FORTINET®

High Performance Network Security

FortiOS - FortiOS Log Reference

VERSION 5.2.5

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

FORTINET®

January 27, 2017

FortiOS 5.2.5 FortiOS Log Reference

01-525-302745-20170127

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-12-07	Updated for version 5.2.5.
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.

This chapter includes the following topics:

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*.

NOTE: 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

Log Types and Sub Types

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

Log Details

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 • 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.	• System • High Availability • Router • Endpoint Control • GTP • Virtual Private Network (VPN) • WAD • Wireless • User

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).

Priority Levels

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	Funcationality is affected.
3	Error	An error exists and funcationality could be affected.
4	Warning	Funcationality 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.

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.

Example: Log Message Details

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.

Example: 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 entries.

Header and Body Fields

Each log entry 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 caategory, severity level, and where the log originated. These fields are common to all log types.
- Body - Describes the reason why the log was created and actions taken by the FortiGate device to address it. These fields vary by log type.

Following is an example of traffic log entry 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 describes each possible header and body field, according to its name as it appears in the **Formatted** or **Raw** view.

Example: Traffic Log (Raw Format)

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`

Example: Traffic Log (Raw Format)

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (raw format)
MSG (msg)	See Message IDs	√	√	√	`msg=000100000012`
Type (type)	See Type	√	√	√	`type=traffic`
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 protocl 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`

Example: Traffic Log (Raw Format)

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (raw format)
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`
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`".

Log ID number components	Description	Examples
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 - gtp:6 - endpoint:7 - ha:8

Log Type IDs	Sub Type IDs
antivirus: 2	• virus:2 • suspicious:0 • analytics:1 • botnet:2 • infected:11 • filename:12 • oversize:13 • scanerror:62 • switchproto:63
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
UTM	• virus:2 • webfilter:3 • ips:4 • spam:5 • contentlog:6 • voip:8 • dlp:9 • app-ctrl:10

Log Types and Sub Types

FortiGate devices can record the following types and subtypes of log messages:

Log Types and Sub Types

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 • 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.	• System • High Availability • Router • Endpoint Control • GTP • Virtual Private Network (VPN) • WAD • Wireless • User

Type

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

Subtype

Each log message contains a Sub Type (subtype) field that further subdivides its category based on the feature associated with the cause of the log message.

For example:

- In event logs, some logs have a subtype of user, system, or other subtypes.
- In security (UTM) logs, some logs have a subtype of *waf_illegal_xml_format*, *waf_padding_oracle,* or other subtypes.
- In traffic logs, the subtypes are: local, forward, multicast, and sniffer.

Priority Level

Each log message contains a Level (pri) field that indicates the estimated severity of the event that caused the log message, 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).

Priority Levels

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	Funcationality is affected.
3	Error	An error exists and funcationality could be affected.
4	Warning	Funcationality 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 12-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 Message Format

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

Example: Log Message Details

Message ID	Message	Severity
2	LOG_ID_TRAFFIC_ALLOW	Notice

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 caategory, 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 describes each possible header and body field, according to its name as it appears in the**Formatted** or **Raw** view.

Example: Traffic Log (Raw Format)

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`
Sub Type (subtype)	See Sub Type	√	√	√	`subtype=local`

Example: Traffic Log (Raw Format)

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (Raw format)
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 protocl 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-p=10.6.30.254`

Example: Traffic Log (Raw Format)

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (Raw format)
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 traffic	√	√	√	`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`

Example: Traffic Log (Raw Format)

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (Raw format)
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

Log ID is a 10 digit number and it shows in the logs as ‘logid’ field. It consists of the information for 3 parts:

- The first 2 digits are for Type, eg Traffic log starts with '00' and Event log starts with '01'

The ID (log_id) is a 10-digit field located in the header, immediately following the time and date fields. It includes the following:

Log Type	SubType or EventType	Message ID
First 2 digits. Example: Traffi log begins with "00". Event log begins with "01"	Second 2 digits. Example: The 2nd two digits are for Subtype: eg. the VPN Subtype for Event log is '01', thus all VPN related Event log IDs will begin with: 0101... - The last 6 digits are for Message ID	

`Log Type, Subtype or Eventtype and Message ID`

The log_id field is a number assigned to all permutations of the same message. It classifies a log message 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.

For example, an administrator account always has the log ID `00003401`.

FortiOS 5.2 Log Messages

The following tables list the FortiOS 5.2 log messages.

Anomaly

Log Field Name	Description	Data Type	Length
action		string	16
agent		string	66
attack		string	256
attackcontext		string	2040
attackcontextid		string	10
attackid		uint32	10
count		uint32	10
craction		uint32	10
crlevel		string	10
crscore		uint32	10
date		string	10
devid		string	16
direction		string	8
dstintf		string	64
dstip		ip	39
dstport		uint16	5
eventtype		string	32
group		string	64
hostname		string	256

Log Field Name	Description	Data Type	Length
icmpcode		string	6
icmpid		string	8
icmptype		string	6
incidentserialno		uint32	10
level		string	11
logid		string	10
msg		string	518
policyid		uint32	10
policyid		uint32	64
profiletype		string	64
proto		uint8	3
ref		string	
service		string	36
sessionid		uint32	10
severity		string	8
sniffer		uint32	64
srcintf		string	64
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
user		string	256
vd		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		string	10
crscore		uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of the packets	string	8
dstintf		string	64
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstname		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
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid		uint32	10
profile		string	36
profiletype		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		string	64
srcip	Source IP	ip	39
srcname		string	64
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8

Log Field Name	Description	Data Type	Length
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

Log Field Name	Description	Data Type	Length
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		string	10
crscore		uint32	10
date	Date	string	10
devid	Device serial number	string	16
direction	Message/packets direction	string	8
dstintf		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		uint32	10

Log Field Name	Description	Data Type	Length
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
sessionid	Session ID	uint32	10
srcintf		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
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

Message ID	Message	Severity
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
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
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

Log Field Name	Description	Data Type	Length
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		string	32
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		string	3

Log Field Name	Description	Data Type	Length
msg	Log message	string	512
policyid		uint32	10
profile	DLP 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 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		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
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		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

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	512
policyid		uint32	10
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		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
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
41227	LOGID_GTPV2_TUNNEL_LIMIT	Information
41228	LOGID_GTPV2_TRAFFIC_COUNT	Information
41229	LOGID_GTPU_FORWARD	Information
41230	LOGID_GTPU_DENY	Information

Event

Log Field Name	Description	Data Type	Length

Event Log Messages

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

Message ID	Message	Severity

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
date	Date	string	10
devid	Device ID	string	16
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	Message	string	
name	Display Name of the Connection	string	128
reason	Reason	string	256
repeat	Number of Times Repeated for the Action	uint16	5
status	Status	string	23
subtype	Log subtype	string	20
time	Time	string	8
type	Log Type	string	16
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
used_for_type	Connection for the type	uint16	5
user	User Name	string	256
vd	Virtual Domain	string	32

Event Log Messages

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

Message ID	Message	Severity
45056	LOG_ID_FCC_EXCEED	Notice
45057	LOG_ID_FCC_ADD	Information
45058	LOG_ID_FCC_CLOSE	Information
45059	LOG_ID_FCC_UPGRADE_SUCC	Notice
45060	LOG_ID_FCC_UPGRADE_FAIL	Error
45061	LOG_ID_FCC_CLOSE_BY_TYPE	Information
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

Message ID	Message	Severity
45112	LOG_ID_EC_REG_FAIL_KEY	Warning
45113	LOG_ID_EC_REG_FAIL_BLOCKED	Warning

GTP

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
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 teid	uint32	10
cpdlteid	control plane downlink teid	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

Log Field Name	Description	Data Type	Length
dstport		uint16	5
dtlexp	Detailed Explanation	string	64
duration	tunnel duration	uint32	10
end-usr-address	End User IP Address	ip	39
from		string	128
headerteid		uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv		string	32
imsi	International mobile subscriber ID	string	16
level		string	11
linked-nsapi		uint8	3
logdesc		string	
logid		string	10
msg		string	
msg-type		uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
nsapi		uint8	3
profile		string	64
rai		string	32
rat-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		uint16	5

Log Field Name	Description	Data Type	Length
status		string	23
subtype	Log Subtype	string	20
time	Time	string	8
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
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 teid	uint32	10
uli		string	32
user_data	user traffic content inside gtp-u tunnel	string	256
vd		string	32
version		string	64

Event Log Messages

The following table describes the log message IDs and messages of the Event 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

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

HA

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

Log Field Name	Description	Data Type	Length
level		string	11
logdesc		string	
logid		string	10
msg		string	
sn		string	64
subtype		string	20
sync_status	The sync status with the master	string	11
sync_type	The sync type with the master	string	14
time		string	8
to_vcluster	destination virtual cluster number	uint32	10
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		string	32
vdname	vdom name	string	16

Event Log Messages

The following table describes the log message IDs and messages of the Event 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
35005	LOG_ID_HA_SYNC_IPS	Notice
35007	LOG_ID_HA_SYNC_AV	Notice

Message ID	Message	Severity
35008	LOG_ID_HA_SYNC_VCM	Notice
35009	LOG_ID_HA_SYNC_CID	Notice
35010	LOG_ID_HA_SYNC_FAIL	Error
35011	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
37900	MESGID_HBDEV_DELETE	Notice
37901	MESGID_HBDEV_DOWN	Critical
37902	MESGID_HBDEV_UP	Information
37903	MESGID_SYNC_STATUS	Information
37904	MESGID_HA_ACTIVITY	Information
37905	MESGID_HA_ENABLE_SET_AS_MASTER	Notice
37906	MESGID_HA_DISABLE_SET_AS_MASTER	Notice

ROUTER

Log Field Name	Description	Data Type	Length
action		string	32
date	Date	string	10
devid	Device ID	string	16
dhcp_msg		string	
dns_ip		ip	39
dns_name		string	64
dst_int		string	64
interface	Interface	string	32
lease		uint32	10
level	Log Level	string	11
logdesc		string	
logid	Log ID	string	10
mac		string	17
msg	Message	string	
service		string	64
src_int		string	64
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
vd	Virtual Domain	string	32

Event Log Messages

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

Message ID	Message	Severity
20300	LOG_ID_BGP_NB_STAT_CHG	Unknown
20301	LOG_ID_VZ_LOG	Unknown
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

Log Field Name	Description	Data Type	Length
cipher	Encryption Type	uint16	
community		string	36
conserve	Flag for Conserve Mode	string	32
count	Count	uint32	10
cpu	CPU Usage	uint8	3
created	Sessions Created	string	64
crl		string	
daddr	Destination IP Address	string	80
daemon	Daemon Name	string	32
datarange	data range for reports	string	50
date	Date	string	10
desc	Description	string	128
devid	Device ID	string	16
dhcp_msg	DHCP Message	string	
dintf	Destination Interface	string	36
dir		string	8
disk	Disk Usage	uint8	3
disklograte		uint64	20
dns_ip	DNS IP Address	ip	39
dns_name	DNS Name	string	64
dst_int	Destination Interface	string	64
dstip		ip	39
dstport		uint16	5
duration	Duration	uint32	10

Log Field Name	Description	Data Type	Length
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		string	
expectedsignature		uint8	
fams_pause		uint32	10
fazlograte		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		string	64
groupid	User Group ID	uint32	10
handshake		string	32
hash	Hash Value of Downloaded File	string	32
hostname	Hostname	string	128
identidx	use 'id' ?	uint32	10
infected	Infected MMS	uint32	10
informationsource		string	
intercepted	Intercepted MMS	uint32	10
interface	Interface	string	32

Log Field Name	Description	Data Type	Length
intf	Interface	string	16
ip		ip	39
iptype	IP Protocol Type	string	16
lease	DHCP Lease	uint32	10
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		string	
logid	Log ID	string	10
mac		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		string	12
module	Configuration Module Name	string	32
monitor-name	Health Monitor Type	string	32
monitor-type	Health Monitor Name	string	32

Log Field Name	Description	Data Type	Length
msg	Message Text	string	
msgproto	Message Protocol Number	string	16
mtu	Max Transmission Unit Value	uint32	10
name	Name	string	128
nat	NAT IP Address	ip	39
new_status	New Status	string	512
new_value	New Virtual Domain Name	string	128
newchannel	New Channel Number	uint8	
newchassisid	New Chassis ID	uint8	
newslot	New Slot Number	uint8	
nf_type	Notification Type	string	14
old_status	Original Status	string	512
old_value	Original Virtual Domain name	string	16
oldchannel	Original Channel Number	uint8	
oldchassisid	Original Chassis Number	uint8	
oldslot	Original Slot Number	uint8	
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

Log Field Name	Description	Data Type	Length
process	Process	string	
processtime	process time for reports	uint32	
profile		string	64
profile_vd	Virtual Domain Name	string	64
profilegroup	Profile Group Name	string	4
profiletype	Profile Type	string	64
proto	Protocol Number	uint8	3
reason	Reason	string	256
received	Received Packet	uint8	
receivedhandshake		string	
receivedsignature		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	Service Name	string	64
sess_duration	Session Duration	uint32	10
session_id	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
setuprate	Session Setup Rate	uint64	20
slot	Slot Number	uint8	
sn		string	64
src_int	Source Interface	string	64
srcip		ip	39
srcport		uint16	5
ssl2		uint8	
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		uint32	10
url		string	512
used	Number of Used IPs	uint32	10
user	User Name	string	256

Log Field Name	Description	Data Type	Length
vd	Virtual Domain	string	32
version		string	64
vip	Virtual IP	string	64
virus	Virus Name	string	128

Event Log Messages

The following table describes the log message IDs and messages of the Event 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

Message ID	Message	Severity
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
20027	LOG_ID_REPORT_DEL_OLD_REC	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

Message ID	Message	Severity
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
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

Message ID	Message	Severity
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
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	Information
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

Message ID	Message	Severity
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
20115	LOG_ID_IPSA_STATUSUPD_FAIL	Error
20116	LOG_ID_SPAM_LIC_EXPIRED	Critical
20117	LOG_ID_AV_LIC_EXPIRED	Critical
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

Message ID	Message	Severity
22005	LOG_ID_FAIL_CREATE_SOCKET_RETRY	Warning
22006	LOG_ID_FAIL_REG_CMDB_EVENT	Warning
22009	LOG_ID_FAIL_FIND_AV_PROFILE	Warning
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

Message ID	Message	Severity
22110	LOG_ID_SPARE_BLOCK_LOW	Critical
22150	LOG_ID_VOLT_NOM	Notice
22151	LOG_ID_FAN_NOM	Notice
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
22202	LOG_ID_AUTO_UPT_CERT_FAIL	Error
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
22900	LOG_ID_CAPUTP_SESSION	Notice
22901	LOG_ID_FAZ_CON	Notice

Message ID	Message	Severity
22902	LOG_ID_FAZ_DISCON	Notice
22903	LOG_ID_FAZ_CON_ERR	Critical
22913	LOG_ID_FDS_SRV_DISCON	Notice
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
29001	LOG_ID_PPPD_MSG	Unknown
29002	LOG_ID_PPPD_AUTH_SUC	Notice
29003	LOG_ID_PPPD_AUTH_FAIL	Notice
29009	LOG_ID_PPPOE_STATUS_REPORT	Notice
29011	LOG_ID_PPPD_FAIL_TO_EXEC	Error

Message ID	Message	Severity
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
32001	LOG_ID_ADMIN_LOGIN_SUCC	Information
32002	LOG_ID_ADMIN_LOGIN_FAIL	Alert
32003	LOG_ID_ADMIN_LOGOUT	Information
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	Emergency
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
32016	LOG_ID_FDS_QUOTA_WARN	Emergency
32017	LOG_ID_FDS_DAILY_QUOTA_FULL	Alert
32018	LOG_ID_FIPS_ENTER_ERR_MOD	Emergency

Message ID	Message	Severity
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
32042	LOG_ID_MEM_LOG_SECOND_FULL	Warning
32043	LOG_ID_MEM_LOG_FINAL_FULL	Warning
32045	LOG_ID_MGR_LIC_EXPIRE	Warning

Message ID	Message	Severity
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
32112	LOG_ID_UPD_SIGN_NETSCAN_DB	Critical
32113	LOG_ID_UPD_SIGN_SRCVIS_DB	Critical
32114	LOG_ID_UPD_SIGN_GEOIP_DB	Critical
32115	LOG_ID_UPD_SIGN_SERVER_LIST	Critical

Message ID	Message	Severity
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
32153	LOG_ID_DEL_IP6_LOCAL_POL	Notice
32155	LOG_ID_ACT_FTOKEN_REQ	Notice
32156	LOG_ID_ACT_FTOKEN_SUCC	Notice

Message ID	Message	Severity
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	Notice
32205	LOG_ID_RESTORE_VDOM_LIC	Critical
32206	LOG_ID_RESTORE_SCRIPT	Warning
32207	LOG_ID_RETRIEVE_CONF_LIST	Warning

Message ID	Message	Severity
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
32230	LOG_ID_LOAD_IMG_FAIL_INVALID_RSA	Critical
32231	LOG_ID_RESTORE_FGD_SVR_FAIL	Critical
32232	LOG_ID_RESTORE_VDOM_LIC_FAIL	Notice

Message ID	Message	Severity
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
32340	LOG_ID_LOG_DISK_UNAVAIL	Warning
32341	LOG_ID_LOG_DISK_DEFAULT_DISABLED	Notice
32400	LOG_ID_CONF_CHG	Alert
32545	LOG_ID_SYS_RESTART	Critical

Message ID	Message	Severity
32546	LOG_ID_APPLICATION_CRASH	Warning
32560	LOG_ID_ADMIN_LOGIN_DISCLAIMER_SUCC	Information
32561	LOG_ID_ADMIN_LOGOUT_DISCONNECT	Information
32562	LOG_ID_STORE_CONF_FAIL_SPACE	Critical
32563	LOG_ID_STORE_CONF_FAIL_FIRST_LINE	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
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
38411	LOGID_EVENT_TWO_F_AUTH_CODE_SENDTO	Notice
38412	LOGID_EVENT_TOKEN_CODE_SENDTO	Notice

Message ID	Message	Severity
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
41005	LOG_ID_UPD_VCM	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	Information
44545	LOGID_EVENT_CONFIG_OBJ	Information
44546	LOGID_EVENT_CONFIG_ATTR	Information
44547	LOGID_EVENT_CONFIG_OBJATTR	Information
45000	LOG_ID_VSD_SSL_RCV_HS	Debug

Message ID	Message	Severity
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
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

Message ID	Message	Severity
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
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

Log Field Name	Description	Data Type	Length
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		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		string	
logid	Log ID	string	10
msg	Message	string	
oldwprof	Old Web Filter Profile	string	64
policyid	Policy ID	uint32	10
poolname		string	36
portbegin		uint16	5
portend		uint16	5
proto	Protocol Number	uint8	3
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
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		string	64
user	User Name	string	256
vd	Virtual Domain Name	string	32

Event Log Messages

The following table describes the log message IDs and messages of the Event 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
38658	LOGID_EVENT_RAD_RPT_CTX_NOT_FOUND	Notice
38659	LOGID_EVENT_RAD_RPT_ACCT_STOP_MISSED	Notice

Message ID	Message	Severity
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
43027	LOG_ID_EVENT_AUTH_PROXY_TIME_OUT	Notice
43028	LOG_ID_EVENT_AUTH_PROXY_AUTHORIZATION_FAILED	Notice

Message ID	Message	Severity
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		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		string	53
espauth	ESP Authentication	string	17
esptransform	ESP Transform	string	8
exch	In SPI	string	12
group	User Name Group	string	64

Log Field Name	Description	Data Type	Length
in_spi		string	16
init		string	6
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		string	64
mode		string	12
msg	Message	string	
name		string	128
nextstat	Time interval in seconds for the next statistics	uint32	10
out_spi	Out SPI	string	16
outintf	Out interface	string	32
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		string	9
sentbyte	Bytes Sent	uint64	20
seq	Sequence	string	16

Log Field Name	Description	Data Type	Length
spi		string	16
stage		uint8	3
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		string	64
user		string	256
vd	Virtual Domain	string	32
vpntunnel	IPsec Vpn Tunnel Name	string	128
xauthgroup	XAuth Group Name	string	128
xauthuser	XAuth User Name	string	128

Event Log Messages

The following table describes the log message IDs and messages of the Event 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
37124	MESGID_NEG_I_P1_ERROR	Error
37125	MESGID_NEG_I_P2_ERROR	Error

Message ID	Message	Severity
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
37140	MESGID_AUTO_IPSEC	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
37191	MESGID_NEG_PROGRESS_P1_NOTIF_IKEV2	Unknown

Message ID	Message	Severity
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
39943	LOG_ID_EVENT_SSL_VPN_SESSION_NEW_CON	Unknown

Message ID	Message	Severity
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
40016	LOG_ID_L2TPD_SVR_DISCON	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

WAD

Log Field Name	Description	Data Type	Length
action		string	32
addr_type		string	4
alert		string	256
app-type		string	64
authgrp		string	36

Log Field Name	Description	Data Type	Length
date		string	10
desc		string	128
devid		string	16
dstip		ip	39
dstport		uint16	5
fqdn		string	256
fwserver_name		string	32
handshake		string	32
host		string	256
ip		ip	39
level		string	11
local		ip	39
logdesc		string	
logid		string	10
msg		string	
peer		string	36
policyid		uint32	10
port		uint16	5
reason		string	256
remote		ip	39
serial		uint32	10
session_id		uint32	10
srcip		ip	39
srcport		uint16	5

Log Field Name	Description	Data Type	Length
subtype		string	20
time		string	8
type		string	16
vd		string	32

Event Log Messages

The following table describes the log message IDs and messages of the Event 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
48027	LOG_ID_WAD_SSL_INVALID_CONT_TYPE	Error

Message ID	Message	Severity
48029	LOG_ID_WAD_SSL_BAD_CCS_LEN	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		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		string	42
bssid	Service Set ID	string	17
cfgtxpower	Config TX power	uint32	10
channel		uint8	3
configcountry	Config Country	string	4

Log Field Name	Description	Data Type	Length
date		string	10
detectionmethod		string	21
devid		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		string	12
frametype		string	32
group		string	64
invalidmac	the MAC address with invalid OUI	string	17
ip		ip	39
level		string	11
live	time in seconds	uint32	10
logdesc		string	
logid		string	10
mac		string	17
manuf	Manufacturer name	string	20
meshmode	Mesh mode	string	19
mgmtcnt	The number of unauthorized client flooding managemet frames	uint32	10
msg		string	
noise		int8	4

Log Field Name	Description	Data Type	Length
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		string	64
radioband		string	64
radioid		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		uint16	5
reason		string	256
rssi	Received signal strength indicator	uint8	3
security		string	40
securitymode		string	40
seq		string	16
signal		int8	4
sn		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		ip	39
ssid	Base Service Set ID	string	33
stacount	Number of stations/clients	uint32	10
stamac	Station/Client MAC address	string	17
subtype		string	20

Log Field Name	Description	Data Type	Length
tamac	the MAC address of Transmitter, if none, then Receiver	string	17
threattype	WIDS threat type	string	64
time		string	8
type		string	16
user		string	256
vap		string	36
vd		string	32
weakwepiv	Weak Wep Initiation Vector	string	8

Event Log Messages

The following table describes the log message IDs and messages of the Event 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
43546	LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH	Notice
43548	LOG_ID_EVENT_WIRELESS_WIDS_ASLEAP	Notice

Message ID	Message	Severity
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
43572	LOG_ID_EVENT_WIRELESS_STA_ASSO	Notice
43573	LOG_ID_EVENT_WIRELESS_STA_AUTH	Notice

Message ID	Message	Severity
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
43596	LOG_ID_EVENT_WIRELESS_CLB_RETRY	Notice
43597	LOG_ID_EVENT_WIRELESS_WTP_ADD	Notice

Message ID	Message	Severity
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

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		uint32	10

Log Field Name	Description	Data Type	Length
crlevel		string	10
crscore		uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of packets	string	8
dstintf		string	64
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtype	IPS Event Type	string	32
group	User group name	string	64
hostname		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		uint32	10
policyid		uint32	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

Log Field Name	Description	Data Type	Length
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
sniffer		uint32	64
srcintf		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 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

Netscan

Log Field Name	Description	Data Type	Length
action		string	17
agent		string	64
assetid		uint32	10

Log Field Name	Description	Data Type	Length
assetname		string	64
date		string	10
devid		string	16
direction		uint32	10
dstintf		string	32
dstip		ip	39
dstname		string	64
dstport		uint16	5
end		uint32	10
engine		string	32
eventtype		string	32
group		string	64
level		string	11
logid		string	10
method		string	4
msg		string	
os		string	
osfamily		string	64
osgen		string	64
osvendor		string	64
plugin		string	32
policyid		uint32	10
profile		string	64
profilegroup		string	4

Log Field Name	Description	Data Type	Length
proto		string	3
serial		uint32	10
service		string	64
severity		string	8
srcintf		string	32
srcip		ip	39
srcname		string	64
srcport		uint16	5
start		uint32	10
status		string	8
subtype		string	20
time		string	8
type		string	16
user		string	256
vd		string	32
vuln		string	128
vulncat		string	32
vulncnt		uint32	10
vulnid		uint32	10
vulnref		string	
vulnscore		string	128

Netscan Log Messages

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

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

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
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
apprisk	Application Risk Level	string	16
collectedemail	Email address from Email Collection Captive Portal	string	66

Log Field Name	Description	Data Type	Length
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
countweb	Number of the Web Filter logs associated with the session	uint32	10
craction	Action performed by Client Reputation	uint32	10
crlevel		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
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

Log Field Name	Description	Data Type	Length
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
poluuid	UUID of the Firewall Policy	string	37
proto	protocol number	uint8	3
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	36
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
srccountry	Country name for Source IP	string	64
srcintf	Source interface name	string	32

Log Field Name	Description	Data Type	Length
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
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
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
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
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

VoIP

Log Field Name	Description	Data Type	Length
action		string	15
call_id		string	64
column		uint32	10

Log Field Name	Description	Data Type	Length
count		uint32	10
date		string	10
devid		string	16
dir		string	8
dst_int		string	16
dst_port		uint16	5
dstip		ip	39
duration		uint32	10
endpoint		string	128
epoch		uint32	10
event_id		uint32	10
eventtype		string	32
from		string	128
group		string	64
kind		string	10
level		string	11
line		string	64
logid		string	10
malform_data		uint32	10
malform_desc		string	47
message_type		string	16
phone		string	64
policy_id		uint32	10
profile		string	64

Log Field Name	Description	Data Type	Length
profile_group		string	64
profile_type		string	64
proto		uint8	3
reason		string	128
request_name		string	64
session_id		uint32	10
src_int		string	16
src_port		uint16	5
srcip		ip	39
status		string	23
subtype		string	20
time		string	8
to		string	512
type		string	16
user		string	256
vd		string	32
voip_proto		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

Message ID	Message	Severity
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

WAF Log Messages

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

Message ID	Message	Severity

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		string	10
crscore		uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
direction	Direction of the web traffic	string	8

Log Field Name	Description	Data Type	Length
dstintf		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
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		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

Log Field Name	Description	Data Type	Length
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
reqtype	Request type	string	8
ruledata	Rule data	string	512
ruletype	Rule type	string	9
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcintf		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
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
12800	LOG_ID_WEB_FTGD_ERR	Error

Message ID	Message	Severity
12801	LOG_ID_WEB_FTGD_WARNING	Warning
12802	LOG_ID_WEB_FTGD_QUOTA	Information
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 Diff for 5.2.4 and 5.2.5

Refer to the *FortiOS Log Reference Guide Version 5.2.4* for a complete list of log field details related to version 5.2.4. This section covers changes applicable to the 5.2.5 version only. It is recommended that you keep both the 5.2.4 and 5.2.5*FortiOS Log Reference Guides* 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 5.2.5 but exists in version 5.2.4. Similarly, the term **Added** indicates that a log filed was added in version 5.4.0 but does not exist in version 5.2.4.

Traffic

The following table provide a list of log fields that were added newly or removed from the traffic log subtypes in FortiOS version 5.2.5.

Log Field Name	Description
N/A	N/A

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 5.2.5.

System

Log Field Name	Description
member	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 5.2.5.

Anomaly

Log Field Name	Description
policyid	Added
profile	Removed
sniffer	Added

Application

Log Field Name	Description
policyid	Added

DLP

Log Field Name	Description
policyid	Added

Email

Log Field Name	Description
policyid	Added

IPS

Log Field Name	Description
policyid	Added
profile	Removed
sniffer	Added

Web

Log Field Name	Description
policyid	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 5.2.5.

Log Field Name	Description
N/A	N/A

FORTINET®

High Performance Network Security