_ID_OSPF_NB_STAT_CHG	Added
20303	LOG_ID_OSPF6_NB_STAT_CHG	Added
20401	LOG_ID_ROUTER_CLEAR	Added

System

Log ID	Message	Description
20000	20000	Removed
20008	LOG_ID_POLICY6_TOO_BIG	Added
20010	LOG_ID_KERNEL_ERROR	Added
20022	LOG_ID_MODEM_USB_REMOVED	Added

Log ID	Message	Description
20023	LOG_ID_MODEM_USBLTE_DETECTED	Added
20024	LOG_ID_MODEM_USBLTE_REMOVED	Added
20028	LOG_ID_REPORT_RECREATE_DB	Added
20109	LOG_ID_WEB_LIC_EXPIRED	Added
20113	LOG_ID_IPSA_DOWNLOAD_FAIL	Added
20114	LOG_ID_IPSA_SELFTEST_FAIL	Added
20115	LOG_ID_IPSA_STATUSUPD_FAIL	Added
20116	LOG_ID_SPAM_LIC_EXPIRED	Added
20118	LOG_ID_WEBF_STATUS_REACH	Added
20119	LOG_ID_WEBF_STATUS_UNREACH	Added
20207	LOG_ID_RAD_MISMATCH_VALID_TIME	Added
20208	LOG_ID_ZOMBIE_DAEMON_CLEANUP	Added
20209	LOG_ID_DISK_UNAVAIL	Added
20220	20220	Added
20221	20221	Added
22017	LOG_ID_EXCEED_GLOB_RES_LIMIT	Added
22018	LOG_ID_EXCEED_VD_RES_LIMIT	Added
22103	LOG_ID_QUAR_DAILY_LIMIT_REACHED	Added
22107	LOG_ID_VOLT_ANOM	Added
22108	LOG_ID_FAN_ANOM	Added
22109	LOG_ID_TEMP_TOO_HIGH	Added
22150	LOG_ID_VOLT_NOM	Added
22151	LOG_ID_FAN_NOM	Added
22152	LOG_ID_TEMP_TOO_LOW	Added

Log ID	Message	Description
22153	LOG_ID_TEMP_NORM	Added
22202	LOG_ID_AUTO_UPT_CERT_FAIL	Removed
22204	LOG_ID_AUTO_GEN_CERT_PENDING	Added
22205	LOG_ID_AUTO_GEN_CERT_SUCC	Added
22206	LOG_ID_CRL_EXPIRED	Added
22701	LOG_ID_IPS_FAIL_OPEN_END	Added
22891	LOG_ID_FLCFGD	Added
22913	LOG_ID_FDS_SRV_DISCON	Added
22914	LOG_ID_FDS_SRV_CHG	Added
22915	LOG_ID_FDS_SRV_CON	Added
22918	LOG_ID_FDS_CTRL_STATUS	Added
26006	LOG_ID_DHCP_LEASE_USAGE_FULL	Added
26007	LOG_ID_DHCP_BLOCKED_MAC	Added
26008	LOG_ID_DHCP_DDNS_ADD	Added
26009	LOG_ID_DHCP_DDNS_DELETE	Added
26010	LOG_ID_DHCP_DDNS_COMPLETED	Added
26011	LOG_ID_DHCPV6_REPLY	Added
26012	LOG_ID_DHCPV6_RELEASE	Added
29021	LOG_ID_EVENT_AUTH_SNMP_QUERY_FAILED	Added
29022	LOG_ID_DDNS_UPDATE_FAIL	Added
32016	LOG_ID_FDS_QUOTA_WARN	Added
32017	LOG_ID_FDS_DAILY_QUOTA_FULL	Added
32019	LOG_ID_CC_ENTER_ERR_MOD	Added
32026	LOG_ID_STORE_CONF_FAIL	Removed

Log ID	Message	Description
32031	LOG_ID_VIEW_MEM_LOG_FAIL	Added
32032	LOG_ID_DISK_DLP_ARCH_FULL	Added
32033	LOG_ID_DISK_QUAR_FULL	Added
32034	LOG_ID_DISK_REPORT_FULL	Added
32036	LOG_ID_DISK_IPS_ARCH_FULL	Added
32037	LOG_ID_DISK_LOG_FIRST_FULL	Added
32038	LOG_ID_LOG_ROLL_FORTICRON	Added
32039	LOG_ID_VIEW_MEM_LOG_SUCC	Added
32041	LOG_ID_REPORT_DELETED_GUI	Added
32042	LOG_ID_MEM_LOG_SECOND_FULL	Added
32043	LOG_ID_MEM_LOG_FINAL_FULL	Added
32044	LOG_ID_LOG_DELETE	Added
32046	LOG_ID_SSL_CORRPUT_MAC	Added
32104	LOG_ID_CHG_CONFIG_GUI	Added
32105	LOG_ID_NTP_SVR_STAUS_CHG_REACHABLE	Added
32106	LOG_ID_NTP_SVR_STAUS_CHG_RESOLVABLE	Added
32107	LOG_ID_NTP_SVR_STAUS_CHG_UNRESOLVABLE	Added
32108	LOG_ID_NTP_SVR_STAUS_CHG_UNREACHABLE	Added
32109	LOG_ID_UPD_SIGN_AV_DB	Added
32110	LOG_ID_UPD_SIGN_IPS_DB	Added
32111	LOG_ID_UPD_SIGN_AVIPS_DB	Added
32113	LOG_ID_UPD_SIGN_SRCVIS_DB	Added
32114	LOG_ID_UPD_SIGN_GEOIP_DB	Added
32115	LOG_ID_UPD_SIGN_SERVER_LIST	Added

Log ID	Message	Description
32116	LOG_ID_UPD_SIGN_AVPKG_FAILURE	Added
32117	LOG_ID_UPD_SIGN_AVPKG_SUCCESS	Added
32118	LOG_ID_UPD_ADMIN_AV_DB	Added
32119	LOG_ID_UPD_SCANUNIT_AV_DB	Added
32139	LOG_ID_UPD_SIGN_DB	Removed
32141	LOG_ID_TIME_NTP_SETTING_CHG	Added
32143	LOG_ID_BACKUP_CONF_BY_SCP	Added
32169	LOG_ID_ALARM_DLP_DB	Added
32188	LOG_ID_SSL_PROXY_CA_INIT_FAIL	Removed
32190	LOG_ID_UPT_INVALID_IMG	Added
32191	LOG_ID_UPT_INVALID_IMG_CC	Added
32192	LOG_ID_UPT_INVALID_IMG_RSA	Added
32193	LOG_ID_UPT_IMG_RSA	Added
32194	LOG_ID_UPT_IMG_FAIL	Added
32199	LOG_ID_RESTORE_IMG_USB	Added
32227	LOG_ID_UPD_DLP_FAIL	Added
32228	LOG_ID_LOAD_IMG_FAIL_WRONG_IMG	Added
32229	LOG_ID_LOAD_IMG_FAIL_NO_RSA	Added
32230	LOG_ID_LOAD_IMG_FAIL_INVALID_RSA	Added
32231	LOG_ID_RESTORE_FGD_SVR_FAIL	Added
32232	LOG_ID_RESTORE_VDOM_LIC_FAIL	Added
32233	LOG_ID_BACKUP_IMG_FAIL	Added
32234	LOG_ID_RESTORE_IMG_INVALID_CC	Added
32235	LOG_ID_RESTORE_IMG_FORTIGUARD	Added

Log ID	Message	Description
32236	LOG_ID_BACKUP_MEM_LOG	Added
32237	LOG_ID_BACKUP_MEM_LOG_FAIL	Added
32238	LOG_ID_BACKUP_DISK_LOG_FAIL	Added
32239	LOG_ID_BACKUP_DISK_LOG_USB	Added
32241	LOG_ID_BACKUP_DISK_LOG_USB_FAIL	Added
32242	LOG_ID_UPD_VDOM_LIC_FAIL	Added
32243	LOG_ID_UPD_IPS_SCP	Added
32244	LOG_ID_UPD_IPS_SCP_FAIL	Added
32245	LOG_ID_BACKUP_USER_DEF_IPS_FAIL	Added
32340	LOG_ID_LOG_DISK_UNAVAIL	Removed
32547	LOG_ID_AUTOSCRIPT_START	Added
32548	LOG_ID_AUTOSCRIPT_STOP	Added
32561	LOG_ID_ADMIN_LOGOUT_DISCONNECT	Added
32562	LOG_ID_STORE_CONF_FAIL_SPACE	Added
32564	LOG_ID_RESTORE_CONF_FAIL	Added
32565	LOG_ID_RESTORE_CONF_BY_MGMT	Added
32566	LOG_ID_RESTORE_CONF_BY_SCP	Added
32567	LOG_ID_RESTORE_CONF_BY_USB	Added
32568	LOG_ID_DEL_REVISION_DB	Added
32569	LOG_ID_FSW_SWITCH_LOG_EVENT	Added
38408	LOGID_EVENT_OFTP_SSL_CONNECTED	Added
38409	LOGID_EVENT_OFTP_SSL_DISCONNECTED	Added
38410	LOGID_EVENT_OFTP_SSL_FAILED	Added
38411	LOGID_EVENT_TWO_F_AUTH_CODE_SENDTO	Added

Log ID	Message	Description
38412	LOGID_EVENT_TOKEN_CODE_SENDTO	Added
41005	LOG_ID_UPD_VCM	Removed
42201	LOG_ID_NETX_VMX_ATTACH	Added
42203	LOG_ID_NETX_VMX_DENIED	Added
43777	LOG_ID_EVENT_NAC_ANOMALY_QUARANTINE	Added
44548	LOGID_EVENT_CONFIG_EXEC	Added
45161	LOG_ID_EVENT_DSSCC_EXEC	Added

User

Log ID	Message	Description
38012		Added
43008		Added
43009		Added
43010		Added
43014		Added
43015		Added
43040		Added
43041		Added
43042		Added
43043		Added
43044		Added

VPN

Log ID	Message	Description
37120	MESGID_NEG_GENERIC_P1_NOTIF	Added

Log ID	Message	Description
37121	MESGID_NEG_GENERIC_P1_ERROR	Added
37122	MESGID_NEG_GENERIC_P2_NOTIF	Added
37123	MESGID_NEG_GENERIC_P2_ERROR	Added
37127	MESGID_NEG_PROGRESS_P1_NOTIF	Added
37128	MESGID_NEG_PROGRESS_P1_ERROR	Added
37129	MESGID_NEG_PROGRESS_P2_NOTIF	Added
37130	MESGID_NEG_PROGRESS_P2_ERROR	Added
37131	MESGID_ESP_ERROR	Added
37132	MESGID_ESP_CRITICAL	Added
37140	MESGID_AUTO_IPSEC	Removed
37184	MESGID_NEG_GENERIC_P1_NOTIF_IKEV2	Added
37185	MESGID_NEG_GENERIC_P1_ERROR_IKEV2	Added
37186	MESGID_NEG_GENERIC_P2_NOTIF_IKEV2	Added
37187	MESGID_NEG_GENERIC_P2_ERROR_IKEV2	Added
37191	MESGID_NEG_PROGRESS_P1_NOTIF_IKEV2	Added
37192	MESGID_NEG_PROGRESS_P1_ERROR_IKEV2	Added
37193	MESGID_NEG_PROGRESS_P2_NOTIF_IKEV2	Added
37194	MESGID_NEG_PROGRESS_P2_ERROR_IKEV2	Added
37195	MESGID_ESP_ERROR_IKEV2	Added
37196	MESGID_ESP_CRITICAL_IKEV2	Added
39424	LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_UP	Added
39425	LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_DOWN	Added
39426	LOG_ID_EVENT_SSL_VPN_USER_SSL_LOGIN_FAIL	Added
39936	LOG_ID_EVENT_SSL_VPN_SESSION_WEB_TUNNEL_ STATS	Added

Log ID	Message	Description
39937	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_DENY	Added
39938	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_PASS	Added
39939	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_TIMEOUT	Added
39940	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_CLOSE	Added
39941	LOG_ID_EVENT_SSL_VPN_SESSION_SYS_BUSY	Added
39942	LOG_ID_EVENT_SSL_VPN_SESSION_CERT_OK	Added
39943	LOG_ID_EVENT_SSL_VPN_SESSION_NEW_CON	Added
39944	LOG_ID_EVENT_SSL_VPN_SESSION_ALERT	Added
39945	LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_FAIL	Added
39946	LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_ERR	Added
39947	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UP	Added
39948	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_DOWN	Added
39949	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_STATS	Added
39950	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ UNKNOWNTAG	Added
39951	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ERROR	Added
39952	LOG_ID_EVENT_SSL_VPN_SESSION_ENTER_CONSERVE_ MODE	Added
39953	LOG_ID_EVENT_SSL_VPN_SESSION_LEAVE_CONSERVE_ MODE	Added
40001	LOG_ID_PPTP_TUNNEL_UP	Added
40002	LOG_ID_PPTP_TUNNEL_DOWN	Added
40003	LOG_ID_PPTP_TUNNEL_STAT	Added
40016	LOG_ID_L2TPD_SVR_DISCON	Removed
40101	LOG_ID_L2TP_TUNNEL_UP	Added
40102	LOG_ID_L2TP_TUNNEL_DOWN	Added

Log ID	Message	Description
40103	LOG_ID_L2TP_TUNNEL_STAT	Added
41986	LOG_ID_EVENT_VPN_CERT_REGEN	Added
41991	LOG_ID_EVENT_VPN_CERT_EXPORT	Added

WAD

Log ID	Message	Description
48030	LOG_ID_WAD_SSL_CLIENT_CERT_REQUEST	Added
48038	LOG_ID_WAD_SSL_RCV_FATAL_ALERT	Added
48039	LOG_ID_WAD_SSL_SENT_FATAL_ALERT	Added

Wireless

Log ID	Message	Description
43520	LOG_ID_EVENT_WIRELESS_SYS	Removed
43522	LOG_ID_EVENT_WIRELESS_WTP	Removed
43524	LOG_ID_EVENT_WIRELESS_STA	Removed
43526	LOG_ID_EVENT_WIRELESS_WTPR	Removed
43527	LOG_ID_EVENT_WIRELESS_ROGUE_CFG	Removed
43529	LOG_ID_EVENT_WIRELESS_CLB	Removed
43551	LOG_ID_EVENT_WIRELESS_WTP_JOIN	Added
43552	LOG_ID_EVENT_WIRELESS_WTP_LEAVE	Added
43553	LOG_ID_EVENT_WIRELESS_WTP_FAIL	Added
43554	LOG_ID_EVENT_WIRELESS_WTP_UPDATE	Added
43555	LOG_ID_EVENT_WIRELESS_WTP_RESET	Added
43556	LOG_ID_EVENT_WIRELESS_WTP_KICK	Added
43557	LOG_ID_EVENT_WIRELESS_WTP_ADD_FAILURE	Added

Log ID	Message	Description
43558	LOG_ID_EVENT_WIRELESS_WTP_CFG_ERR	Added
43559	LOG_ID_EVENT_WIRELESS_WTP_SN_MISMATCH	Added
43560	LOG_ID_EVENT_WIRELESS_SYS_AC_RESTARTED	Added
43561	LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_UP	Added
43562	LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_DOWN	Added
43563	LOG_ID_EVENT_WIRELESS_ROGUE_DETECT	Added
43564	LOG_ID_EVENT_WIRELESS_ROGUE_OFFAIR	Added
43565	LOG_ID_EVENT_WIRELESS_ROGUE_ONAIR	Added
43566	LOG_ID_EVENT_WIRELESS_ROGUE_OFFWIRE	Added
43567	LOG_ID_EVENT_WIRELESS_FAKEAP_DETECT	Added
43568	LOG_ID_EVENT_WIRELESS_FAKEAP_ONAIR	Added
43569	LOG_ID_EVENT_WIRELESS_ROGUE_SUPPRESSED	Added
43570	LOG_ID_EVENT_WIRELESS_ROGUE_UNSUPPRESSED	Added
43571	LOG_ID_EVENT_WIRELESS_ROGUE_DETECT_CHG	Added
43572	LOG_ID_EVENT_WIRELESS_STA_ASSO	Added
43573	LOG_ID_EVENT_WIRELESS_STA_AUTH	Added
43574	LOG_ID_EVENT_WIRELESS_STA_DASS	Added
43575	LOG_ID_EVENT_WIRELESS_STA_DAUT	Added
43576	LOG_ID_EVENT_WIRELESS_STA_IDLE	Added
43577	LOG_ID_EVENT_WIRELESS_STA_DENY	Added
43578	LOG_ID_EVENT_WIRELESS_STA_KICK	Added
43579	LOG_ID_EVENT_WIRELESS_STA_IP	Added
43580	LOG_ID_EVENT_WIRELESS_STA_LEAVE_WTP	Added
43581	LOG_ID_EVENT_WIRELESS_STA_WTP_DISCONN	Added

Log ID	Message	Description
43582	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_UNCLASSIFIED	Added
43583	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ACCEPTED	Added
43584	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ROGUE	Added
43585	LOG_ID_EVENT_WIRELESS_ROGUE_CFG_SUPPRESSED	Added
43586	LOG_ID_EVENT_WIRELESS_WTPR_DARRP_CHAN	Added
43587	LOG_ID_EVENT_WIRELESS_WTPR_DARRP_START	Added
43588	LOG_ID_EVENT_WIRELESS_WTPR_OPER_CHAN	Added
43589	LOG_ID_EVENT_WIRELESS_WTPR_RADAR	Added
43590	LOG_ID_EVENT_WIRELESS_WTPR_NOL	Added
43591	LOG_ID_EVENT_WIRELESS_WTPR_COUNTRY_CFG_ SUCCESS	Added
43592	LOG_ID_EVENT_WIRELESS_WTPR_OPER_COUNTRY	Added
43593	LOG_ID_EVENT_WIRELESS_WTPR_CFG_TXPOWER	Added
43594	LOG_ID_EVENT_WIRELESS_WTPR_OPER_TXPOWER	Added
43595	LOG_ID_EVENT_WIRELESS_CLB_DENY	Added
43596	LOG_ID_EVENT_WIRELESS_CLB_RETRY	Added
43597	LOG_ID_EVENT_WIRELESS_WTP_ADD	Added
43598	LOG_ID_EVENT_WIRELESS_WTP_ADD_XSS	Added
43599	LOG_ID_EVENT_WIRELESS_WTP_DEL	Added
43600	LOG_ID_EVENT_WIRELESS_WTPR_DARRP_STOP	Added
43601	LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON	Added
43602	LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_SUCCESS	Added
43603	LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_FAILURE	Added
43604	LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_REQUEST	Added
43605	LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_SUCCESS	Added

Log ID	Message	Description
43606	LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_FAILURE	Added
43607	LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_CHECK	Added
43608	LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_DECLINE	Added
43609	LOG_ID_EVENT_WIRELESS_SYS_AC_DARRP_START	Added
43610	LOG_ID_EVENT_WIRELESS_SYS_AC_DARRP_STOP	Added
43611	LOG_ID_EVENT_WIRELESS_SYS_AC_UP	Added
43612	LOG_ID_EVENT_WIRELESS_SYS_AC_CFG_LOADED	Added
43613	LOG_ID_EVENT_WIRELESS_WTP_ERR	Added
43614	LOG_ID_EVENT_WIRELESS_DHCP_STAVATION	Log ID Added

GTP

The following tables provide a list of log IDs that were added newly or removed between from the GTP logs in FortiOS version 5.4.0.

Log ID	Message	Description
41216	LOGID_GTP_FORWARD	Added
41217	LOGID_GTP_DENY	Added
41218	LOGID_GTP_RATE_LIMIT	Added
41219	LOGID_GTP_STATE_INVALID	Added
41220	LOGID_GTP_TUNNEL_LIMIT	Added
41221	LOGID_GTP_TRAFFIC_COUNT	Added
41222	LOGID_GTP_USER_DATA	Added
41223	LOGID_GTPV2_FORWARD	Added
41224	LOGID_GTPV2_DENY	Added

Log ID	Message	Description
41225	LOGID_GTPV2_RATE_LIMIT	Added
41226	LOGID_GTPV2_STATE_INVALID	Added
41227	LOGID_GTPV2_TUNNEL_LIMIT	Added
41228	LOGID_GTPV2_TRAFFIC_COUNT	Added
41229	LOGID_GTPU_FORWARD	Added
41230	LOGID_GTPU_DENY	Added

Security

The following tables provide a list of log IDs that were added newly or removed between from the security log subtypes in FortiOS version 5.4.0.

Anomaly

Log ID	Message	Description
18432	LOGID_ATTCK_ANOMALY_TCP_UDP	Added
18433	LOGID_ATTCK_ANOMALY_ICMP	Added
18434	LOGID_ATTCK_ANOMALY_OTHERS	Added

AntiVirus

Log ID	Message	Description
9238	MESGID_ANALYTICS_FSA_RESULT	Added
9248	MESGID_BOTNET_WARNING	Added
9249	MESGID_BOTNET_NOTIF	Added

IPS

Log ID	Message	Description
18432	LOGID_ATTCK_ANOMALY_TCP_UDP	Removed

Log ID	Message	Description
18433	LOGID_ATTCK_ANOMALY_ICMP	Removed
18434	LOGID_ATTCK_ANOMALY_OTHERS	Removed

Web Filter

Log ID	Message	Description
12560	LOG_ID_URL_WISP_BLOCK	Added
12561	LOG_ID_URL_WISP_REDIR	Added
12562	LOG_ID_URL_WISP_ALLOW	Added

Traffic

The following tables provide a list of log IDs that were added newly or removed between from the traffic log in FortiOS version 5.4.0.

Log ID	Message	Description
19	LOG_ID_TRAFFIC_BROADCAST	Added

WAF

The following tables provide a list of log IDs that were added newly or removed between from the WAF logs in FortiOS version 5.4.0.

Log ID	Message	Description
30248	LOGID_WAF_SIGNATURE_BLOCK	Added
30249	LOGID_WAF_SIGNATURE_PASS	Added
30250	LOGID_WAF_SIGNATURE_ERASE	Added
30251	LOGID_WAF_CUSTOM_SIGNATURE_BLOCK	Added
30252	LOGID_WAF_CUSTOM_SIGNATURE_PASS	Added
30253	LOGID_WAF_METHOD_BLOCK	Added

Log ID	Message	Description
30255	LOGID_WAF_ADDRESS_LIST_BLOCK	Added
30257	LOGID_WAF_CONSTRAINTS_BLOCK	Added
30258	LOGID_WAF_CONSTRAINTS_PASS	Added
30259	LOGID_WAF_URL_ACCESS_PERMIT	Added
30260	LOGID_WAF_URL_ACCESS_BYPASS	Added
30261	LOGID_WAF_URL_ACCESS_BLOCK	Added

Other Logs

The following tables provide a list of log IDs that were added newly or removed between from the security log subtypes in FortiOS version 5.4.0.

Netscan

Log ID	Message	Description
4096	LOG_ID_NETSCAN_VULN_SCAN	Removed
4097	LOG_ID_NETSCAN_DISCOVERY_SCAN	Removed
4098	LOG_ID_NETSCAN_VULN_DETECT	Removed
4099	LOG_ID_NETSCAN_OS_DETECT	Removed
4100	LOG_ID_NETSCAN_SERVICE_DETECT	Removed
4101	LOG_ID_NETSCAN_VULN_MESSAGE	Removed
4102	LOG_ID_NETSCAN_DISCOVERY_MESSAGE	Removed
4103	LOG_ID_NETSCAN_VULN_COUNT	Removed
4104	LOG_ID_NETSCAN_HOST_DETECT	Removed
4105	LOG_ID_NETSCAN_PORT_DETECT	Removed

VOIP

Log ID	Message	Description
44032	LOGID_EVENT_VOIP_SIP	Added
44033	LOGID_EVENT_VOIP_SIP_BLOCK	Added
44034	LOGID_EVENT_VOIP_SIP_FUZZING	Added
44035	LOGID_EVENT_VOIP_SCCP_REGISTER	Added
44036	LOGID_EVENT_VOIP_SCCP_UNREGISTER	Added
44037	LOGID_EVENT_VOIP_SCCP_CALL_BLOCK	Added
44038	LOGID_EVENT_VOIP_SCCP_CALL_INFO	Added

Appendix D: Log ID Diff for 5.2.9 and 5.4.0

Refer to the *FortiOS 5.2.9 Log Reference* for a complete list of log ID details related to version 5.2.9. This section covers changes applicable to the 5.4.0 version only. It is recommended that you keep both the 5.2.9 and 5.4.0 *FortiOS Log Reference* available for a comparison of log ID delta between the versions.

For all reference purposes, in the tables provided below (see tables) , the term **Removed** indicates that a log ID was removed in version 5.4.0 but exists in version 5.2.9. Similarly, the term **Added** indicates that a log ID was added in version 5.4.0 but does not exist in version 5.2.9.

Traffic

The following table provide a list of log IDs that were added newly or removed from the traffic log subtypes in FortiOS version 5.4.0.

Log ID	Message	Description
19	LOG_ID_TRAFFIC_BROADCAST	Added

Event

The following tables provide a list of log IDs that were added newly or removed between from the event log subtypes in FortiOS version 5.4.0.

Compliance-Check

Log ID	Message	Description
45151	LOG_ID_EVENT_DSSCC_FAIL	Added
45152	LOG_ID_EVENT_DSSCC_PASS	Added

Endpoint

Log ID	Message	Description
45056	LOG_ID_FCC_EXCEED	Removed
45059	LOG_ID_FCC_UPGRADE_SUCC	Removed

Log ID	Message	Description
45060	LOG_ID_FCC_UPGRADE_FAIL	Removed
45071	LOG_ID_FCC_VULN_SCAN	Added
45114	LOG_ID_EC_REG_QUARANTINE	Added
45115	LOG_ID_EC_REG_UNQUARANTINE	Added
45116	LOG_ID_EC_REG_UNQUARANTINE_ALL	Added
45117	LOG_ID_EC_REG_FAIL_VER	Added

HA

Log ID	Message	Description
35004	LOG_ID_HA_SYNC_FLDB	Added
35008	LOG_ID_HA_SYNC_VCM	Removed
35012	LOG_ID_CONF_SYNC_FAIL	Added
37907	MESGID_VLAN_HB_UP	Added
37908	MESGID_VLAN_HB_DOWN	Added
37909	MESGID_VLAN_HB_DOWN_SUM	Added

Router

Log ID	Message	Description
203202	LOG_ID_OSPF_NB_STAT_CHG	Added
20303	LOG_ID_OSPF6_NB_STAT_CHG	Added
20401	LOG_ID_ROUTER_CLEAR	Added

System

Log ID	Message	Description
20028	LOG_ID_REPORT_RECREATE_DB	Added

Log ID	Message	Description
20117	LOG_ID_AV_LIC_EXPIRED	Removed
20118	LOG_ID_WEBF_STATUS_REACH	Added
20119	LOG_ID_WEBF_STATUS_UNREACH	Added
22202	LOG_ID_AUTO_UPT_CERT_FAIL	Removed
22891	LOG_ID_FLCFGD	Added
26008	LOG_ID_DHCP_DDNS_ADD	Added
26009	LOG_ID_DHCP_DDNS_DELETE	Added
26010	LOG_ID_DHCP_DDNS_COMPLETED	Added
26011	LOG_ID_DHCPV6_REPLY	Added
26012	LOG_ID_DHCPV6_RELEASE	Added
29022	LOG_ID_DDNS_UPDATE_FAIL	Added
32044	LOG_ID_LOG_DELETE	Added
32112	LOG_ID_UPD_SIGN_NETSCAN_DB	Removed
32340	LOG_ID_LOG_DISK_UNAVAIL	Removed
32341	LOG_ID_LOG_DISK_DEFAULT_DISABLED	Removed
32547	LOG_ID_AUTOSCRIPT_START	Added
32548	LOG_ID_AUTOSCRIPT_STOP	Added
32560	LOG_ID_ADMIN_LOGIN_DISCLAIMER_SUCC	Removed
32563	LOG_ID_STORE_CONF_FAIL_FIRST_LINE	Removed
32569	LOG_ID_FSW_SWITCH_LOG_EVENT	Added
41005	LOG_ID_UPD_VCM	Removed
42201	LOG_ID_NETX_VMX_ATTACH	Added
42203	LOG_ID_NETX_VMX_DENIED	Added
44548	LOGID_EVENT_CONFIG_EXEC	Added
45161	LOG_ID_EVENT_DSSCC_EXEC	Added

VPN

Log ID	Message	Description
37140	MESGID_AUTO_IPSEC	Removed
40016	LOG_ID_L2TPD_SVR_DISCON	Removed
41991	LOG_ID_EVENT_VPN_CERT_EXPORT	Added

WAD

Log ID	Message	Description
48030	LOG_ID_WAD_SSL_CLIENT_CERT_REQUEST	Added

Wireless

Log ID	Message	Description
43609	LOG_ID_EVENT_WIRELESS_SYS_AC_DARRP_START	Added
43610	LOG_ID_EVENT_WIRELESS_SYS_AC_DARRP_STOP	Added
43611	LOG_ID_EVENT_WIRELESS_SYS_AC_UP	Added
43612	LOG_ID_EVENT_WIRELESS_SYS_AC_CFG_LOADED	Added
43613	LOG_ID_EVENT_WIRELESS_WTP_ERR	Added
43614	LOG_ID_EVENT_WIRELESS_DHCP_STAVATION	Added

Security (UTM)

The following tables provide a list of log IDs that were added newly or removed from the security (UTM) log subtypes in FortiOS version 5.4.0.

Web

Log ID	Message	Description
12560	LOG_ID_URL_WISP_BLOCK	Added

Log ID	Message	Description
12561	LOG_ID_URL_WISP_REDIR	Added
12562	LOG_ID_URL_WISP_ALLOW	Added

Email

Log ID	Message	Description
20480	LOGID_ANTISPAM_EMAIL_SMTP_NOTIF	Added
20481	LOGID_ANTISPAM_EMAIL_SMTP_BWORD_NOTIF	Added
20482	LOGID_ANTISPAM_EMAIL_POP3_NOTIF	Added
20483	LOGID_ANTISPAM_EMAIL_POP3_BWORD_NOTIF	Added
20484	LOGID_ANTISPAM_EMAIL_IMAP_NOTIF	Added
20485	LOGID_ANTISPAM_ENDPOINT_FILTER_WARNING	Added
20486	LOGID_ANTISPAM_ENDPOINT_FILTER_NOTIF	Added
20487	LOGID_ANTISPAM_ENDPOINT_MM7_WARNING	Added
20488	LOGID_ANTISPAM_ENDPOINT_MM7_NOTIF	Added
20489	LOGID_ANTISPAM_ENDPOINT_MM1_WARNING	Added
20490	LOGID_ANTISPAM_ENDPOINT_MM1_NOTIF	Added
20491	LOGID_ANTISPAM_EMAIL_IMAP_BWORD_NOTIF	Added
20492	LOGID_ANTISPAM_MM1_FLOOD_WARNING	Added
20493	LOGID_ANTISPAM_MM1_FLOOD_NOTIF	Added
20494	LOGID_ANTISPAM_MM4_FLOOD_WARNING	Added
20495	LOGID_ANTISPAM_MM4_FLOOD_NOTIF	Added
20496	LOGID_ANTISPAM_MM1_DUPE_WARNING	Added
20497	LOGID_ANTISPAM_MM1_DUPE_NOTIF	Added
20498	LOGID_ANTISPAM_MM4_DUPE_WARNING	Added

Log ID	Message	Description
20499	LOGID_ANTISPAM_MM4_DUPE_NOTIF	Added
20500	LOGID_ANTISPAM_EMAIL_MSN_NOTIF	Added
20501	LOGID_ANTISPAM_EMAIL_YAHOO_NOTIF	Added
20502	LOGID_ANTISPAM_EMAIL_GOOGLE_NOTIF	Added
20503	LOGID_EMAIL_SMTP_GENERAL_NOTIF	Added
20504	LOGID_EMAIL_POP3_GENERAL_NOTIF	Added
20505	LOGID_EMAIL_IMAP_GENERAL_NOTIF	Added
20506	LOGID_EMAIL_MAPI_GENERAL_NOTIF	Added
20507	LOGID_ANTISPAM_EMAIL_MAPI_BWORD_NOTIF	Added
20508	LOGID_ANTISPAM_EMAIL_MAPI_NOTIF	Added
20509	LOGID_ANTISPAM_FTGD_ERR	Added
41216	LOGID_GTP_FORWARD	Removed
41217	LOGID_GTP_DENY	Removed
41218	LOGID_GTP_RATE_LIMIT	Removed
41219	LOGID_GTP_STATE_INVALID	Removed
41220	LOGID_GTP_TUNNEL_LIMIT	Removed
41221	LOGID_GTP_TRAFFIC_COUNT	Removed
41222	LOGID_GTP_USER_DATA	Removed
41223	LOGID_GTPV2_FORWARD	Removed
41224	LOGID_GTPV2_DENY	Removed
41225	LOGID_GTPV2_RATE_LIMIT	Removed
41226	LOGID_GTPV2_STATE_INVALID	Removed
41227	LOGID_GTPV2_TUNNEL_LIMIT	Removed
41228	LOGID_GTPV2_TRAFFIC_COUNT	Removed

Log ID	Message	Description
41229	LOGID_GTPU_FORWARD	Removed
41230	LOGID_GTPU_DENY	Removed

GTP

Log ID	Message	Description
41216	LOGID_GTP_FORWARD	Added
41217	LOGID_GTP_DENY	Added
41218	LOGID_GTP_RATE_LIMIT	Added
41219	LOGID_GTP_STATE_INVALID	Added
41220	LOGID_GTP_TUNNEL_LIMIT	Added
41221	LOGID_GTP_TRAFFIC_COUNT	Added
41222	LOGID_GTP_USER_DATA	Added
41223	LOGID_GTPV2_FORWARD	Added
41224	LOGID_GTPV2_DENY	Added
41225	LOGID_GTPV2_RATE_LIMIT	Added
41226	LOGID_GTPV2_STATE_INVALID	Added
41227	LOGID_GTPV2_TUNNEL_LIMIT	Added
41228	LOGID_GTPV2_TRAFFIC_COUNT	Added
41229	LOGID_GTPU_FORWARD	Added
41230	LOGID_GTPU_DENY	Added

WAF

Log ID	Message	Description
30248	LOGID_WAF_SIGNATURE_BLOCK	Added
30249	LOGID_WAF_SIGNATURE_PASS	Added
30250	LOGID_WAF_SIGNATURE_ERASE	Added
30251	LOGID_WAF_CUSTOM_SIGNATURE_BLOCK	Added
30252	LOGID_WAF_CUSTOM_SIGNATURE_PASS	Added
30253	LOGID_WAF_METHOD_BLOCK	Added
30255	LOGID_WAF_ADDRESS_LIST_BLOCK	Added
30257	LOGID_WAF_CONSTRAINTS_BLOCK	Added
30258	LOGID_WAF_CONSTRAINTS_PASS	Added
30259	LOGID_WAF_URL_ACCESS_PERMIT	Added
30260	LOGID_WAF_URL_ACCESS_BYPASS	Added
30261	LOGID_WAF_URL_ACCESS_BLOCK	Added

Other

Netscan

Log ID	Message	Description
4096	LOG_ID_NETSCAN_VULN_SCAN	Removed
4097	LOG_ID_NETSCAN_DISCOVERY_SCAN	Removed
4098	LOG_ID_NETSCAN_VULN_DETECT	Removed
4099	LOG_ID_NETSCAN_OS_DETECT	Removed
4100	LOG_ID_NETSCAN_SERVICE_DETECT	Removed

Log ID	Message	Description
4101	LOG_ID_NETSCAN_VULN_MESSAGE	Removed
4102	LOG_ID_NETSCAN_DISCOVERY_MESSAGE	Removed
4103	LOG_ID_NETSCAN_VULN_COUNT	Removed
4104	LOG_ID_NETSCAN_HOST_DETECT	Removed
4105	LOG_ID_NETSCAN_PORT_DETECT	Removed

FORTINET®

High Performance Network Security

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.